Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Digitaler Verbraucherschutz: BSI-Jahresrückblick 2023

Themen-
schwerpunkt:

Digitale Verbraucher-resilienz

Inhaltsverzeichnis

Vorwort 3

1 Verbraucherinnen und Verbraucher in der vernetzten Welt besser schützen! 4

2 Jahresübersicht 2023: Relevante Bedrohungen auf dem digitalen Verbrauchermarkt 8

3 Bessere digitale Verbraucherresilienz – aber wie? 14

4 Cybersicherheit für Unternehmen und Institutionen nützt allen 22

5 Wissen, wo ich Hilfe finde – BSI-Angebote für Verbraucherinnen und Verbraucher 26

6 Literaturverzeichnis/Quellen 28

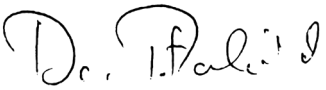
Vorwort

Ein Blick zurück auf die Ereignisse des vergangenen Jahres, sowohl auf IT-Vorfälle als auch auf Trendthemen im digitalen Verbrauchermarkt, ist für uns immer auch ein Blick nach vorn. Als zentraler Ansprechpartner für den Digitalen Verbraucherschutz in Deutschland ist es unser Anspruch, die Menschen in ihrem digital vernetzten Alltag besser zu schützen. Dafür stehen wir als Bundesamt für Sicherheit in der Informationstechnik (BSI) als neutrale Cybersicherheitsbehörde gemeinsam mit unseren Partnern und weiteren Akteuren.

Wir leben in einer Zeit, in der die Digitalisierung mit ihren rasanten technologischen Entwicklungen unaufhaltsam voranschreitet. Da ist es unerlässlich, dass wir Schritt halten und proaktiv für eine Stärkung der IT-Sicherheit handeln. Eine für die Verbraucherinnen und Verbraucher einfache und zugleich sichere IT-Nutzung dürfen dabei keine Gegensätze sein!

Unsere intensive Informations-, Sensibilisierungs- und Aufklärungsarbeit verfolgt seit Jahren das Ziel, das Bewusstsein für IT-Sicherheit zu schärfen und den Menschen das notwendige Wissen und Werkzeug an die Hand zu geben, damit sie sich sicher in der digitalisierten Welt bewegen können. Eigenes Handeln reicht zum Schutz jedoch nicht aus. Deshalb wollen wir uns zukünftig viel stärker dem aktiven Schutz der Verbraucherinnen und Verbraucher widmen – dem aktiven Schutz vor den vielfältigen Gefahren, die im Umgang mit IT und im Netz lauern. Denn IT-Bedrohungen, die bei den Verbraucherinnen und Verbrauchern gar nicht erst ankommen, müssen von ihnen auch nicht erkannt und bewältigt werden. Das Ziel: Verbraucherinnen und Verbraucher sollen sich trotz einer sich kontinuierlich zuspitzenden IT-Gesamtbedrohungslage auch in Zukunft selbstbestimmt und sicher in der digitalen vernetzten Welt bewegen können.

Mit unserem Engagement leisten wir einen wichtigen Beitrag auf dem Weg zur Cybernation Deutschland. Denn nur wenn Verbraucherinnen und Verbraucher besser geschützt sind und unvermeidliche IT-Sicherheitsvorfälle bewältigen können, werden wir als Gesamtgesellschaft hinreichend widerstandsfähig gegenüber Cyberbedrohungen. Wir arbeiten kontinuierlich und mit hoher Intensität daran, die IT-Sicherheit für alle zu verbessern und so eine sichere digitale Zukunft zu gestalten - und laden Sie als Partner und Multiplikatoren dazu ein, dies gemeinsam mit uns zu tun.



Dr. Timo Hauschild,
Abteilungsleiter
Cyber-Sicherheit für Wirtschaft und Gesellschaft
Bundesamt für Sicherheit in der Informationstechnik (BSI)

1

Verbraucherinnen und Verbraucher in der vernetzten Welt besser schützen!

Der vorliegende Jahresrückblick des BSI macht deutlich, mit welchen vielfältigen Herausforderungen Verbraucherinnen und Verbraucher in ihrem digitalen Alltag konfrontiert sind.

So zeigen unter anderem die Sicherheitsvorfälle im digitalen Verbrauchermarkt für das Jahr 2023 (siehe Kapitel 2), dass der Schutz und die Resilienz der Menschen bei ihren Aktivitäten im Netz dringend verbessert werden müssen. Der thematische Schwerpunkt widmet sich daher der „Digitalen Verbraucherresilienz“ (siehe Kapitel 3) – im Fokus steht der Umgang mit digitalen Notfällen, Betrugsversuchen in der Online-Welt, aber auch mit technischen Pannen. Resiliente, also widerstandsfähige Verbraucherinnen und Verbraucher sind deutlich besser in der Lage, sich aktiv zu schützen, im Notfall schnell zu reagieren, Schäden zu minimieren und sich von Rückschlägen zu erholen.

Doch wie kann die Resilienz der Verbraucherinnen und Verbraucher grundsätzlich gestärkt werden? Können Verbraucherinnen und Verbraucher dies aus eigener Kraft – oder wer kann bzw. muss sie dabei unterstützen? Welche Instrumente sollten Menschen an die Hand gegeben werden, um ihre digitale Sicherheit und Privatsphäre zu schützen? Welche Rolle spielen technische Schutzmaßnahmen und Aktivitäten von Anbietern, Herstellern und Staat?

Diesen und weiteren Fragen geht der Themenschwerpunkt mit der gebotenen Intensität nach. Neben einer wissenschaftlich-analytischen Betrachtung kommen mit Expertinnen und Experten der Verbraucherzentrale Nordrhein-Westfalen e. V., des eco – Verband der Internetwirtschaft e. V. sowie der Hochschule Bonn-Rhein-Sieg auch Praxispartner des BSI zu Wort, um entsprechende Handlungsfelder zur Stärkung der digitalen Verbraucherresilienz für Akteure aus den Bereichen Staat, Wirtschaft und Gesellschaft aufzuzeigen. Mit der Darstellung der Arbeit der „Allianz für Cyber-Sicherheit“ wird zudem ein gesonderter Blick auf die Verantwortung der Hersteller und Anbieter in diesem Themenfeld geworfen (siehe Kapitel 4). Darüber hinaus werden die bereits bestehenden vielfältigen Informations- und Interaktionsangebote des BSI für Verbraucherinnen und Verbraucher näher beleuchtet (siehe Kapitel 5).

Die dargestellten Inhalte veranschaulichen unverkennbar: Wirksamer Digitaler Verbraucherschutz ist eine Gemeinschaftsaufgabe, die kooperativ gelöst werden muss. Deshalb richtet sich dieser BSI-Jahresrückblick an alle institutionellen Akteure und Multiplikatoren, die sich mit der digitalen Seite des Verbraucherschutzes beschäftigen. Wir wollen informieren, aktivieren, einbinden und so gemeinsam die Verbraucherinnen und Verbraucher in der vernetzten Welt besser schützen!

Februar

Neue Produktuntersuchung

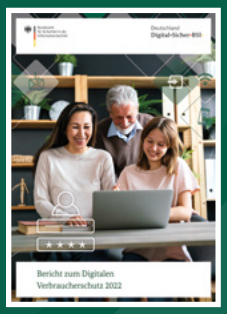
Veröffentlichung der Studie „IT-Sicherheit auf dem digitalen Verbrauchermarkt: Fokus Online-shopping-Plattformen“

Erste wissenschaftliche Tagung „Digitaler Alltag in Gefahr“

Schwerpunkt: Verbraucher-bezogene IT-Sicherheitsfor-schung

Veranstalter: BSI, Institut für Verbraucherinformatik (IVI), Kompetenzzentrum Verbrau-cherforschung NRW

März



Bericht zum Digitalen Verbraucherschutz 2022

Veröffentlichung des 3. Be-richts zum Digitalen Verbrau-cherschutz mit dem Schwer-punktthema „Gefahrenquelle Phishing“

Neues Informationsangebot

Start des regelmäßig erscheinenden „BSI-Newsletters für Partner und Akteure im Digitalen Verbraucherschutz“

April

Girls Day

Workshop mit Schülerinnen zum Thema „Sicher im digitalen Alltag“

Schwerpunkt: Smartphone- und App-Sicherheit

August

Gamescom

Messestand und Rahmenprogramm mit mehr als 3.000 Standbesucherin-nen und -be suchern

Thema: sicheres Gaming

Juni

1. Tag des Bevölkerungs-schutzes in Potsdam

Vorstellung des Cyber-Sicherheitsnetzwerkes sowie von Angeboten des Digitalen Verbraucherschutzes

it-sa IT-Security Messe und Kongress

Messestand des BSI mit Speakers-Corner

Roadshow „Digital? Aber sicher!“

Einmonatige Roadshow durch 16 sächsische Städte

Fokus: Aufklärung und Sensibilisierung gegenüber Cybersicherheitsthemen im digitalen Alltag

Dialog für Cybersicherheit

Durchführung der Denkwerkstatt 2023 in Frankfurt/M.: Dialogplattform für Themen der gesamtgesellschaftlichen Cybersicherheit

Veröffentlichung des Cybersicherheitsmonitors 2023

Publikation auf Grundlage einer deutschlandweiten Online-Befragung des BSI und der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK)

Fokus: Schutzverhalten und Betroffenheit der Bevölkerung in Bezug auf die Themen IT-Sicherheit und Cyberkriminalität

Kooperation

BSI und Bundeskartellamt verlängern ihre Kooperation im Digitalen Verbraucherschutz um weitere drei Jahre

Oktober

Dezember

September

November

Internationale Funkausstellung (IFA)

Themenstand zu IT-Sicherheitskennzeichen und zum Digitalen Verbraucherschutz

Berliner Cybersicherheitsgipfel 2023

Gestaltung der Paneldiskussion „Für besseren digitalen Verbraucherschutz: Sicherheitsstandards, Technologien und Trends“

Dialog für Cybersicherheit

Start von neuen Workstreams zu den Themen „Technische Anlaufstelle für Betroffene Digitaler Partnerschaftsgewalt“ und „Cyber-Resilience-Framework. In IT-Krisen schneller agieren“

2023 im Überblick

2

Jahresübersicht 2023: Relevante Bedrohungen auf dem digitalen Verbrauchermarkt

Der digitale Verbrauchermarkt unterliegt weiterhin einer angespannten Sicherheitslage. Datenleaks bei Unternehmen und Institutionen sowie Phishing-Angriffe auf Verbraucherinnen und Verbraucher gehören zu den häufigsten Bedrohungen. Gleichzeitig sorgten neue Trends wie die weite Verbreitung von Anwendungen mit sogenannter „Künstlicher Intelligenz“ (KI) für eine hohe Dynamik im digitalen Verbrauchermarkt, welche eine unmittelbare Auswirkung auf das Bedrohungspotential hat.

