Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Bericht zum Digitalen Verbraucherschutz 2021

Sicher im
digitalen Alltag

2021 im Überblick

Januar

Kooperation: Bundeskartellamt/BSI

Unterzeichnung einer Absichtserklärung (MoU-Memorandum of Understanding) zwischen dem BSI und dem Bundeskartellamt zur Zusammenarbeit beim Digitalen Verbraucherschutz

Mai

Bürgerbroschüren

Redesign von kompakten Praxistipps unter dem Titel „Wegweiser für den digitalen Alltag“

März

Studie IT-Sicherheit auf dem digitalen Verbrauchermarkt

Veröffentlichung einer Studie zur IT-Sicherheit auf dem digitalen Verbrauchermarkt mit dem Fokus „Gesundheits-Apps“

Kampagnenstart

Start der bundesweiten Kampagne zur Information und Sensibilisierung der Bevölkerung in der IT-Sicherheit unter dem Motto: #einfachaBSIchern

Juni

Beirat Digitaler Verbraucherschutz

Konstituierende Sitzung des Beirats Digitaler Verbraucherschutz

Bericht zum Digitalen Verbraucherschutz

Veröffentlichung des 1. Berichts zum Digitalen Verbraucherschutz mit dem Schwerpunktthema „Cyber-Sicherheit im Gesundheitswesen“.

Juli

Standort Freital

Präsentation des Digitalen Verbraucherschutzes im Rahmen der offiziellen Eröffnung einer neuen BSI-Liegenschaft im sächsischen Freital

August

Messe: Gamescom

Messebeteiligung und Ansprache der Gamerinnen und Gamer mit zielgruppengerechten Formaten rund um IT-Sicherheitsthemen

September

Podcast „Update verfügbar“

Der Podcast feiert nach 13 erfolgreichen Folgen seinen einjährigen Geburtstag und ist zum reichweitenstärksten BSI-Kanal avanciert.

Digitalbarometer

Ergebnisveröffentlichung der Bürgerbefragung zur Cyber-Sicherheit vom BSI und der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK)

November

Messenger-Publikation

Veröffentlichung einer BSI-Publikation „Moderne Messenger – heute verschlüsselt, morgen interoperabel?“ im Rahmen der Zusammenarbeit mit dem Bundeskartellamt

Messe: Deutscher Seniorentag

Erstmalige BSI-Messebeteiligung auf der wichtigsten bundesweiten Veranstaltung für die Zielgruppe der 60+

Dezember

IT-Sicherheits-kennzeichen

Start der Beantragungs-möglichkeit für Hersteller/ Anbieter mit den ersten zwei Produktkategorien „Breitbandrouter“ und „E-Mail-Dienste“

Inhaltsverzeichnis

Digitaler Verbraucherschutz ist das Fundament einer sicheren IT-Landschaft in Deutschland

Mit dem Einzug digitaler Anwendungen in den Alltag der Menschen ist klar geworden: Digitaler Verbraucherschutz ist wichtiger denn je. Smarte Fernseher, Staubsaugerroboter, Smartwatches, Sprachassistenten, Smartphone und Tablet – wir nutzen immer mehr vernetzte Geräte. Und jedes vernetzte Gerät ist potenziell angreifbar. Dadurch sind private Haushalte zunehmend verletzlich, wie der vorliegende Bericht darlegt.

Die Bundesregierung hat der wachsenden Bedeutung des Themas Digitaler Verbraucherschutz im vergangenen Jahr mit dem IT-Sicherheitsgesetz 2.0 Rechnung getragen. Darin werden die Kompetenzen des BSI für diesen Bereich deutlich gestärkt. Es ist gut, dass die seit drei Jahrzehnten etablierte Expertise des BSI nun noch stärker dafür genutzt wird, Verbraucherinnen und Verbraucher zu schützen.

Einer der wichtigsten Fortschritte ist die Einführung des IT-Sicherheitskennzeichens. Damit können Verbraucherinnen und Verbraucher schon bei der Kaufentscheidung erkennen, ob sich der Hersteller eines Geräts oder der Anbieter eines Dienstes dazu verpflichtet hat, bestimmte Sicherheitsanforderungen zu erfüllen – beispielsweise Updates zum Schließen von Sicherheitslücken bereitzustellen. Wir stellen damit die Informationen bereit, die sie benötigen, um ihren Einfluss als Konsumentinnen und Konsumenten zu nutzen. Wenn IT-Sicherheit ein relevanter Faktor bei der Kaufentscheidung ist, erhöht das für Hersteller und Anbieter den Anreiz, die Sicherheit ihrer Produkte zu verbessern.

In immer größerem Maße gilt das auch für Autos. Schon heute erzeugen, übermitteln und nutzen sie eine Vielzahl von Daten. Der Gebrauch von künstlicher Intelligenz vor allem im Bereich des autonomen Fahrens wird das in künftigen Modellen noch verstärken. Grund genug, diesem Bericht einen Schwerpunkt zu widmen, wie die Mobilität der Zukunft sicher gestaltet werden kann – damit Verbraucherinnen und Verbraucher sicher an ihr Ziel kommen.

Das BSI hat einen integrierten Blick auf Cyber-Sicherheit in Staat, Wirtschaft und Gesellschaft. Der Digitale Verbraucherschutz steht in dieser Perspektive in direktem Zusammenhang mit anderen Themen wie Bedrohungen für Unternehmen und kritische Infrastrukturen, für Staat und Verwaltung oder der Diskussion um Cyber-Angriffe als Mittel hybrider Kriegsführung. Denn individuelle Sicherheitskompetenzen sind das unverzichtbare Fundament für eine sichere Digitalisierung in Deutschland. Der Faktor Mensch spielt nach wie vor eine zentrale Rolle bei Cyber-Angriffen, der Klick auf kompromittierte Links oder Anhänge ist zum traurigen Klassiker im Repertoire der Angriffswerkzeuge geworden.