Zunahme von Betrugsmaschen durch KI

KI gehört für viele Menschen bereits zum digitalen Alltag. KI-gestützte Verbraucherprodukte und -dienste bieten breite, zukunftsträchtige und teils disruptive Anwendungsfelder, welche die Digitalisierung in der Gesellschaft vorantreiben. Es ist daher nicht überraschend eines der im Jahr 2023 meist debattierten Themen. Insbesondere breit verfügbare Anwendungen auf Basis generativer KI und großer Sprachmodelle (LLM: „Large Language Models"), wie Spracherkennungssysteme sowie textbasierte Audio-, Bild- und Videogeneratoren, prägten die Diskussion maßgeblich. Im Rahmen der Befragung „CyMon – Der Cybersicherheitsmonitor“ wurde festgestellt, dass 96 % der Befragten bereits von KI gehört haben. Mehr als die Hälfte der Befragten (60 %) gab sogar an, genau zu wissen, was mit KI gemeint ist.

Weniger bekannt sind KI-gestützte Betrugsmaschen. Auch die Kenntnis über das Risiko von Angriffen auf KI-Anwendungen ist wenig verbreitet. Durch die gestiegene Verfügbarkeit und Einfachheit von KI-Anwendungen benötigen Betrügerinnen und Betrüger keine technischen Vorkenntnisse oder Know-how im Bereich Programmierung, um etwa Sprachgeneratoren für ihre Zwecke zu nutzen. Mit wenigen Schritten lassen sich Betrugsmaschen umsetzen. KI-Anwendungen können beispielsweise täuschend echte Phishing-Mails erzeugen oder Stimmen nachahmen. Laut dem Cybersicherheitsmonitor kennt die Hälfte der Befragten (52 %) sogenannte "Schockanrufe" mit KI-generierten Stimmen als kriminelle Masche. Bekannt sind auch künstlich erstelltes und manipuliertes Video- und Bildmaterial (48 %), die Nutzung von Social-Media-Profildaten für Betrugsversuche (46 %) sowie Phishing-Nachrichten, die von KI-Sprachmodellen verfasst wurden (36 %). Dass Angreifende KI-Anwendungen mitunter manipulieren, also die eingebauten Regeln der KI umgehen könnten, ist weniger geläufig (14 %, vgl. Abbildung 1).

Der sensible Umgang mit persönlichen Daten ist von Bedeutung, um potenzielle Sicherheitsrisiken bei der Nutzung von generativer KI zu minimieren. Eine bedenkenlose Bereitstellung von Informationen in Anfragen an die KI („Prompting“) birgt das Risiko, dass Angreifer diese Informationen auslesen und missbräuchlich verwenden. Gleichermaßen kann es Angreifern durch das geschickte Formulieren solcher Anfragen gelingen, an sensible Informationen oder persönliche Daten Dritter zu gelangen, mit welchen beispielsweise die KI zu einem früheren Zeitpunkt trainiert worden ist.

Bluetooth-Tracker

Bluetooth-Tracker sind neuere technologische Produkte, die den digitalen Alltag erleichtern. Sie werden beispielsweise als Haustier-Tracker, Schlüsselfinder oder zum Lokalisieren anderer persönlicher Gegenstände genutzt. Ein Vorteil von Bluetooth-Trackern ist, dass sie in der Regel nicht größer als eine Geldmünze sind und dadurch leicht an Taschen, Kleidungsstücken oder anderen Gegenständen angebracht werden können.

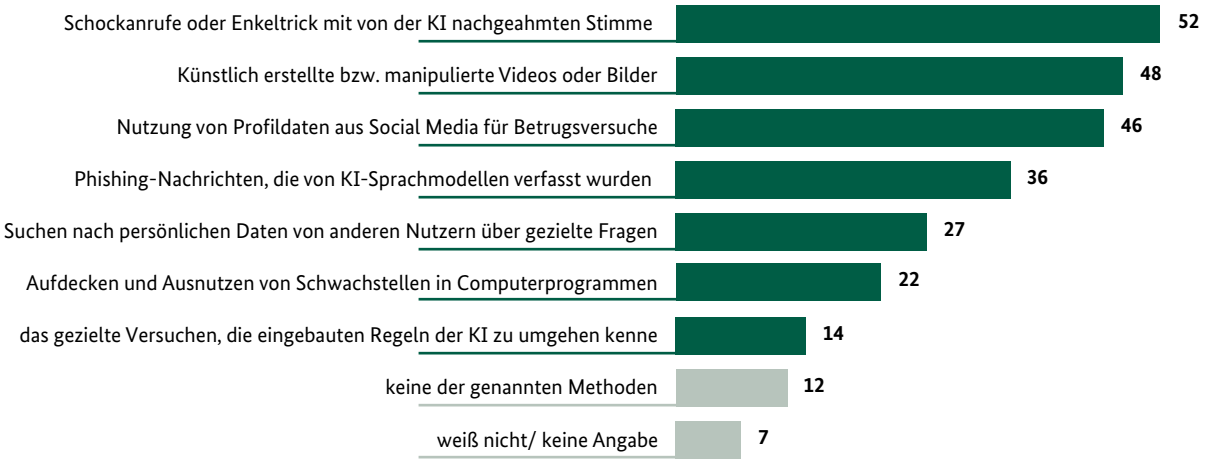


Abbildung 1 :Verbraucherkenntnisse zu Arten krimineller Methoden mittels KI in % (n=3.012, Mehrfachnennung möglich)

Durch missbräuchliche Nutzung bergen diese Technologien jedoch ein Gefahrenpotenzial, da sie es ermöglichen, Personen zu orten, zu kontrollieren oder zu verfolgen. Ein solcher Missbrauch wird als „Digitale Gewalt im sozialen Nahraum“ (vgl. bff 2021) bezeichnet.

Im Laufe des Berichtsjahres 2023 wurde die missbräuchliche Nutzung der kleinen Tracker mehrfach thematisiert und es haben sich mehrere Stalking-Opfer in Nachrichten und Medien zu Wort gemeldet. Das Bundeskriminalamt erfasste deutschlandweit 21.436 Stalking-Anzeigen, eine Steigerung um 4,7 % gegenüber 2022 (vgl. BKA 2022). Die Anzahl der Fälle, in denen die Tatverdächtigen digitale Hilfsmittel für ihre Straftat nutzten, ist zwar unbekannt, jedoch ist eine substanzielle Größenordnung naheliegend.

Aufgrund dieser Beobachtungen wird das Thema „Schutz vor digitaler Gewalt“ im Digitalen Verbraucherschutz des BSI aufgebaut. Der Workstream „Technische Anlaufstelle für Betroffene digitaler Partnerschaftsgewalt“ im Dialog für Cybersicherheit bearbeitet seit November 2023 das Thema mittels eines Multistakeholder-Ansatzes. Ein Zusammenschluss von Expertinnen und Experten setzt sich im Rahmen dessen dafür ein, die Relevanz des Themas in der Gesellschaft aufzuzeigen und Unterstützungsmöglichkeiten für Betroffene zu sichten und bereitzustellen.

Weiterführende Informationen zum Umgang mit KI sowie zu deren Chancen und Risiken finden Sie auf unserer Themenseite:

Wissenswertes zum Thema KI liefert darüber hinaus der Cybersicherheitsmonitor 2023:

Auswirkungen der Sicherheitslage im öffentlichen Sektor auf Verbraucherinnen und Verbraucher

Das Jahr 2023 war geprägt von zahlreichen Sicherheitsvorfällen bei öffentlichen Institutionen, wodurch viele Verbraucherinnen und Verbraucher teils gravierende Einschränkungen von Verwaltungsdienstleistungen oder die Offenlegung von sensiblen persönlichen Daten hinnehmen mussten. Cyberkriminelle griffen im Jahr 2023 digitale Infrastrukturen unter anderem von Kommunen, Krankenhäusern und Universitäten an.

Die Cyberattacke im Oktober 2023 auf einen kommunalen IT-Dienstleister in NRW war eine der größten Attacken auf die öffentliche Verwaltung in Deutschland. Die Gemeinden, Städte und Kreise selbst wurden nicht gehackt, jedoch waren viele Verwaltungsdienstleistungen nur eingeschränkt oder gar nicht verfügbar (vgl. SIT 2023).

Medien berichteten über insgesamt 16 Hochschulen, die von Cyberangriffen betroffen waren (vgl. KonBriefing 2023a). Im Juni 2023 wurde beispielsweise die IT-Infrastruktur einer Hochschule in Rheinland-Pfalz angegriffen. Die Folgen: Lahmgelegte IT-Systeme und durch Verschlüsselung unbrauchbar gewordene Daten. Zudem wurden Datensätze entwendet und im Darknet veröffentlicht (vgl. Hochschule Kaiserslautern 2023).

Auch eine Universität in Nordrhein-Westfalen fiel Cyberkriminellen zum Opfer. Hier wurden über einen ehemaligen Dienstleister personenbezogene Daten von 4.500 Hochschulangehörigen entwendet. Der im Darknet angebotene Datensatz enthielt Namen, E-Mail-Adressen und in rund 800 Fällen auch Passwort-Hashes der Betroffenen (vgl. CSO 2023).