Das Bewusstsein für und das Wissen über Cyber-Sicherheit zu fördern, ist deshalb nicht nur ein Beitrag zum individuellen Schutz von Verbraucherinnen und Verbrauchern, sondern auch zur Stärkung der Informationssicherheit in Deutschland. In diesem Sinne informieren und sensibilisieren wir mit unserer breit angelegten Kampagne „#einfachaBSIchern“, die wir im vergangenen Jahr gestartet haben. Und wir setzen darauf, Kräfte zu bündeln und mit zivilgesellschaftlichen Institutionen sowie der Wirtschaft Hand in Hand zu arbeiten, um so viele Menschen wie möglich zu erreichen.

Arne Schönbohm
Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI)

Digitale Sicherheit für Verbraucherinnen und Verbraucher ist eine Gemeinschaftsaufgabe

„Wie können sich Verbraucherinnen und Verbraucher im digitalen, vernetzten Raum sicher bewegen?“ Das ist die zentrale Fragestellung des Digitalen Verbraucherschutzes. Eine Antwort darauf ist komplex, bedarf vieler Perspektiven und zugleich der Anstrengungen unterschiedlichster Akteure.

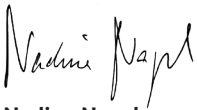
Der „Bericht zum Digitalen Verbraucherschutz 2021“ zeigt, mit welchen Risiken und aktuellen Bedrohungen der private, digitale Alltag konfrontiert wird. Nur: Was tun? Starke Passwörter, eng getaktete Updates, mächtige Firewalls, … die Liste an technischen Schutzmöglichkeiten ist lang. Vergessen wird dabei oft der Mensch selbst. Wie tickt die Person? Was macht sie verletzlich? Welche Sicherheitshinweise und guten Ratschläge nimmt sie wahr – und wie handelt sie dann tatsächlich? Die Brücke zwischen den Möglichkeiten der IT-Sicherheitstechnik und der realen Verbraucherwelt ist oft ein fragiles Konstrukt. Die Vielfalt an (technischen) Optionen und Anforderungen führt in Kombination mit zunehmenden Risiken leicht zur Überforderung. Das gilt unabhängig vom Wissensstand jedes Einzelnen. Nicht zu vernachlässigen ist auch die Rolle der Hersteller und Anbieter. Für ihre digitalen Angebote müssen sie nicht nur ein Mindestmaß an Informationssicherheit bieten, sondern ihre Kundinnen und Kunden geschickt „an die Hand nehmen“, den sicheren Gebrauch vereinfachen und bestenfalls Begeisterung für IT-Sicherheitsthemen entfachen.

Die Verbesserung des Schutzniveaus für Verbraucherinnen und Verbraucher im vernetzten Alltag – in allen Facetten – ist eine gesamtgesellschaftliche Aufgabe. Wir als Bundesamt für Sicherheit in der Informationstechnik leisten unseren Beitrag dazu. Auf Basis unseres kooperativen Ansatzes setzen wir uns für den Dialog und die Vernetzung der beteiligten Akteure ein. Nur gemeinsam können wir diese Aufgabe angehen und mehr erreichen. Dazu zählt beispielsweise der „Dialog für Cyber-Sicherheit“, ein moderierter, strukturierter Dialogprozess.

Hier treffen Vertreterinnen und Vertreter der organisierten Zivilgesellschaft sowie aus Wissenschaft, Kultur und Medien, Wirtschaft und Staat zusammen. Der 2021 im BSI begründete „Beirat Digitaler Verbraucherschutz“ vernetzt vielfältige Stakeholder, setzt wichtige Impulse von außen und öffnet den „Blick über den Tellerrand“.

Das Schwerpunktthema „Automotive“ des vorliegenden Berichts zeigt eindrucksvoll die vielfältigen Herausforderungen, die allein dort im Bereich der Informationssicherheit vor uns liegen. Die skizzierten Handlungsfelder verdeutlichen einmal mehr die Notwendigkeit einer intensiven Zusammenarbeit vieler Akteure aus Wirtschaft, Staat und Zivilgesellschaft. Denn nur so erreichen wir das Ziel, Verbraucherinnen und Verbrauchern eine sichere (Auto-)Mobilität zu ermöglichen.

Ich wünsche Ihnen im Namen des gesamten Verbraucherschutz-Teams im BSI viel Freude und Erkenntnisgewinn bei der Lektüre!



Nadine Nagel
Leiterin der Abteilung WG
„Cyber-Sicherheit für Wirtschaft und Gesellschaft“

1 Einleitung: Verbraucherinnen und Verbraucher stark machen für den digitalen Alltag

Das Bundesamt für Sicherheit in der Informationstechnik verfolgt beim Digitalen Verbraucherschutz das Ziel, Verbraucherinnen und Verbraucher so zu stärken, dass sie sich im digitalen, vernetzten Alltag sicher bewegen können. Das Thema ist vielschichtig, einer enormen Dynamik ausgesetzt und eine Gemeinschaftsaufgabe, bei der viele Herangehensweisen verschiedenster handelnder Akteure zusammentreffen. Daher wollen wir mit dem „Bericht zum Digitalen Verbraucherschutz"...

- Orientierung in diesem Themenfeld bieten,
- aktuelle Herausforderungen der Informationssicherheit beleuchten und
- Anknüpfungspunkte für den Austausch der unterschiedlichen gesellschaftlichen Stakeholder schaffen.

Was dürfen Sie in diesem Jahresbericht erwarten?

Der vorliegende Band geht auf aktuelle Themenstellungen der Informationssicherheit im Kontext des Digitalen Verbraucherschutzes im Berichtsjahr 2021 ein. Aufbauend auf den Erkenntnissen des zurückliegenden Jahres widmen wir uns der Frage, welchen Herausforderungen Verbraucherinnen und Verbraucher in der Digitalisierung gegenüberstehen und welche Methoden zur Steigerung der individuellen IT-Sicherheit sie unterstützen können. Dabei werden unter anderem Erkenntnisse aus der BSI-internen „Arbeitsgruppe Verbraucher(leit)bilder" sowie der aktuellen Verbraucherforschung einbezogen. Ein Fokus liegt auf den Anforderungen der Wissens- und Informationsvermittlung.

Ein weiterer inhaltlicher Punkt ist die IT-Sicherheitslage für Verbraucherinnen und Verbraucher. Die 2021 bekannt gewordenen Sicherheitsrisiken und -vorfälle, unter denen erneut zahlreiche Datenleaks bei Unternehmen waren, erhielten viel Aufmerksamkeit in den Medien. Ransomware-Angriffe, welche oftmals in Verbindung mit Datenleaks stehen, sind ein Kernthema im Kapitel zu Schwerpunkten bei Sicherheitsvorfällen auf dem digitalen Verbrauchermarkt. Ergänzend werden weitere Gefahren beleuchtet, darunter Social Engineering am Beispiel von Smishing-Wellen oder Betrugsmaschen beim Online-Shopping.

Das Themenfeld „Automotive" ist ein weiterer Schwerpunkt dieser Ausgabe. Digitalisierung verändert nicht nur das einzelne Fahrzeug, die Vernetzung revolutioniert auch die Mobilität insgesamt. Das Automobil erlebt einen enormen Innovationsschub. Nur: Wie kann die IT-Sicherheit in der Automobilbranche kontinuierlich auf hohem Niveau gehalten werden? Wie können Verbraucherinnen und Verbrauchern sichere Produkte und Dienste in diesem Bereich bereitgestellt werden? Die vorliegende Publikation nähert sich diesen Herausforderungen und betrachtet zugleich Trends wie das autonome Fahren und die E-Mobilität aus der Verbraucherperspektive. Gleichermaßen geben wir durch ein spannendes Interview Einblicke in die institutionelle Zusammenarbeit mit dem Kraftfahrt-Bundesamt (KBA).

Der Bericht zum Digitalen Verbraucherschutz leistet einen Beitrag zum gesamtgesellschaftlichen Dialog in den Bereichen Informationssicherheit und Verbraucherschutz. Er beleuchtet etablierte sowie neu entstehende Handlungsfelder für Akteure aus Politik, Wirtschaft und Gesellschaft und formuliert Empfehlungen zur Stärkung von Verbraucherinnen und Verbrauchern in der digitalen Welt.

2 Verbraucherinnen und Verbraucher im Blickpunkt

Verbraucherinnen und Verbraucher sind ein integraler Bestandteil einer sicheren Digitalisierung. Durch den Kauf sicherer Produkte, vor allem aber durch deren sichere Nutzung tragen sie zunehmend mehr Verantwortung. Doch die Informationssicherheit stellt nur einen kleinen Ausschnitt dessen dar, womit sich Verbraucherinnen und Verbraucher im Alltag auseinandersetzen müssen. Deshalb ist die adressatengerechte Kommunikation von Sicherheitsempfehlungen ein wichtiger Bestandteil einer erfolgreichen Cyber-Sicherheitsstrategie.

Mehr über die Verbraucherinnen und Verbraucher zu wissen – welche Kompetenzen wie in der Bevölkerung verteilt sind, welche Faktoren Verletzlichkeit auslösen und welche Produkte und Anwendungen bei der Nutzung erhöhte Risiken für welche Verbraucherinnen und Verbraucher verursachen – ist ein zentrales Anliegen des Digitalen Verbraucherschutzes im BSI. Daher werden im Folgenden vor allem wissenschaftliche Erkenntnisse rund um das Verhalten von Verbraucherinnen und Verbrauchern im Bereich der Informationssicherheit dargestellt. Dem geht eine Klärung des Begriffsverständnisses zu den Verbraucherinnen und Verbrauchern im Digitalen Verbraucherschutz voraus, um dann auf verschiedene, für die Informationssicherheit von Verbraucherinnen und Verbrauchern relevante Aspekte wie Digitalkompetenz und Schutzmaßnahmen einzugehen. Dies erfolgt sowohl anhand BSI-eigener Studien wie auch ausgewählter Publikationen, unter anderem im Bereich der Human–Computer Interaction und der Verbraucherforschung. Im Anschluss daran werden sowohl besondere Problemstellungen und Lösungsansätze herausgearbeitet wie auch blinde Flecken an der Schnittstelle von Verbraucher- und Sicherheitsforschung aufgezeigt.

Der Verbraucherbegriff im Digitalen Verbraucherschutz

Zunächst ist es wichtig, sich dem Begriff des Verbrauchers selbst weiter anzunähern. Denn während beispielsweise für die Arbeit der Verbraucherzentralen die Definition nach Paragraf 13 des Bürgerlichen Gesetzbuches maßgebend ist, gerät der Fokus auf die Verbraucherinnen und Verbraucher als Vertragspartnerinnen und -partner, Kundinnen und Kunden sowie Käuferinnen und Käufer zu eng, wenn es um Informationen und die Beratung zu Informationssicherheit geht. Hier ist ein weiter gefasstes Verständnis von Konsum notwendig, das explizit die Nutzung mit einschließt:

Verbraucherin beziehungsweise Verbraucher im Sinne des Digitalen Verbraucherschutzes des BSI ist jede natürliche Person, der bei der privaten Nutzung von Produkten, Dienstleistungen oder Anwendungen ein Risiko in der Informationssicherheit entsteht oder entstehen könnte.