Nicht alle Angriffe waren erfolgreich: Anfang Februar versuchten Unbekannte, in die Systeme einer thüringischen Universität einzudringen und interne Netzwerkrechte zu erlangen. Damit wäre es möglich gewesen, Netzwerke von außen vorübergehend abzuschalten, einzelne Systeme zu isolieren sowie Dienste und Server herunterzufahren. Der Zugriff wurde jedoch durch das Rechenzentrum unterbunden. Es handelte sich nicht um einen gezielten Angriff auf kritische IT-Strukturen der Universität. Vielmehr wurde ein Brute-Force-Angriff festgestellt. Es konnten keine Daten abgegriffen oder verschlüsselt werden. Die Studierenden waren nicht betroffen, lediglich einige wenige Mitarbeiterinnen und Mitarbeiter konnten vorübergehend ihren Arbeitsplatz nicht nutzen (vgl. DSGVO-Portal 2023).

Gefährdung von Verbraucherdaten durch eine Schwachstelle

Eine Mitte des Jahres bekannt gewordene Schwachstelle hatte weitreichende Folgen für zahlreiche Organisationen und gefährdete Verbraucherdaten. Der BSI-Lagebericht 2023 beschreibt ausführlich das Ausmaß der Sicherheitslücke. Der Softwarehersteller Progress gab am 31. Mai 2023 eine gravierende Schwachstelle seiner Transfersoftware MOVEit bekannt. Als Reaktion veröffentlichte das BSI am 1. Juni 2023 eine Cyber-Sicherheitswarnung (vgl. BSI 2023).

Am 2. Juni 2023 stellte Progress einen Patch für die kritische Schwachstelle zur Verfügung. Der Angreifergruppe Cl0p war es zuvor bereits gelungen, massenhaft sensible Daten von Organisationen zu kopieren. Noch im Juni begannen die Cyberkriminellen damit, die Daten der betroffenen Unternehmen auf ihrer Leak-Seite zu veröffentlichen. Laut Medienberichten waren circa 2.610 Organisationen weltweit von der Ausnutzung der Schwachstelle betroffen, etwa 40 davon in Deutschland. Die genaue Anzahl ist bis heute unbekannt, es kann mit einer hohen Dunkelziffer gerechnet werden (vgl. KonBriefing 2023b).

Zu den angegriffenen Organisationen gehörten unter anderem Banken, Krankenversicherungen und ein Preisvergleichsportal. Obwohl dieses Portal die betroffene Umgebung nach Bekanntwerden der Schwachstelle vom Netz nahm, konnten auch in diesem Fall sensible Kundendaten von den Angreifern kopiert werden. Eine forensische Untersuchung ergab, dass sich darunter persönliche Angaben wie Name, Adresse und E-Mail-Adresse sowie in einigen Fällen auch IBAN-Daten der Nutzerinnen und Nutzer befanden (vgl. Verivox 2023).

Unzureichender Accountschutz

Im Durchschnitt besitzt jeder Internetnutzende 78 Onlinekonten (vgl. DsiN 2023). Dementsprechend begleiten die nötigen Zugangsdaten wie Passwörter den digitalen Alltag. Sie werden für die Anmeldung in sozialen Netzwerken und in Onlineshops ebenso gebraucht wie für das Login auf Gaming-Plattformen. Laut Hasso-Plattner-Institut zählen einfache Passwörter wie „123456“ und „password“ nach wie vor zu den beliebtesten (vgl. HPI 2023). Die Einfachheit häufig genutzter Passwörter und die mehrfache Benutzung eines Passworts für verschiedene Onlinekonten führt zu der erhöhten Gefahr, dass Angreifer Zugang zu Accounts erlangen und auf die hinterlegten Daten zugreifen. Durch diesen unzureichenden Accountschutz werden Verbraucherinnen und Verbraucher häufig Opfer von Phishing-Angriffen und Identitätsdiebstahl.

Das BSI gibt die klare Empfehlung, Passwort-Manager zu nutzen, um sowohl eine hinreichende Komplexität von Passwörtern als auch deren Einzigartigkeit für einen spezifischen Account zu bewerkstelligen. Die Ausgestaltung und die Auswahl eines konkreten Passwort-Managers sind dabei abhängig von der individuellen Abwägung von gewünschten Nutzungsszenarien und tragbaren Risiken.

Eine gemeinsame Untersuchung des Bundeskanzleramtes und des BSI zum Schutz von Onlinekonten ergab, dass nur 39 % der Befragten Passwort-Manager zum Schutz von Onlineaccounts kennen. Von den Befragten, denen Passwort-Manager bekannt waren, gaben nur 37 % an, diese auch zu nutzen. Unter den 63 % der Befragten, die Passwort-Manager kennen, aber nicht nutzen, äußerten zwei Drittel Sicherheitsbedenken als Grund für diese Entscheidung (vgl. Bundeskanzleramt 2020).

Passwort-Manager als attraktives Angriffsziel

Aufgrund der Aggregierung von Zugangsdaten an einer Stelle ergibt es sich von selbst, dass Passwort-Manager ein attraktives Angriffsziel darstellen und einen besonderen Schutz benötigen. Dabei spielt die besagte Ausgestaltung der Nutzung eines Passwort-Managers die maßgebliche Rolle. Aller Ausgestaltung gemein ist das Anlegen eines hinreichend komplexen, merkfähigen und einmaligen Master-Passworts. Falls verfügbar, sollte ein zweistufiges Anmeldeverfahren für den Passwort-Manager eingerichtet werden („Zwei-Faktor-Authentisierung“).

Die Notwendigkeit solcher erhöhter Schutzmaßnahmen verdeutlicht folgender Vorfall: Unbekannten gelang der Zugriff auf die Onlinekonten eines Anbieters für Passwort-Manager und sie entwendeten die hinterlegten Anmeldedaten. Das betroffene Unternehmen stellte eine ungewöhnlich hohe Anzahl von Anmeldeversuchen fest – ein Indiz für Credential Stuffing. Dabei nutzen die Angreifer Anmeldedaten, die aus früheren Datenleak-Vorfällen stammen. Anfang 2023 verkündete der betroffene Anbieter, dass 925.000 inaktive und aktive Konten identifiziert wurden, die möglicherweise Ziel des Angriffs waren (vgl. Bleepingcomputer 2023a).

Passwort-Manager sind, wie dargestellt, ein sehr nützliches Werkzeug zur effektiven Steigerung der Cybersicherheit von Onlineaccounts. Das macht sie mitunter zum Ziel von Phishing-Kampagnen. Im Jahr 2023 versuchten Cyberkriminelle mit Phishing die Anmeldedaten von Nutzerinnen und Nutzern für den Zugang zu verschiedenen Passwort-Managern zu entwenden. Die von den Angreifern erstellten Phishing-Websiten waren darauf ausgerichtet, Anmeldedaten für Passworttresore sowie möglicherweise auch Authentifizierungs-Cookies zu stehlen (vgl. Bleepingcomputer 2023b).

Phishing als Gesamtbedrohung

Phishing ist weiterhin eine der größten Bedrohungen für Verbraucherinnen und Verbraucher. Im Zeitraum 1. Juni 2022 bis 30. Juni 2023 konnte in der E-Mail-Verkehrsstatistik beobachtet werden, dass Phishing-Mails unter den E-Mails mit betrügerischem Hintergrund mit 84 % am häufigsten vertreten sind. Phishing-Nachrichten zielen darauf ab, das Opfer mittels Social-Engineering-Techniken dazu zu bringen, seine Identitäts- beziehungsweise Authentisierungsdaten offenzulegen.

Demgegenüber wurden im genannten Zeitraum bei der Verbraucherzentrale NRW 30.576 Phishing-E-Mails gemeldet – ein Bruchteil der tatsächlich täglich versendeten Phishing-Mails. Es ist naheliegend, dass Provider und diverse Tools und Dienste mit Spam-Filter bereits

einen großen Teil dieser Nachrichten abfangen. Von den tatsächlich bei den Verbraucherinnen und Verbrauchern eingehenden Phishing-E-Mails werden nur wenige als solche identifiziert und ein Teil dieser an die Verbraucherzentrale NRW gemeldet. Die Meldungen sowie die daraus zur Verfügung gestellten Warnungen und Beispielnachrichten der Verbraucherzentrale NRW können Verbraucherinnen und Verbraucher dabei unterstützen, aktuelle Phishing-Kampagnen nachzuverfolgen oder die Legitimität von E-Mails nachzuvollziehen.

Das BSI sieht zwei Handlungsbedarfe: Zum einen müssen Menschen in ihrer Fähigkeit, Phishing-Mails zu erkennen und auf diese richtig zu reagieren, unterstützt werden. Zum anderen müssen Schutz- und Meldemaßnahmen etabliert werden, um Verbraucherinnen und Verbraucher sowie Unternehmen vor monetären Schäden oder Rufschädigung zu schützen.

In Bezug auf die „Gefahrenquelle Phishing" – dem thematischen Schwerpunkt im Berichtsjahr 2022 – konnten 2023 neue Entwicklungen verzeichnet werden. Wie sich der vermehrte Einsatz von generativer Künstlicher Intelligenz auf Phishing und private Nutzende auswirkt, beleuchtet die Jahresübersicht 2023.

Aktivitäten des BSI

Das BSI nimmt für den aktiven Schutz der Menschen in der digitalen Welt eine entscheidende Rolle ein. Als unabhängige Stelle für den Digitalen Verbraucherschutz untersucht das BSI regelmäßig einzelne Segmente des digitalen Verbrauchermarktes, wie zum Beispiel Gesundheits- und Steuererklärungs-Apps sowie Onlineshopping-Plattformen.

Die im Jahr 2023 bekannt gewordenen Schwachstellen und IT-Sicherheitsvorfälle haben das BSI dazu veranlasst, eine sicherheitstechnische Untersuchung von Passwort-Managern in die Wege zu leiten. Denn deren Nutzung ist bei korrekter Anwendung eine wesentliche Maßnahme zur Erhöhung des Accountschutzes. Auf Basis der gewonnenen Informationen und im Austausch mit den Herstellern bzw. Diensteanbietern soll dieses Marktsegment für Verbraucherinnen und Verbraucher gestärkt werden.

Alternativen zur Nutzung von Passwort-Managern sind Methoden und Anwendungen der passwortlosen Authentisierung mittels kryptografischer Schlüssel. Um die Sicherheit, Vertrauenswürdigkeit und Verbreitung der passwortlosen Authentisierung einschätzen zu können, wird das BSI eine weitere Untersuchung anschließen.