Diese Definition trägt zudem der Erkenntnis Rechnung, dass sich in digitalen Handlungszusammenhängen traditionelle Rollenzuschreibungen zwischen Bürgerinnen beziehungsweise Bürgern und Verbraucherinnen beziehungsweise Verbrauchern zunehmend auflösen. Eine Differenzierung zwischen diesen Rollen erscheint hier nicht mehr zweckgemäß. In der Verbraucherforschung wurde deshalb vorgeschlagen, zwischen dem stark an Paragraf 13 des Bürgerlichen Gesetzbuches angelehnten Begriff des Verbrauchs, der auf den Abschluss eines Rechtsgeschäfts sowie die dahinterliegenden Zwecke abzielt, einerseits und dem allgemeinen Konsum als Tätigkeit andererseits zu differenzieren (Fridrich et alia 2014: Seite 323; Fridrich et alia 2017: Seite 5 und folgende). Dies betrifft unter anderem auch den Bereich der öffentlichen Verwaltung, in dem sich eine zunehmende Kundenorientierung feststellen lässt. Gleichzeitig steigt die Erwartung, dass Verbraucherinnen und Verbraucher selbst ihr Handeln im Bereich der Informationssicherheit am Gemeinwohl ausrichten, um zum Beispiel Gefährdungen durch „Distributed-Denial-of-Service“-Angriffe zu reduzieren (vgl. Kapitel 4).

Demgegenüber ergeben sich für Verbraucherinnen und Verbraucher Risiken der Informationssicherheit bei der Nutzung digitaler Produkte, Anwendungen und Dienstleistungen durch die Gefährdung der Authentizität, Vertraulichkeit, Integrität und Verfügbarkeit der dabei verarbeiteten und gespeicherten Daten. Aus diesem Grund greift die Definition von Paragraf 13 des Bürgerlichen Gesetzbuches zu kurz, da sie den Abschluss eines Rechtsgeschäfts voraussetzt, was einen Großteil der oben beschriebenen Anwendungsszenarien im privaten Nutzungsalltag ausschließt und damit den Schutzzielen der Informationssicherheit (Vertraulichkeit, Integrität und Verfügbarkeit) nicht oder nicht hinlänglich gerecht wird.

Digitale (Verbraucher-)Kompetenz

Während das Begriffsverständnis von Verbraucherin und Verbraucher im Digitalen Verbraucherschutz inklusiv angelegt ist, gilt es bei der Kommunikation, der Heterogenität der zu Adressierenden Rechnung zu tragen. Diese bilden in ihren Wahrnehmungen und Einstellungen sowie den Fähigkeiten im Umgang mit Gefahren in der digitalen Welt keine homogene Gruppe. Deutlich wird dies mit Bezug auf die Verteilung von Kompetenz, als Verbraucherin oder Verbraucher in digitalen Settings zu agieren.

So legte im Jahr 2021 der Sachverständigenrat für Verbraucherfragen erstmals ein Gutachten zur Lage der Verbraucherinnen und Verbraucher in Deutschland vor, in dem folgende Problemstellungen für den Digitalen Verbraucherschutz benannt wurden:

- Digitalkompetenzen sind in der Bevölkerung lückenhaft und sozial ungleich verteilt (ebenda: Seite 22), hier seien differenzierte und zielgruppenorientierte Verbraucherbildungsmaßnahmen zu entwickeln (ebenda: Seite 10).

- Geringes Interesse der Verbraucherinnen und Verbraucher an Transparenzinformationen, wodurch die Notwendigkeit einer (behördlichen) Aufsicht betont wird; gleichermaßen solle der Informationsaufwand auf Seiten der Verbraucherinnen und Verbraucher reduziert werden (ebenda).

- Bezüglich des Internet of Things wird das zügige Vorantreiben eines praxistauglichen Kennzeichens der Informationssicherheit gefordert, flankiert von der Förderung zielgruppenspezifischer Informations- und Unterstützungsangebote. Informationssicherheit und Nutzerfreundlichkeit dürften nicht gegeneinander abgewogen werden.

Zu berücksichtigen ist, dass im Gutachten die empirische Datenlage in Bezug auf Digitalkompetenz von Verbraucherinnen und Verbrauchern als unzureichend dargestellt wird. Dies gilt in besonderem Maße für den Aspekt der Informationssicherheit im Verbraucheralltag. Das Gutachten trägt dazu bei, diese Lücke zu schließen. Es ergeben sich jedoch Einschränkungen durch die Erhebungsmethode (deutschsprachige Bevölkerung), das Erhebungsinstrument (Wissensfragen statt Performanz) sowie dessen Inhalte (stark am Verhalten vor dem Kauf und rechtlichen Fragenstellungen orientiert), womit nur ein sehr spezifischer Teil der digitalen Verbraucherkompetenz aus BSI-Sicht abgedeckt ist.