Durch den kooperativen Austausch mit den Herstellern und Dienstanbietern in den untersuchten Marktsegmenten steigert das BSI die Cybersicherheit für konkrete Produkte im Verbraucheralltag, damit sich alle online sicherer bewegen können.

3

Bessere digitale Verbraucherresilienz – aber wie?

Handlungsfelder zur Stärkung der digitalen Verbraucherresilienz

Bei rund einem Drittel aller Anfragen, die das zentrale Service-Center des BSI im Jahr 2023 aus dem Verbraucherbereich erreichten, ging es um akute IT-Sicherheitsvorfälle im privaten digitalen Alltag. Der Umgang mit und die Folgen von Phishing und Smishing, das heißt dem Abgreifen von Informationen durch gefälschte E-Mails oder SMS von vermeintlich vertrauten Unternehmen bzw. Organisationen, sowie von geleakten Daten zählten dabei zu den häufigsten Problemen. Zudem weist der aktuelle Cybersicherheitsmonitor 2023 des BSI und der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK) aus, dass mehr als ein Viertel der befragten Bürgerinnen und Bürger bereits persönlich Erfahrung mit Cyberkriminalität sammeln musste. Die weiterhin angespannte IT-Sicherheitslage auf dem digitalen Verbrauchermarkt (siehe unter anderem Kapitel 2) untermauert zudem die Notwendigkeit vielseitiger Anstrengungen, um Verbraucherinnen und Verbraucher effektiv vor den komplexen Gefahren im Netz zu schützen und ihre Widerstandsfähigkeit (Resilienz) zu stärken. Was ist zu tun?

Die folgenden Handlungsfelder umfassen drei grundlegende Dimensionen zur Stärkung der digitalen Verbraucherresilienz: die technische und anbieterorientierte Seite, die Herausforderungen der Verbraucherinnen und Verbraucher bei der sicheren und einfachen Techniknutzung sowie die Rolle der Akteure mit vermittelnder und regulierender Funktion in der Mensch-Technik-Interaktion.

Technikdimension –
technische und anbieterorientierte Sicherheit:

- Einführung aktiver, technischer Schutzmaßnahmen für eine sichere Nutzung vernetzter Produkte
- Förderung sicherer, schwachstellenfreier Produkte, die IT-Sicherheit über den gesamten Produktlebenszyklus einschließen und in ihrer Nutzung nicht überfordern (Security by Default, Usable Security)
- Etablierung von praktikablen Sicherheitsstandards in der Entwicklung digitaler Produkte und Dienste (Security by Design)
- Transparenzverpflichtung von Herstellern bzw. Anbietern in Bezug auf ihre IT- und Datensicherheitsmaßnahmen

Verbraucherdimension –
Bildung, Notfallvorsorge und Krisenmanagement:

- Förderung von Bildungs- und Schulungsprogrammen, um die Verbraucherinnen und Verbraucher über die Risiken und mögliche Sicherheitsmaßnahmen im digital vernetzten Raum zu sensibilisieren, aufzuklären und darüber zu informieren
- Unterstützung der Verbraucherinnen und Verbraucher bei der Gefahrenerkennung und beim Umgang mit IT-Sicherheitsvorfällen
- Entwicklung von geeigneten Checklisten für Verbraucherinnen und Verbraucher, die bei Cyberangriffen, Datenverlust, IT-Sicherheitsvorfällen u. a. m. praktische und einfache Hilfe leisten

Vermittlerdimension –
Kooperation und Vernetzung:

- Stärkung der Zusammenarbeit zwischen allen relevanten IT-Sicherheitsakteuren aus den Bereichen der (Zivil-)Gesellschaft, Wissenschaft, Wirtschaft sowie dem staatlich-öffentlichen Sektor
- Etablierung von Plattformen für den Wissenstransfer und den Austausch von Informationen, zum Beispiel über bewährte Verfahren oder Fallbeispiele aus dem Bereich der digitalen Verbraucherresilienz

Im Folgenden beleuchten Expertinnen und Experten die einzelnen Dimensionen zur Förderung der digitalen Verbraucherresilienz genauer.

3 Fragen zur Verbraucherdimension an …
Dr. Ayten Öksüz, Geschäftsführende Koordinatorin der bundesweiten „Marktbeobachtung der Verbraucherzentralen GbR“ und Referentin für den Bereich Digitalisierung und Datensicherheit bei der Verbraucherzentrale NRW e. V., Mitglied im Beirat Digitaler Verbraucherschutz des BSI.

3 Fragen zur Technikdimension an …
Philipp Ehmann, Referent bei eco – Verband der Internetwirtschaft e. V., Mitglied im Beirat Digitaler Verbraucherschutz des BSI.

3 Fragen zur Vermittlerdimension an …
Prof. Dr. Alexander Boden, Hochschule Bonn-Rhein-Sieg (HBRS), Institut für Verbraucherinformatik an der HBRS, Fraunhofer-Institut für Angewandte Informationstechnik (FIT).

Gastbeitrag der Verbraucherzentrale Nordrhein-Westfalen e. V.

Welche Bedürfnisse, aber auch Ängste haben die Verbraucherinnen und Verbraucher in ihrem digitalen Alltag?

Der digitale Alltag bedeutet nicht nur ein Mehr an Komfort, Effizienz und Sicherheit, sondern auch ein Mehr an Komplexität. Verbraucherinnen und Verbraucher verlieren zunehmend den Überblick darüber, welche Daten über sie erhoben und verarbeitet werden, wo ihre Nutzerprofile gespeichert sind und ob auf Basis dieser Angaben negative Auswirkungen wie Diskriminierung zu befürchten sind. Hier geht es für Nutzende darum, die Kontrolle ein Stück weit zurückzubekommen. Die Datensammelwut von Unternehmen ist nicht nur ein rein datenschutzrechtliches Problem. Sind Unternehmen von einem Datenleak betroffen, ist entscheidend, wie viele und welche Daten sich auf den betroffenen Servern befanden und abgegriffen werden konnten. Sind die Daten einmal in die Hände von Cyberkriminellen geraten, wissen Betroffene oft nicht, welche möglichen Schäden drohen und was sie dagegen tun können. In solchen Situationen brauchen Verbraucherinnen und Verbraucher die notwendigen Hilfestellungen, damit sie souverän reagieren können. Darüber hinaus möchten Nutzende aber auch schon im Vorhinein wissen, wie sie sich in einem digital vernetzten Alltag schützen können, angefangen bei der Auswahl von sicheren Produkten.

Welche Schritte wären notwendig, um die digitale Verbraucherresilienz nachhaltig zu stärken?

Digitale Verbraucherresilienz muss ganzheitlich betrachtet und als Aufgabe verstanden werden, die nicht von einer Person oder Instanz getragen werden kann. Ein wichtiger Baustein ist die Vermittlung von Digitalkompetenzen. Bildungsangebote und Anlaufstellen für Verbraucherinnen und Verbraucher, die konkrete Hilfestellungen in Form von Informationsangeboten und Beratungen zur Verfügung stellen, sind nur ein Teil des Ganzen. Wichtig ist auch die Frage, wie unterschiedliche Verbrauchergruppen erreicht, für die Problematik sensibilisiert und digitale Kompetenzen richtig vermittelt werden können.

Digitale Verbraucherresilienz bedeutet nicht nur, auf technologische Herausforderung im komplexen digitalen Alltag mit der bloßen Anwendung von Schritt-für-Schritt-Anleitungen zu reagieren, sondern es bedarf der Anpassungsfähigkeit bei Veränderungen, also des souveränen Umgangs mit dem Unbekannten. Aber auch geeignete gesetzliche Rahmenbedingungen, die Verbraucherinnen und Verbrauchern entsprechende Rechte

Dr. Ayten Öksüz

an die Hand geben, sind fundamental. Und nicht zuletzt braucht es Instanzen wie die Verbraucherzentralen, die dafür sorgen, dass Unternehmen sich an Gesetze halten und Nutzende ihre Rechte in der Praxis durchsetzen können.

Wo beginnt die Eigenverantwortung der Verbraucherinnen und Verbraucher zur Steigerung ihrer Widerstandsfähigkeit und wo endet sie?

Grundsätzlich sieht die Verbraucherzentrale NRW Unternehmen in der Pflicht, im Sinne von Security by Design und Security by Default für die Sicherheit ihrer Produkte und Dienste zu sorgen. Diese Pflicht ist auch in der EU-DSGVO verankert. Der Verordnung zufolge haben Unternehmen technische und organisatorische Maßnahmen zu ergreifen, um den Schutz personenbezogener Daten zu gewährleisten. Mit dem Cyber Resilience Act werden auf Unternehmen weitere Pflichten zukommen, was wir sehr begrüßen.

Da Datenschutz und Datensicherheit sehr vielschichtig sind, können und sollten Verbraucherinnen und Verbraucher ebenfalls entsprechende Maßnahmen vornehmen. Der erste Schritt ist die Auswahl der Produkte. Auch bei vermeintlich harmlosen Dingen wie smarten Glühbirnen sollten nicht nur Preis und Design ausschlaggebend für die Kaufentscheidung sein. Käuferinnen und Käufer sollten sich auch fragen, welche Daten für welche Zwecke gespeichert werden und wie es mit der Sicherheit der vernetzten Produkte aussieht. Selbst ein grundsätzlich sicheres System kann nicht vor Datendiebstahl schützen, wenn Sicherheitsupdates nicht installiert werden oder das gewählte Passwort einfach zu erraten ist.

Gastbeitrag des eco – Verband der Internetwirtschaft e. V.

Welchen Einfluss hat die Technikdimension auf die digitale Verbraucherresilienz?

Die Gestaltung von Technik hat enormen Einfluss auf die Fähigkeit von Verbraucherinnen und Verbrauchern, selbstbestimmt Sicherheit für ihre Geräte herzustellen. Die Herausforderung besteht darin, dass ein angemessener Ausgleich zwischen Zugänglichkeit der Technologie auf der einen Seite und individueller Anpassbarkeit auf der anderen Seite hergestellt wird – so wie bei jeder anderen Technologie auch. Die besondere Komplexität der Informationstechnologie besteht darin, dass sie in verschiedenen Kontexten und Szenarien zum Einsatz kommt, in denen unterschiedliche Risiken, Angriffsvektoren und Probleme relevant sind. Da oftmals der Wissensstand der Verbraucherinnen und Verbraucher hinter den aktuellen Entwicklungen zurückbleibt, entsteht das Gefühl der Überforderung.

Philipp Ehmann

Welche nationalen bzw. internationalen Entwicklungen bezüglich IT-sicherer und zugleich verbraucherfreundlicher Produkte gibt es?

Auf nationaler Ebene sind derzeit vor allem operative Maßnahmen im B2B-Kontext erkennbar. Schulungen, Trainings und Lernangebote für Mitarbeitende werden vor allem von der (Internet-)Wirtschaft betrieben, da diese ein genuines Interesse an der Fortsetzung ihrer Geschäftstätigkeit hat. Hier bleibt zu hoffen, dass die von den Mitarbeitenden gewonnenen Erkenntnisse auch privat Anwendung finden. Bedauerlicherweise sind sonstige zivilgesellschaftliche Initiativen sehr selten. Auf internationaler Ebene werden die Trends – soweit sich dies überblicken lässt – überwiegend in den USA gesetzt, wo die Standardsoftware und die am meisten verbreiteten Betriebssysteme entwickelt werden. Dort sind klare Schritte zur Verbesserung der Systeme, beispielsweise durch Zwei-Faktor-Authentifizierung, erkennbar.

Wo sehen Sie die größten Barrieren für die digitale Verbraucherresilienz?

Die größten Probleme im Bereich der digitalen Resilienz sind mangelndes Interesse und Sorgfalt beim Umgang mit digitalen Technologien. Ein versehentlich falsch angeklickter Link eines Mitarbeitenden kann ein ganzes Unternehmen lahmlegen. Es sollte verstärkt daran gearbeitet werden, Kausalitäten, Einfallstore und Sicherungsmaßnahmen aufzuzeigen. Nur wenn Nutzerinnen und Nutzer verstehen, dass auch sie selbst von den von ihnen ergriffenen Maßnahmen profitieren, kann digitale Resilienz gelingen.

Gastbeitrag der Hochschule Bonn-Rhein-Sieg

Wie lässt sich die Vermittlerdimension bzw. die Schnittmenge zwischen Technik- und Verbraucherperspektive charakterisieren und welche Handlungsfelder können daraus abgeleitet werden?

Aus Sicht der Verbraucherinnen und Verbraucher ist Technik sowohl Teil des Problems als auch Teil der Lösung. Einerseits ist es stressig, wenn man sich um Updates kümmern muss. Andererseits ist es notwendig für die IT-Sicherheit. Daher brauchen wir gut gestaltete Produkte, die Sicherheit einfacher machen und das Problem nicht auf die Nutzenden abwälzen. Wir brauchen aber auch eine erweiterte Sicht auf Technik, die die gesellschaftlichen Auswirkungen berücksichtigt. Hier kann man von der Krisenforschung lernen, die Resilienz nicht nur als Robustheit von technischen Systemen versteht, sondern auch deren Auswirkungen auf unsere sozialen Systeme mitdenkt. In New Orleans gab es nach dem Hurricane Katrina eine Bewegung gegen die Idee gesteigerter Resilienz, da das auch Schutzmaßnahmen delegitimieren kann. Die Stärkung der Abwehrkräfte der Bürgerinnen und Bürger darf nicht dazu führen, dass Hersteller nur das Minimum an Sicherheit umsetzen. Eine umfassende digitale Verbraucherschutzstrategie braucht beides: die Förderung der Sicherheitskompetenzen seitens der Nutzenden und die Umsetzung einfacher Sicherheit seitens der Hersteller.

Lässt sich die Steigerung der digitalen Verbraucherresilienz für die Entwicklung zielführender Maßnahmen überhaupt messen?

Wir können für Resilienz sicher Kennzahlen finden, etwa die Anzahl von Sicherheitsvorfällen, die Höhe des finanziellen und psychischen Schadens etc. Es müssen aber auch die vielen Interdependenzen und die ständigen Veränderungen der technischen und gesellschaftlichen Rahmenbedingungen berücksichtigt werden. Deshalb sollte man allzu einfache Kennzahlen, die die Resilienz der oder des Einzelnen bzw. der Gesellschaft im Ganzen auf einzelne Verbraucherschutz-Maßnahmen zurückführen wollen, mit Vorsicht betrachten. Im sozialen Raum herrschen keine Laborbedingungen. Das ist ein bisschen so wie bei anderen gesellschaftlichen Herausforderungen, etwa Bildung, Klima etc. Wir wissen, dass wir da alle möglichen Probleme haben, aber es ist schwer, daraus effektive Maßnahmen abzuleiten. Daher wäre wichtig, das Konzept der digitalen Verbraucherresilienz theoretisch stärker zu fundieren, empirisch zu erforschen und hierbei auch die Zielkonflikte zu berücksichtigen. Dabei werden wir vermutlich qualitative und quantitative Methoden kombinieren müssen, um ein umfassendes Lagebild zu erhalten.

Prof. Dr. Alexander Boden

Wie sollten onlinefähige Geräte und Anwendungen in Bezug auf eine IT-sichere Nutzung im Verbraucheralltag gestaltet sein?

Im Prinzip bedeutet resilienz-orientiertes Design, eine integrierte Sicht auf Prävention und Reaktion einzunehmen. Gute Produkte müssen zunächst, lapidar gesagt, sicher gestaltet werden, also so, dass möglichst keine Schwachstellen vorhanden sind. Ferner müssen Sicherheitsmechanismen alltagstauglich sein. IT-Sicherheit ist im Alltag der Menschen nur eine von vielen Aufgaben und Zielen, zumal wir gerade in Zeiten einer Polykrise leben. Wir dürfen die Menschen nicht überfordern, sondern müssen Usable Security bzw. Security by Design fördern. Wir müssen darüber hinaus Verbraucherinnen und Verbraucher dabei unterstützen, Gefahren einzuschätzen und mit Sicherheitsvorfällen umgehen zu können. Dabei dürfen wir nicht nur auf die einzelnen Nutzenden schauen, sondern müssen auch das soziale Umfeld berücksichtigen, also die Umgebung, in der IT-Sicherheit stattfinden soll. Resilienz heißt, in Netzwerken und Sicherheitsallianzen zu denken. Hier gibt es noch viel Potenzial. So muss erforscht werden, wie man Verbraucherinnen und Verbraucher nicht nur verständlich informiert, sondern auch ihr Handeln praktisch unterstützen kann, ohne mit Warnungen und Sicherheitshinweisen zu überfordern.

Exkurs zur digitalen Verbraucherresilienz: IT-Sicherheit ganzheitlich denken

Der folgende Abschnitt vertieft wissenschaftlich-analytisch das thematische Spektrum der digitalen Verbraucherresilienz und untermauert damit die zu Beginn des Kapitels aufgeführten Handlungsfelder.

Die digitale Verbraucherresilienz stellt das kritische Ereignis in den Fokus. Dementsprechend wird die Zeit vor, während und nach einem IT-Sicherheitsvorfall betrachtet. Abbildung 2 stellt einen exemplarischen Ablauf dar und verdeutlicht zugleich die Komplexität. So bedarf die Thematik eines ganzheitlichen Blickwinkels, um die Wahrscheinlichkeit von Angriffen zu reduzieren **(Prävention)**, Unregelmäßigkeiten und Vorfälle selbst zu erkennen **(Detektion)** sowie Angriffsversuche abzuwehren oder den Alltagsbetrieb im Schadensfall wiederherzustellen **(Reaktion)**.

Wie in den Handlungsfeldern bereits skizziert: Maßnahmen zur Förderung der Resilienz zielen auf die Berücksichtigung der Handlungsparameter der Nutzerinnen und Nutzer **(Verbraucherdimension)** sowie auf die Gestaltung der Technik **(Technikdimension)** ab. Durch Intermediäre werden bestehende Resilienzaspekte, zu denen die Robustheit von technischen Systemen gehört (vgl. Die Lage der IT-Sicherheit in Deutschland 2022, S. 110), um soziologische und psychologische Perspektiven der Verbraucherresilienz erweitert und miteinander verknüpft **(Vermittlerdimension)**. Dies entspricht neueren wissenschaftlichen Ansätzen innerhalb der Cyber-Resilienz-Diskussion, die den Aspekt des menschlichen Handelns in der Mensch-Maschine-Interaktion als entscheidenden Baustein für ein Plus an Cybersicherheit berücksichtigt (Joinson et al. 2023).

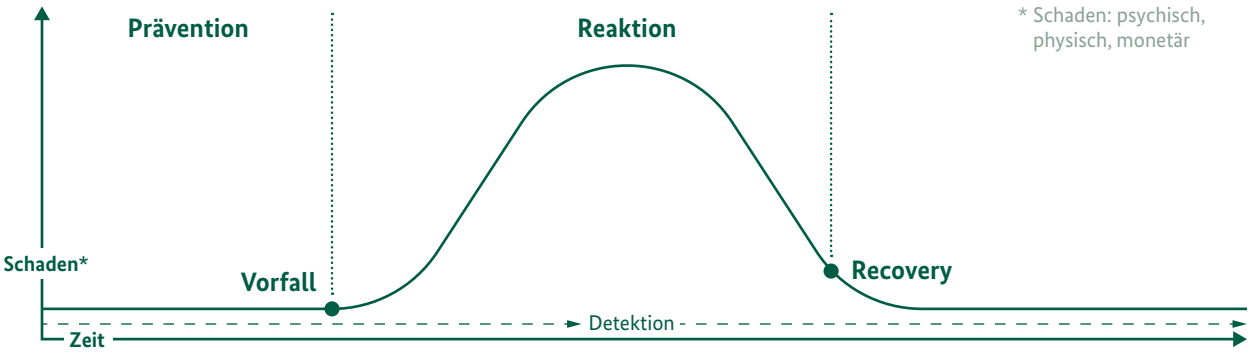


Abbildung 2: Exemplarischer Ablauf eines IT-Sicherheitsvorfalls

a) Die Verbraucherdimension – Umdenken und lebenslanges Lernen

Den IT-Sicherheitsvorfall im eigenen, privaten Bereich als wahrscheinliches Ereignis zu betrachten, erfordert auch ein Umdenken bei den Verbraucherinnen und Verbrauchern. Die Frage ist nicht, „ob", sondern „wann" ein IT-Sicherheitsvorfall eintritt. Folglich sind präventive Maßnahmen – wie beispielsweise das regelmäßige, verfügbare und sichere Back-up – zum Schutz vor IT-Sicherheitsrisiken unerlässlich, da diese im Falle einer Krise helfen können.