Demgegenüber wurden Digitalkompetenzen im Sonderbericht der Initiative D21 breiter erfasst. Insgesamt ließ sich feststellen, dass die Nutzung digitaler Anwendungen und Dienste weiter zugenommen, das Kompetenzniveau sich jedoch kaum verändert hat. Analog zu den Erkenntnissen im Gutachten des Sachverständigenrats für Verbraucherfragen zur Lage der Verbraucherinnen und Verbraucher sind es wiederum insbesondere ältere Bevölkerungsgruppen und Personen mit geringer Bildung, bei denen die Defizite über alle Bereiche besonders stark ausgeprägt sind (vgl. ebenda: Seite 14). Als grundlegendes Problem zeigt sich eine Diskrepanz zwischen Anwendungs- und Problemlösungskompetenz. Das heißt, die Nutzerinnen und Nutzer zeigen sich kompetent darin, digitale Angebote zu nutzen, sie verstehen aber nicht die ihnen zugrundeliegenden Mechanismen (ebenda: Seite 11). Blickt man auf die unterschiedlichen Kompetenzbereiche, so zeigen sich hier mitunter stark ausgeprägte Defizite. Denn während sich ein Großteil der Nutzerinnen und Nutzer sowohl bei Daten- und Informationskompetenz sowie bei Kommunikation und Kollaboration als handlungsfähig erweist, zeigt sich im Bereich der Gestaltungskompetenz ein anderes Bild. Während noch 59 Prozent der Befragten eigene Texte erstellen können, beherrschen nur 14 Prozent eine Programmiersprache (ebenda: Seite 44). Dies ist nicht nur besorgniserregend, weil die Teilhabemöglichkeiten an der Gestaltung digitaler Handlungsumgebungen damit auf eine sehr kleine Gruppe und deren Bedarfe sowie Vorstellungen begrenzt sind, sondern auch, weil Selbstwirksamkeit eng an die Erfahrung der praktischen Umsetzbarkeit eigener Inhalte und Ideen gekoppelt ist (ebenda: Seite 54). Hinsichtlich der Sicherheit zeigen sich Diskrepanzen bezüglich Bildung und beruflicher Tätigkeit. So liegt die Verwendung einer Anti-Viren-Software bei Personen mit Bürojob bei 81 Prozent gegenüber 56 Prozent ohne. Ein weiterer wichtiger Kompetenzbereich betrifft die Fähigkeit zur Aneignung digitaler Kompetenzen allgemein. Hier zeigt die Befragung eine deutliche Verzerrung hinsichtlich des Geschlechts. So wissen 66 Prozent der höher gebildeten Männer, wie sie sich selbst digitale Kompetenzen aneignen – bei den höher gebildeten Frauen gilt das gerade einmal für 30 Prozent (ebenda: Seite 76). Insgesamt deuteten die Ergebnisse auf das Innovativeness-needs-Paradox hin, demzufolge gerade diejenigen, die am meisten von neuen (digitalen) Unterstützungsangeboten profitierten, die letzten seien, die sie nutzten (ebenda: Seite 82). Folglich müsse es beim Auf- und Ausbau von Digitalkompetenzen zentral darum gehen, gesellschaftliche Ungleichheit zu reflektieren und durch entsprechende Angebote zu adressieren. Neben der Etablierung eines Basisschutzes von digitalen Anwendungen und Produkten sehen die Autorinnen und Autoren die Steigerung von Digitalkompetenz durch gezielte Bildungsmaßnahmen als entscheidenden Schritt, um die Digitalisierung der Gesellschaft inklusiv und sicher weiterzuentwickeln.

Die Cyber-Sicherheit im privaten Alltag

Um die Risiken und Kompetenzen auf Seiten der Verbraucherinnen und Verbraucher richtig einzuschätzen und entsprechende Maßnahmen zu entwickeln, erstellt das BSI gemeinsam mit der Polizeilichen Kriminalprävention der Länder und des Bundes seit 2019 das Digitalbarometer. Es ermöglicht durch eine jährliche repräsentative Befragung nicht nur, das Verhalten der Verbraucherinnen und Verbraucher in puncto Informationssicherheit zu erheben, sondern gleichzeitig auch einen Entwicklungsverlauf darzustellen.

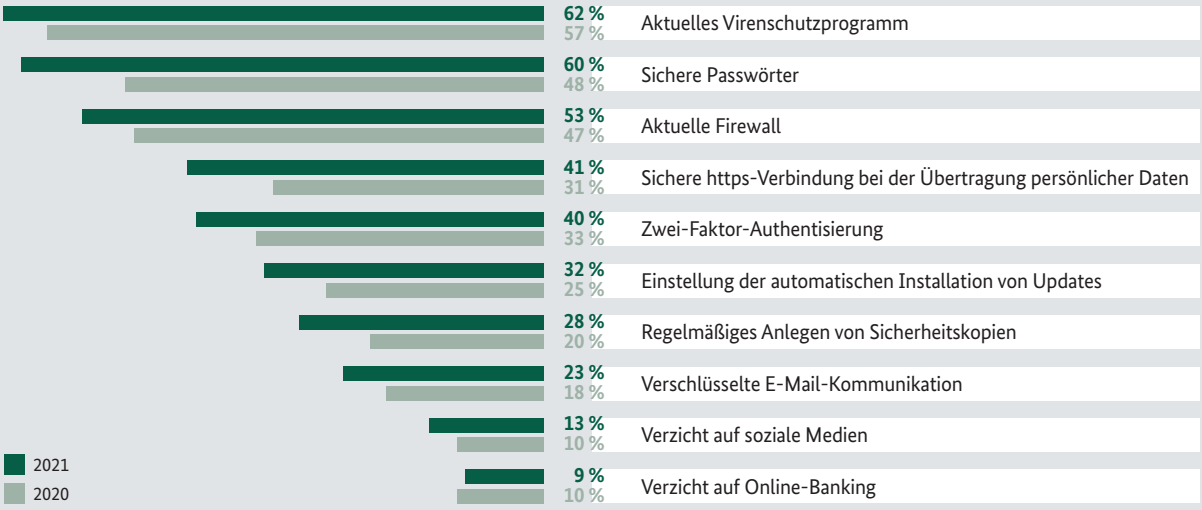
Die Ergebnisse des Digitalbarometers 2021 zeigen: Die Bedrohungslage bleibt weiterhin hoch. Jeder bzw. jede Vierte

war bereits betroffen von Cyber-Kriminalität. Zudem konnte eine besonders schützenswerte Zielgruppe identifiziert werden: Unter den Befragten im Alter zwischen 19 und 29 Jahren ist fast jede und jeder Dritte schon einmal Opfer von Online-Kriminalität geworden. Zu den häufigsten Straftaten zählen für alle Betroffenen Fremdzugriffe auf den eigenen Online-Account (31 %), Download von Schadsoftware (28 %) und Phishing (25 %).