Gleichwohl gewinnen Detektion und Reaktion an Bedeutung. Technisch-organisatorische Maßnahmen lassen sich aktuell nur bedingt auf die digitale Verbraucherresilienz beziehen. Joinson et al. legen dabei vier Kernelemente für die Verbraucherdimension zugrunde:

1. **Self-Efficacy (Selbstwirksamkeitserwartung):** Damit verbunden ist die Überzeugung, dass die eigenen Handlungen eine Wirkung entfalten. Nur wer sich kompetent fühlt, um zum Beispiel ein Back-up für die Wiederherstellung wichtiger Dokumente oder wertvoller Erinnerungen zu erstellen, wird dies auch umsetzen.

2. **Lernen und Wachsen:** So erfordert die digital vernetzte Welt die Bereitschaft zum lebenslangen Lernen. Die digitale Verbraucherresilienz ermutigt Nutzerinnen und Nutzer, Herausforderungen sowie kritische Ereignisse als Chance zu begreifen und sich neue Kompetenzen anzueignen. Wer früher für Back-ups physische Datenträger wie DVDs nutzte, muss sich heute angesichts fehlender physischer Laufwerke und steigender Datenmengen über sichere Alternativen informieren und diverse Kriterien (Kosten für NAS-System vs. Komfort der Cloudlösung) gegeneinander abwägen.

3. **Soziale Unterstützung:** Nicht alle Nutzenden verfügen über die erforderlichen Basiskompetenzen, um kritische IT-Vorfälle zu meistern. Der Zugriff auf entsprechende Kontakte im persönlichen Umfeld ist ein zentraler Baustein, um die Handlungsfähigkeit auch in Krisenzeiten zu erhalten.

4. **Hilflosigkeit:** Das Gefühl der Hilflosigkeit hat einen negativen Einfluss auf die Widerstandsfähigkeit von Nutzerinnen und Nutzern. Sie äußert sich als eine Art Überforderung. Das Fehlen von Kompetenz und die Abwesenheit eines unterstützenden Netzwerks kann dazu führen, dass Menschen den „Kopf in den Sand stecken" und zum Beispiel die Bedeutung eines Back-ups herunterspielen oder das Risiko eines Datenverlustes verdrängen.

Die vier Kernelemente der Verbraucherdimensionen machen eines deutlich: Neben der Förderung des lebenslangen Lernens oder dem Aufzeigen von Handlungsmöglichkeiten im Krisenfall bedarf es effektiver wie auch aktiver Schutzmaßnahmen auf technischer Seite, um der Hilflosigkeit und dem Gefühl der Überforderung entgegenzuwirken und um IT-Sicherheit alltagstauglich zu gestalten.

b) Die Technikdimension – Resilienz als Prozess

IT-Sicherheit bei der Produktentwicklung von Anfang an mitzudenken (Security by Design) und eine einfache, intuitive Umsetzung von IT-Sicherheitsaspekten im täglichen Betrieb zu ermöglichen (Usable Security), gehört zu den grundlegenden Voraussetzungen in puncto digitaler Verbraucherresilienz. Zudem gewinnt die IT-Sicherheit bei der Kaufentscheidung zunehmend an Bedeutung. Dies bezieht sich sowohl auf die Produkte selbst wie auch auf Anwendungsfelder für einen sicheren digitalen Alltag, der immer noch zahlreiche Barrieren von Seiten der

technischen Lösungen mit sich bringt, wie die nachfolgenden Beispiele zeigen.

Verschlüsselte Kommunikation gewährleistet Vertraulichkeit im digitalen Raum. Aber welche technische Lösung zur verschlüsselten Kommunikation ist überhaupt bekannt und zudem einfach wie auch sicher nutzbar?

Back-ups schützen vor Datenverlust. Aber wie erstelle ich einfach und bestenfalls automatisiert ein sicheres Daten-Update? Wie empfehlenswert ist eine Cloud-Lösung? Fragen, an denen viele Menschen scheitern: Wie der eco – Verband der Internetwirtschaft e. V. in zwei 2023 veröffentlichten Studien zeigt, stieg die Anzahl derer, die nie ein Back-up machen, innerhalb der letzten vier Jahre von 10,6 auf 15,7 % (vgl. eco Presse a). Die einfache Möglichkeit des Back-ups in der Cloud wird von gerade einmal 22,5 % der Befragten genutzt (vgl. eco Presse b).

Antischadsoftware kann eine wirksame Maßnahme sein, um besser auf Bedrohungen zu reagieren. Darüber hinaus fördert sie die Entwicklung eigener Kompetenzen beim Erkennen schädlicher Programme und ihrer Bestandteile. Doch Publikationen wie Körber et al. (2022) zeigen, dass sich die Nutzerinnen und Nutzer von den Pop-up-Meldungen der Software mehr verunsichert als unterstützt fühlen.

Diese Aspekte veranschaulichen, dass zum Beispiel die Usable Security bei der Steigerung der digitalen Verbraucherresilienz eine wichtige Rolle spielen sollte. Das Fundament von Usable Security sind jedoch deutlich sicherere Produkte, die weniger Anpassungen bzw. Eingriffe der Nutzenden erforderlich machen würden. Hinzu kommt: Wo sich Sicherheitsmaßnahmen nicht reibungslos in den Verbraucheralltag einfügen, werden sie nicht angewendet. Der rasante technische Wandel ist eine zusätzliche Herausforderung und sorgt mehr denn je dafür, dass Maßnahmen zur Förderung der digitalen Verbraucherresilienz für die technische Seite einen Prozess und keinen Zustand darstellen. Geräte und Dienste müssen sich über ihre gesamte Lebensspanne hinweg durch entsprechende Sicherheitsupdates anpassen. Die aufgeführten Beispiele verdeutlichen zudem das Spannungsfeld zwischen den derzeitigen technischen Lösungen auf der einen und dem Wissen, Denken und Handeln der Verbraucherinnen und Verbraucher auf der anderen Seite.

c) Die Vermittlerdimension – gemeinsam mehr erreichen

Um die zum Teil konträren Technik- und Verbraucherperspektiven zusammenzubringen, bedarf es der Mittler (Intermediäre). Dazu gehören etwa technisch versierte Personen aus dem Freundeskreis, die ein gutes Verständnis für die Fähigkeiten und Bedürfnisse des Einzelnen mitbringen. Aber auch Forschende, die die IT-Sicherheit und/oder das Verbraucherverhalten wissenschaftlich untersuchen, zählen zu den Mittlern. Dazu kommen Interessengruppen, die sich gezielt für die Anforderungen spezifischer Bedarfsträger an die Technikgestaltung stark machen.

IT-Sicherheitsexperten, die Gefahren analysieren und für die Verbraucherinnen und Verbraucher geeignete technische und bildungsbezogene Maßnahmen entwickeln, spielen eine herausragende Rolle — die es in puncto Kompetenzen und Befugnisse zu stärken gilt. Sie helfen dabei, Präventionsmaßnahmen gemäß den jeweiligen Schutzzielen zu priorisieren und abzusichern. Sie detektieren neue Gefahren bzw. Bedrohungsszenarien und informieren darüber. Sie stehen als Ansprechpersonen bei Krisen zur Verfügung und unterstützen Erste-Hilfe-Maßnahmen. Sie kommunizieren Umsetzungsbarrieren an Hersteller und helfen durch die Zusammenarbeit mit unterschiedlichen Interessengruppen, passgenaue Lösungen für die Bedürfnisse der Nutzenden zu entwickeln.

Mit Blick auf die aktuelle Gefahrenlage ist nicht hinnehmbar: Häufig stellt die IT-Sicherheit weder für die Nutzerinnen und Nutzer noch für die Technikentwicklung ein primäres Handlungsziel dar. Ausgenommen sind die Hersteller von Anwendungen zur Steigerung der IT-Sicherheit wie Virenschutz-Programmen oder Passwortmanagern. In der Regel steht jedoch die Funktionalität und die Problemlösungskapazität im Vordergrund. Intermediäre bewerben die IT-Sicherheit auf beiden Seiten, vermitteln zwischen den Anforderungen der IT-Sicherheit und den Anwendungsbedürfnissen, prüfen die rechtlichen Rahmenbedingungen und zeigen soziostrukturelle Barrieren auf. Die dargestellten Bausteine „Self-Efficacy“, „Lernen und Wachsen“ sowie „Soziale Unterstützung“ zeigen, dass sich digitale Verbraucherresilienz nicht nur situativ in der Mensch-Maschine-Aktion erschöpft. Es muss Möglichkeiten zur positiven Selbsterfahrung geben. Aufgabe der Vermittler ist es, diese Möglichkeiten zu schaffen, sei es durch das Nacherleben der Erfolgsstorys anderer, die Teilnahme an Lernräumen oder die konkrete Unterstützung im Krisenfall.

Wichtige und grundlegende Voraussetzung für eine Stärkung der digitalen Verbraucherresilienz sind jedoch Produkte, die mit dem Kauf von Anfang an sicher im Onlinebetrieb nutzbar sind – über die gesamte Lebensdauer hinweg. Dazu zählen auch aktive Schutzmaßnahmen, die Angriffe von vornherein verhindern oder so früh erkennen, dass keine Schäden für die Nutzenden entstehen können.

4

Cybersicherheit für Unternehmen und Institutionen nützt allen

Jedes Unternehmen trägt Verantwortung gegenüber Verbraucherinnen und Verbrauchern. Diese Verantwortung besteht im vertrauensvollen und sicheren Umgang mit Kundendaten und in der wichtigen Aufgabe, IT-Sicherheit von Anfang an in die Produktentwicklung zu integrieren. Dieses Prinzip von Security by Design ist essenziell, um Nutzende vor vermeidbaren Ausnutzungen von Schwachstellen in den Produkten zu schützen. Mit der Allianz für Cyber-Sicherheit (ACS) unterstützt das Bundesamt für Sicherheit in der Informationstechnik Unternehmen und Institutionen, die sich cybersicher aufstellen wollen, durch ein starkes Netzwerk.

Die Allianz für Cyber-Sicherheit – Stärkung der Resilienz in Unternehmen

Die Allianz für Cyber-Sicherheit ist eine öffentlich-private Partnerschaft zwischen dem BSI und der Privatwirtschaft. Gemeinsam mit dem Branchenverband Bitkom im Jahr 2012 gegründet, verfolgt die ACS seit mehr als zehn Jahren die Mission, die IT-Sicherheit der deutschen Wirtschaft auszubauen und ihre Resilienz im Kampf gegen Cyberangriffe zu stärken.

Die ACS hilft Unternehmen, beispielsweise durch ihr breites Informationsangebot, Systeme und somit auch Kundendaten sowie Produkte besser abzusichern. Institutionen und Unternehmen können so effektiver präventiv agieren. Sie erhalten außerdem wertvolle Hilfestellungen, um im Falle eines Sicherheitsvorfalles ein sinnvolles Notfallmanagement zu betreiben.

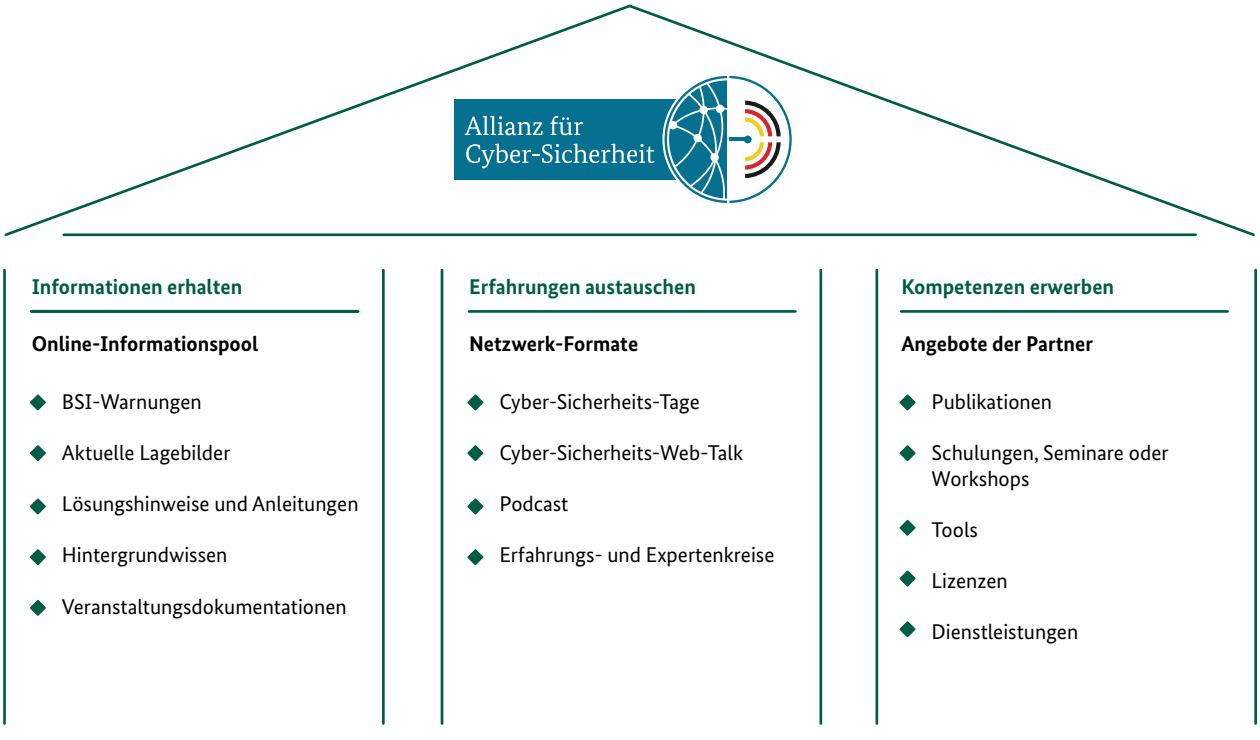


Abbildung 3: Die drei Säulen der Allianz für Cyber-Sicherheit

Geballte Cybersicherheit unter dem Dach der ACS

Teilnehmende profitieren vom Wissen des Netzwerks und dem vertrauensvollen Erfahrungsaustausch. Im Jahr 2023 gehören rund 7.500 Mitglieder der deutschlandweiten Initiative an.

Auf zahlreichen Kommunikationskanälen, wie der Website, dem Newsletter, den Social-Media-Kanälen oder dem Podcast CYBERSNACS, werden Teilnehmerinnen und Teilnehmer über aktuelle Themen informiert und erhalten Handreichungen und Cybersicherheitsempfehlungen.

Unternehmen haben außerdem Zugang zu einem Online-Informationspool mit BSI-Warnungen, monatlichen Lagebildern und Hintergrundwissen zum Thema Cybersicherheit im Mitgliederbereich der Website.

Um das Netzwerk zu stärken und Wissen sowie Best Practices zu teilen, besteht außerdem die Möglichkeit, Partnerbeiträge für andere Teilnehmerinnen und Teilnehmer kostenlos anzubieten und sich damit für den Status als Partner der ACS zu qualifizieren. Durch die zahlreichen Partnerangebote können die Mitglieder der ACS neue Cybersicherheitskompetenzen erwerben und vorhandenes Wissen ausbauen. Das ist ein wichtiger Hebel, um langfristig die Sicherheit in den Firmen zu erhöhen, die entwickelten Produkte zu verbessern, und einen Beitrag zu leisten, den Digitalen Verbraucherschutz voranzubringen.

Die Bandbreite der Partnerbeiträge erstreckt sich von Publikationen, Schulungen, Lizenzen und Dienstleistungen wie kostenfreien Schwachstellenanalysen bis zu umfassenden Penetrationstests oder der individuellen Planung einer Sicherheitsarchitektur.

Institutionen wie beispielsweise Verbände, Kammern und Vereine, Initiativen, Netzwerke oder Medienpartner, die sich besonders engagieren möchten, können sich durch ihren öffentlichkeitswirksamen Einsatz für die ACS als sogenannte Multiplikatoren qualifizieren.

Zum zehnjährigen Jubiläum hat die ACS ihr Leitbild formuliert: „Unsere Vision ist es, Cybersicherheit auf die Straße zu bringen. Durch mehr Thought Leadership und zielgerichtete Hilfe zur Selbsthilfe wollen wir unsere Wirkungsmöglichkeiten verstärken – in Deutschland und international."

So profitieren auch Verbraucherinnen und Verbraucher seit mehr als zehn Jahren effektiv von dem Engagement der Unternehmen in der Allianz für Cyber-Sicherheit.

Weitere Informationen über die Allianz für Cyber-Sicherheit:

Teilnehmer werden:

Zum Cyber-Sicherheits-Web-Talk:

Über das zehnjährige Jubiläum des ACS:

5

Wissen, wo ich Hilfe finde – BSI-Angebote für Verbraucherinnen und Verbraucher

Hilfe für den digitalen Alltag – BSI-Angebote für Verbraucherinnen und Verbraucher

Das BSI verfolgt das Ziel, die Widerstandsfähigkeit der Verbraucherinnen und Verbraucher im Falle einer Cybergefahr zu stärken. Es geht aber nicht darum, den Menschen immer mehr Verantwortung für ihre digitale Sicherheit zu übertragen. Stattdessen zielt das BSI darauf ab, ihnen maßgeschneiderte Hilfestellungen anzubieten, sodass sie den größtmöglichen Nutzen entfalten.

Gibt man die Frage „Wie sieht ein sicheres Passwort aus?“ in eine Suchmaschine ein, erhält man Dutzende von Empfehlungen und Ratschlägen von diversen Akteuren. Das kann schnell überfordern. Verbraucher und Verbraucherinnen stehen vor Fragen wie „Was ist wichtig?“ und „Wie kann ich das in meinen Alltag integrieren?“. Ganz oben in der Ergebnisliste ist der Link zur BSI-Webseite zu finden. Dort wird das Thema mit Videos, Checklisten und Grafiken aufbereitet. Den Lesern und Leserinnen werden mehrere Strategien vorgestellt, wie sie mit den Passwörtern umgehen können – sodass jede und jeder einen individuellen Weg für den digitalen Alltag finden kann. Das ist nur ein Beispiel für das breite Spektrum unterschiedlicher Medienformate, auf die das BSI setzt. Laut Cybersicherheitsmonitor (CyMon) 2023, einer Befragung von BSI und ProPK zu den Einstellungen, Erfahrungen, Kenntnissen und Wünschen der Verbraucher und Verbraucherinnen rund um das Thema Cybersicherheit, benötigt gut ein Drittel der Menschen Schritt-für-Schritt-Anleitungen zur schnellen und einfachen Einrichtung wichtiger Sicherheitseinstellungen. Entsprechend zeigen die neuen Anleitungen des BSI in Print und online beispielsweise, wie ein Gäste-WLAN eingerichtet, wie Backups aktiviert oder wie automatische Updates eingestellt werden – und das ganz konkret für alle gängigen Systeme.

Etwa jeder und jede Vierte informiert sich laut CyMon in Form von Videos oder Podcasts über Cybersicherheit. Darum klärt das BSI unter anderem mithilfe animierter Erklärvideos, eines Talk-Formats zwischen zwei Experten oder des Podcasts „Update verfügbar“ über Themen der digitalen Sicherheit auf. In den Sozialen Medien, die ebenfalls jedem und jeder Vierten als Informationsquelle dienen, zeigt das BSI Gesicht: So besprechen BSI-Influencer, beispielsweise bei Instagram, in kurzen Clips alltägliche Probleme und unterhaltsame Fakten, um die Verbraucherinnen und Verbraucher zu ermutigen, die Vorteile der Digitalisierung auszuschöpfen. Alles alltagsnah und direkt umsetzbar.