Trotz der andauernden Gefahr, Opfer von Cyber-Kriminalität zu werden, interessiert sich nur jeder Zweite beziehungsweise jede Zweite für Informationen über Sicherheit im Internet. 22 Prozent gaben sogar an, sich nie zu informieren. Das Wissen der Menschen führt zudem nicht direkt zu einer Handlung. Denn Sicherheitshinweise wirken auf viele Menschen schwer verständlich und aufwendig in der Umsetzung. So kennen zwei Drittel der Befragten Empfehlungen, um sich vor Internetgefahren zu schützen – aber nur 12 Prozent geben an, diese vollständig umzusetzen. Als Gründe dafür wurden vor allem aufgeführt, dass Sicherheitsempfehlungen zu kompliziert beziehungsweise schwer verständlich seien (43 %) und zu viel Aufwand (44 %) bedeuteten. Diejenigen, die die Empfehlungen umsetzen, empfinden das anders: Nur 9 Prozent sagen, dass ihnen viel Aufwand entsteht.

Im Schnitt nutzen die Befragten drei bis vier Maßnahmen, um sich vor Gefahren im Internet zu schützen – die Nutzung stieg im Vergleich zu den Vorjahren weiter an.

Wie schützen Sie sich vor Gefahren im Internet?



Basis: Alle Befragten (2021: *n* - 2.025). Mehrfachnennungen möglch.

Herausforderungen der Vermittlungsarbeit

Um sich zu schützen, nutzt ein Großteil ein Antivirenprogramm (62 %), sichere Passwörter (60 %) und eine aktuelle Firewall (53 %). Unterschätzt werden noch automatische Updates (32 %) und die Zwei-Faktor-Authentisierung. Dabei sind gerade diese Maßnahmen sehr hilfreich, um häufige Angriffsarten wie Schadprogramme oder Fremdzugriffe auf ein Online-Konto erfolgreich abzuwehren. Aus den Ergebnissen des Digitalbarometers 2021 lassen sich die aktuellen Herausforderungen in der Vermittlungsarbeit ableiten: Einerseits bestehen viele Vorbehalte, sich mit dem Thema Cyber-Sicherheit auseinanderzusetzen, weil es grundsätzlich nicht interessant, kompliziert und aufwendig erscheint. Hier gilt es in der Vermittlungsarbeit Formate zu finden, die besonders niederschwellig sind und eine leichte Umsetzung in den Alltag ermöglichen. Darüber hinaus ist es zielführend, den Verbraucherinnen und Verbrauchern zu kommunizieren, dass ein starker Basisschutz aus mehreren Maßnahmen besteht, und ihnen eine Orientierung zu geben, welche Maßnahmen helfen können, um den häufigsten Straftaten im Internet zu begegnen. Dazu gehören beispielsweise automatische Updates, die Sicherheitslücken schließen, im besten Fall, bevor ein Schadprogramm Schaden anrichten kann.

Die Zahlen des Digitalbarometers zeigen auch, dass viele Verbraucherinnen und Verbraucher ihre Online-Konten nur unzureichend schützen. Um ihnen die richtigen Schutzmaßnahmen an die Hand zu geben, hat das BSI gemeinsam mit dem Bundeskanzleramt das Projekt „Schutz von Online-Konten“ ins Leben gerufen. Im März 2020 ließen sich die ersten Zwischenergebnisse publizieren. Sie zeigen, dass sich ein Großteil der Befragten

bemüht, komplexe und lange Passwörter im Gedächtnis zu behalten oder diese mittels Zettel und Stift zu notieren. Die größte Herausforderung ist es jedoch, sich die Passwörter zahlreicher Accounts zu merken. Verbraucherinnen und Verbraucher reagieren oftmals darauf, indem sie ein Passwort für mehrere Accounts nutzen oder es an den jeweiligen Account nur leicht anpassen. Für die Sicherheit der Online-Konten sind diese Herangehensweisen nur bedingt empfehlenswert. Zudem werden Passwort-Manager skeptisch beurteilt. Einerseits aus einem Misstrauen gegenüber dem Anbieter, andererseits aus der Sorge, dass sich mit einem Schlag alle Passwörter stehlen ließen. Deswegen wurden in der zweiten Phase gezielt Informationen und Hilfestellungen erarbeitet, um Bürgerinnen und Bürgern konkrete Maßnahmen aufzuzeigen, wie sie ihre Accounts sichern können. Die erarbeiteten Handlungsempfehlungen und Materialien werden in einer dritten Phase 2022 in einem Feldexperiment überprüft, unter anderem gemeinsam mit E-Mail-Providern.

Die Anwendersicht im Mittelpunkt: Erkenntnisse aus der Usable Security Forschung

Im Ansatz der Usable Security wird Informationssicherheit aus Sicht der Anwenderinnen und Anwender betrachtet, um der Relevanz des Faktors Mensch gerecht zu werden. Grundlegend ist dabei die Annahme, dass Cyber-Sicherheit kein technisches Phänomen ist, sondern in soziale und kulturelle Kontexte eingebettet ist (Dourish and Anderson, 2006: Seite 319). Auch kann sich das Verständnis von Sicherheit im Laufe der Zeit wandeln, was dazu führt, dass vormals wohl etablierte Verhaltensweisen (Fahrrad- oder Skifahren ohne Helm, unter anderem) als unangemessen und selbstschädigend etikettiert werden. Schließlich sei zu berücksichtigen, dass Information und ihre Nutzung sozialen Intentionen (Identität, Zugehörigkeit, Vertrauen, Intimität und so weiter) folgen. Diese formten den Umgang mit Informationen und entsprechend den mit Sicherheit(sanforderungen) (ebenda: Seite 322 folgende). Bei der Entwicklung von digitalen Produkten hat sich diese Perspektive noch nicht durchgesetzt, die stärker die menschliche Seite von Informationssicherheit akzentuiert. Das zeigt sich beispielsweise an Defiziten im Design (Chong et alia, 2019: Seite 5).