Zur Gamescom 2023 wurde das abstrakte Thema Cybersicherheit für viele Menschen erlebbar gemacht: Mit eigenem VR-Spiel, einer Deepfake-Demonstration und zahlreichen Onlineformaten stand der Digitale Verbraucherschutz des BSI 2023 Rede und Antwort. In hunderten Gesprächen berieten die BSI-Mitarbeitenden die Menschen bei ihren Anliegen und halfen ihnen, sich vor Cybergefahren zu schützen. Begleitend dazu wurden komplizierte technische Themen wie Accountschutz und Künstliche Intelligenz unterhaltsam und zielgruppengerecht in Szene gesetzt, sodass sie über 2,3 Mio. Mal online abgerufen wurden.

Doch Resilienz bedeutet nicht nur, sich präventiv abzusichern. Laut CyMon war jede und jeder Vierte von einem Cybervorfall betroffen. Hierfür gibt das BSI Orientierung, was zu tun ist. Allen voran helfen die „Checklisten für den Ernstfall“ weiter, die das BSI gemeinsam mit der Polizeilichen Kriminalprävention erarbeitet hat. Das Service-Center des BSI gibt zudem telefonisch oder per E-Mail grundlegende Empfehlungen zur Bewältigung des Vorfalls. Damit können auch Betroffene darauf bauen, schnelle und wirksame Hilfe zu erhalten.

Mit diesen Informationsangeboten kann das BSI Verbraucherinnen und Verbraucher begleiten, ihnen Leitplanken bieten und erste Hilfe leisten. Doch hier darf der Digitale Verbraucherschutz nicht enden. Denn laut CyMon informiert sich ein Großteil der Menschen (43 %) nur hin und wieder über Cybersicherheit. Zudem ist es unzumutbar, den Anwenderinnen und Anwendern die alleinige Verantwortung zur Umsetzung wichtiger Schutzmaßnahmen zu übertragen, sodass es zukünftig unbedingt mehr technische Mechanismen braucht, um Schäden und Cyberangriffe bereits in ihrer Entstehung zu unterbinden. Dafür bewegt das BSI schon heute die Hersteller und Betreiber vernetzter Dienste dazu, Sicherheit von Anfang an in ihre Produkte zu implementieren, Updates regelmäßig zur Verfügung zu stellen oder einfache Passwörter wie 123456 gar nicht erst zu erlauben, denn Sicherheit muss einfach und alltagstauglich sein. Gleichzeitig setzt sich der Digitale Verbraucherschutz für Regularien ein, die IT-Produkte bereits beim Kauf für Nutzende transparenter machen und Hersteller stärker in die Pflicht nehmen.

Podcast:

Schritt-für-Schritt-Anleitungen:

BSI-Instagram:

Newsletter „Sicher informiert“:

6

Literaturverzeichnis/ Quellen

Bleepingcomputer (2023a):
NortonLifeLock warns that hackers breached Password Manager accounts.
Einzusehen unter:
https://www.bleepingcomputer.com/news/security/nortonlifelock-warns-that-hackers-breached-password-manager-accounts/,
zuletzt eingesehen am 16.11.2023

Bleepingcomputer (2023b):
Bitwarden password vaults targeted in Google ads phishing attack.
Einzusehen unter:
https://www.bleepingcomputer.com/news/security/bitwarden-password-vaults-targeted-in-google-ads-phishing-attack/,
zuletzt eingesehen am 16.11.2023

Bleepingcomputer (2023c):
LastPass breach linked to theft of $4.4 million in crypto.
Einzusehen unter:
https://www.bleepingcomputer.com/news/security/lastpass-breach-linked-to-theft-of-44-million-in-crypto/,
zuletzt eingesehen am 16.11.2023

BSI (2023):
Die Lage der IT-Sicherheit in Deutschland 2023.
Einzusehen unter:
https://www.bsi.bund.de/lagebericht,
zuletzt eingesehen am 20.11.2023

BSI (2024):
Cyber-Sicherheitswarnungen.
Einzusehen unter:
https://www.bsi.bund.de/dok/14803002,
zuletzt eingesehen am 23.01.2024

Bundeskanzleramt (2020):
Zwischenbericht – Schutz von Online-Konten.
Einzusehen unter:
https://www.bundesregierung.de/resource/blob/975272/1732446/a5bc4cd658458e-ofedd943d8e9544882/de-passwort-download-zwischenbericht-data.pdf?download=1,
zuletzt eingesehen am 16.11.2023

Bundeskriminalamt (2023):
Polizeiliche Kriminalstatistik.
Einzusehen unter:
https://www.bka.de/DE/AktuelleInformationen/Statistiken-Lagebilder/PolizeilicheKriminalstatistik/pks_node.html,
zuletzt eingesehen am 22.12.2023

Bundesverband Frauenberatungsstellen und Frauennotrufe (bff, 2021):
Geschlechtsspezifische Gewalt in Zeiten der Digitalisierung.
Einzusehen unter:
https://www.transcript-verlag.de/shopMedia/openaccess/pdf/oa9783839452813.pdf,
zuletzt eingesehen am 22.12.2023

CSO (2023):
Hacker greifen auf E-Mail-Konten der Uni Düsseldorf zu.
Einzusehen unter:
https://www.csoonline.com/de/a/hacker-greifen-auf-e-mail-konten-der-uni-duesseldorf-zu,3681029,
zuletzt eingesehen am 09.11.2023

CyMon – Der Cybersicherheitsmonitor.
Einzusehen unter:
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Leistungen-und-Kooperationen/Digitaler-Verbraucherschutz/Digitalbarometer/digitalbarometer_node.html,
zuletzt eingesehen am 18.01.2024

DSGVO-Portal (2023):
Details zum Sicherheitsvorfall - TU Ilmenau.
Einzusehen unter:
https://www.dsgvo-portal.de/sicherheitsvorfaelle/sicherheitsvorfall-tu-ilmenau-DE-1910.php,
zuletzt eingesehen am 09.11.2023

DsiN (2023):
Sicherer Login und Passwörter: Online-Konten schützen.
Einzusehen unter:
https://www.sicher-im-netz.de/sicherer-login-online-konten-sch%C3%BCtzen,
zuletzt eingesehen am 16.11.2023

eco Presse a:
eco Umfrage: Deutsche bleiben Backup-Muffel.
Einzusehen unter:
https://www.eco.de/presse/eco-umfrage-deutsche-bleiben-backup-muffel/,
zuletzt eingesehen am 6.12.2023

eco Presse b:
Nur 22,5 Prozent der Deutschen nutzen Cloud-Services, um private Medien zu sichern.
Einzusehen unter:
https://www.eco.de/presse/nur-225-prozent-der-deutschen-nutzen-cloud-services-um-private-medien-zu-sichern/,
zuletzt eingesehen am 6.12.2023

Golem (2023):
Lastpass teilt weitere Details zum Dezember-Hack mit.
Einzusehen unter:
https://www.golem.de/news/passwortmanager-lastpass-teilt-weitere-details-zum-dezember-hack-mit-2302-172255.html,
zuletzt eingesehen am 16.11.2023

Hochschule Kaiserslautern (2023):
Cyberangriff: Aktuelle Meldungen und Hinweise.
Einzusehen unter:
https://www.hs-kl.de/hochschule/aktuelles/cyberangriff/aktuelle-meldungen-und-hinweise,
zuletzt eingesehen am 23.01.2024

HPI (2023):
Statistiken – Die häufigsten Kennwörter aus allen erfassten Leaks.
Einzusehen unter:
https://sec.hpi.de/ilc/statistics?lang=de,
zuletzt eingesehen am 16.11.2023

Joinson et al. (2023):
Adam N. Joinson, Matt Dixon, Lynne Coventry and Pam Briggs: Development of a new „human cyber-resilience scale“, Journal of Cybersecurity, 2023, 1 – 10.

Körber et al. (2022):
Körber, M., Kalysch, A., Massonne, W., & Benenson, Z. (2022). Usability of Antivirus Tools in a Threat Detection Scenario. In Weizhi Meng, Simone Fischer-Hübner, Christian D. Jensen (Eds.), IFIP Advances in Information and Communication Technology (pp. 306-322). Copenhagen, DNK: Springer Science and Business Media Deutschland GmbH

KonBriefing (2023a):
Cyberangriffe auf Universitäten.
Einzusehen unter:
https://konbriefing.com/de-topics/cyber-angriffe-universitaeten.html,
zuletzt eingesehen am 06.11.2023

KonBriefing (2023b):
MOVEit: Betroffene Unternehmen.
Einzusehen unter:
https://konbriefing.com/de-topics/cyberangriffe-moveit-betroffene-unternehmen.html,
zuletzt eingesehen am 18.12.2023

SIT (2023)
Südwestfalen-IT.
Einzusehen unter:
https://notfallseite.sit.nrw/,
zuletzt eingesehen am: 12.02.2024

Verivox (2023):
Ausführliche Kundeninformation: Datenschutzinformation gemäß Art. 34 DSGVO (Stand 16.06.2023).
Einzusehen unter:
https://www.verivox.de/company/datenschutz/kundeninformation-moveit,
zuletzt eingesehen am 23.01.2024

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 2024

Druck
Appel & Klinger Druck und Medien GmbH, Schneckenlohe

Gestaltung
KOMPAKTMEDIEN Agentur für Kommunikation GmbH, Berlin

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

Bildnachweis
Titel: AdobeStock © NDABCREATIVITY
S. 3: BMI © Henning Schacht
S. 5: AdobeStock © mdyn
S. 6, 7: © BSI, Sächsische Staatskanzlei, Bundesfoto
S. 10: AdobeStock © Seventyfour
S. 11: AdobeStock © PintoArt
S. 12: AdobeStock © VITTA GALLERY/Westend61
S. 13: AdobeStock © Missleestocker
S. 16: © Verbraucherzentrale NRW e. V.
S. 17: © Laurin Schmid
S. 18: © HBRS
S. 19: AdobeStock © zeljkomatic76
S. 20: AdobeStock © Mnica
S. 24/25: AdobeStock © BullRun

Artikelnummer
BSI-DVS24/001

www.bsi.bund.de