Das Forschungsfeld der Usable Security reicht von der Untersuchung von Sicherheitspraktiken bis hin zur Entwicklung von Designs, die das Management der Sicherheit von Privatheit befördern sollen. Darüber hinaus betonen Dourish und Anderson (2006) die Relevanz der Forschung, die sich mit der sozialen Einbettung von Sicherheit und Privatheit auseinandersetzt (ebenda: Seite 325). Entscheidende Beiträge zu diesem Bereich verdanken sich der Forschungsarbeit von Sasse (Adams and Sasse, 1999; Sasse and Smith, 2016; Weirich and Sasse, 2001), die bereits 1999 auf Fehler im Bereich der Entwicklung von Technologien in der Informationssicherheit hinwies:

> *It seems that currently, hackers pay more attention to the human link in the security chain than security designers do, for example, by using social engineering techniques to obtain passwords.*
> *(Adams and Sasse, 1999: Seite 41).*

Die überraschende Erkenntnis dieser Untersuchung war, dass gerade jene Anforderungen zu unsicheren Passwörtern führten, die Unternehmen ihren Angestellten beim Erstellen von Passwörtern auferlegten, um ein hohes Maß von Sicherheit zu gewährleisten (vergleiche ebenda: Seite 42). Dieser Zielkonflikt zwischen den Sicherheitsrichtlinien von Unternehmen und den Bedürfnissen von Angestellten zeigt sich trotz dieser frühen Intervention als erstaunlich persistent. Denn während die Sicherheitsanweisungen von Unternehmen primär dem Schutz der Unternehmensdaten dienen, geht es den Mitarbeitenden vorrangig um etwas anderes – nämlich bestimmte Aufgaben zu erledigen, eine Recherche durchzuführen, ein Meeting abzuhalten oder eine Präsentation zu erstellen. Anforderungen an die Informationssicherheit können die Durchführung dieser Aufgaben erschweren, kosten zusätzliche Zeit und lenken von den (eigentlichen) Arbeitszielen ab (Neumann, 2017: Seite 87).

Fox and Titze (2021) sehen deshalb die Veränderung der persönlichen Haltung als entscheidende Voraussetzung, damit Nutzerinnen und Nutzer Sicherheitsempfehlungen als relevant zur Abwehr von Risiken wahrnehmen (ebenda: Seite 728). Ein unspezifisches Warnen sei jedoch sinnlos. Die Angestellten müssten vielmehr die konkreten Risiken kennen und verstehen, die sie mit ihrem Verhalten beeinflussen können (ebenda). Sasse and Smith (2016) kritisieren allerdings die begrenzte Reichweite vieler Studien im Kontext der Usable Security:

> *When we examine published usable security research to date, we find that most studies have been performed in laboratories with a limited number of participants (often students) who were observed on one occasion using a security mechanism.*
> *(Ebenda: Seite 11–12)*

Auch ist fraglich, inwieweit sich die so gewonnenen Erkenntnisse auf die Verbraucherinnen und Verbraucher übertragen lassen. Findet Neumann (2017), wie oben skizziert, bereits im Unternehmenskontext einen Zielkonflikt zwischen Sicherheitsanforderung und Arbeitsauftrag, so dürfte sich dieser im privaten Alltag nicht weniger ausgeprägt gestalten. Vielmehr ist davon auszugehen, dass die Notwendigkeit, zwischen den verschiedenen Interessen und Bedürfnissen von Haushaltsmitgliedern zu vermitteln, die sozio-emotionale Aushandlung von Zuständigkeiten, Verantwortlichkeiten und Freiräumen sowie letztlich auch die rein pragmatische Bewältigung der hauswirtschaftlichen Erfordernisse, der Integration neuer Routinen im Kontext von Informationssicherheit einigen Widerstand entgegensetzen dürften. Auch ist der Zugriff der Kommunikatoren auf die Verbraucherinnen und Verbraucher in der Regel nur mittelbar. Es ist daher ungewiss, ob die Information diese erreicht, von ihnen wahrgenommen und als relevant eingestuft wird – und womöglich sogar eine Verhaltensänderung erfolgt. An dieser Stelle besteht Nachholbedarf auf Seiten der Forschung, wobei Anwendungsbeispiele aus ähnlich gelagerten Problembereichen (wie zum Beispiel der Nachhaltigkeitskommunikation) sich als hilfreich erweisen können. Auch sollte das vorhandene Instrumentarium an Cyber-Sicherheits-Awareness-Maßnahmen dahingehend geprüft werden, inwieweit sich damit die unterschiedlichen Verbraucherinnen und Verbraucher erreichen und zu Verhaltensänderungen bewegen lassen. Angesichts der zunehmenden Gefährdung des digitalen Alltags, ließen sich auch die Entwicklung neuer Methoden, die beispielsweise Awareness-Maßnahmen mit Consumer-Enabling-Technologie (Thorun and Diels, 2020) verknüpfen, erwägen. Dabei käme es auch darauf an, Anwendersicht und Informationssicherheit von Beginn an zu berücksichtigen, beispielsweise durch partizipative Designs.

Resümee

Dem Digitalen Verbraucherschutz im BSI liegt ein weites Verständnis des Verbraucherbegriffs zugrunde. Dieses folgt der Einsicht, dass sich Gefährdungen im Cyber-Raum nicht nur mit Fokus auf das Kaufen sinnvoll bekämpfen lassen. Im Hinblick auf die Übertragbarkeit von Erkenntnissen der Verbraucherforschung einerseits und der Human-Computer Interaction andererseits führt dies zu Einschränkungen. Denn während erstere dem Aspekt des Kaufens gegenüber der Nutzung häufig den Vorrang einräumt, richtet letztere den Blick eher auf die Anwenderin beziehungsweise den Anwender im Unternehmenskontext. Studien wie die der Initiative D21 deuten auf einen Zusammenhang zwischen beruflicher Tätigkeit und Digitalkompetenz im Allgemeinen hin. Wie sich dieser Zusammenhang im Besonderen, nämlich hinsichtlich der für die Informationssicherheit relevanten Kompetenz gestaltet, wäre einer näheren Betrachtung wert. Trotz der starken Gewichtung wirtschaftlicher und rechtlicher Aspekte bei der Messung digitaler Verbraucherkompetenz im Bericht zur Lage der Verbraucherinnen und Verbraucher könnte sich die Erkenntnis der sozialen Ungleichverteilung von Wissen und Fähigkeiten auch bezüglich der Informationssicherheit als relevant erweisen. Knappe finanzielle Ressourcen können dazu führen, dass eher die Zustimmung zur Nutzung der eigenen Daten erteilt wird, anstatt für die Bereitstellung eines Dienstes einen Geldpreis zu zahlen. Auch mögen Sicherheitsbedenken bei der Weiterverwendung von Gütern ohne Sicherheits-Updates in den Hintergrund treten, wenn der Neukauf nicht möglich ist oder eine verhältnismäßig große Belastung darstellen würde. Während sich die Kosten für Sicherheit in Unternehmenskontext recht klar beziffern lassen, steht eine solche Kalkulation für Privathaushalte noch aus. Wie die Zahlen des Digitalbarometers zeigen, fehlt es mitunter auch noch an dem erforderlichen Bewusstsein für grundlegende Maßnahmen wie die Aktivierung der automatischen Updates. Das Bundesamt für Sicherheit in der Informationstechnik setzt genau an dieser Stelle an und trägt durch Projekte wie die gemeinsam mit dem Bundeskanzleramt durchgeführte Studie zum Schutz von Online-Konten dazu bei, die Hürden im Alltag der Verbraucherinnen und Verbraucher bei der Umsetzung von Informationssicherheit besser verstehen zu können.

Das IT-Sicherheitskennzeichen: Mehr Transparenz am digitalen Verbrauchermarkt

Das Internet der Dinge (Internet of Things, kurz: IoT), etwa in Form von vernetzten Smart-TVs, Routern oder Kühlschränken, durchdringt und erleichtert zunehmend den privaten Alltag. Die Digitalisierung des täglichen Lebens bringt neben Annehmlichkeiten auch sicherheitsrelevante Gefahren mit sich. Gleichzeitig wird es für Verbraucherinnen und Verbraucher immer schwieriger, die wesentlichen Sicherheitseigenschaften bei digitalen Geräten und Anwendungen zu beurteilen. Das IT-Sicherheitskennzeichen bietet eine Lösung für dieses Problem und schafft mehr Transparenz auf dem digitalen Verbrauchermarkt.

Ein neuer Pfeiler für den Digitalen Verbraucherschutz im BSI

Mit dem IT-Sicherheitsgesetz 2.0 hat das BSI den Auftrag erhalten, ein auf Freiwilligkeit basierendes IT-Sicherheitskennzeichen einzuführen. Seit dem 8. Dezember 2021 kann das Kennzeichen von Herstellern und Diensteanbietern beantragt werden. Um das IT-Sicherheitskennzeichen zu erhalten, verpflichtet sich der Hersteller beziehungsweise Diensteanbieter freiwillig, vom BSI erarbeitete oder vom BSI anerkannte Branchenstandards einzuhalten. Anbieter müssen also bereits bei der Entwicklung neuer Geräte und Anwendungen die entsprechenden Sicherheitsanforderungen berücksichtigen (Security by Design). Diese Sicherheitsstandards unterscheiden sich je nach Produktkategorie, für die ein IT-Sicherheitskennzeichen beantragt werden kann. So gelten beispielsweise die bereits im letzten Berichtsjahr vorgestellten Technischen Richtlinien BSI TR-03148 für Breitbandrouter oder BSI TR-03108 für E-Mail-Dienste. Weitere Produktkategorien sollen zukünftig auf Basis des vom BSI maßgeblich mitentwickelten Standards ETSI EN 303 645 für IoT-Geräte erschlossen werden.

Das IT-Sicherheitskennzeichen

- schafft **Transparenz** für Verbraucherinnen und Verbraucher, da es wichtige Fakten zu den Sicherheitseigenschaften von vernetzten Produkten und Diensten aktuell, verständlich sowie neutral zusammenfasst und auf bestehende Sicherheitslücken hinweist,
- hilft, die Sicherheitseigenschaften von IT-Produkten leichter zu beurteilen und eine **informierte Kaufentscheidung** zu treffen,

- **steigert das Sicherheitsniveau** von IT-Produkten, da Hersteller und Diensteanbieter einen Anreiz erhalten, Sicherheitsstandards bereits in der Entwicklungsphase mitzudenken und die Geräte bei Auslieferung mit einer entsprechenden Standardkonfiguration zu versehen (Security by Design/ Security by Default).

Das IT-Sicherheitskennzeichen platziert damit die Informationssicherheit von Geräten und digitalen Diensten als verbraucherrelevantes Merkmal stärker am Verbrauchermarkt und wird mithin zu einem neuen Pfeiler des Digitalen Verbraucherschutzes in Deutschland.

Dynamische Sicherheitsinformationen: Mehrwert für Verbraucherinnen und Verbraucher

Hat ein Gerät oder eine Anwendung das IT-Sicherheitskennzeichen erhalten, ist der jeweilige Hersteller berechtigt, das Etikett des IT-Sicherheitskennzeichens auf dem Gerät, der Verpackung oder der Herstellerwebseite zu platzieren. Das Etikett enthält einen Kurzlink und einen QR-Code. Verbraucherinnen und Verbraucher gelangen darüber auf die Produktinformationsseite des BSI und erhalten dort relevante Informationen zu Sicherheitseigenschaften des jeweiligen Produkts, die der Hersteller zugesichert hat. Zudem sind auf der Webseite aktuelle, leicht abrufbare Sicherheitsinformationen zu finden, wie beispielsweise Hinweise zu dem BSI bekannten Schwachstellen oder verfügbaren Updates für die mit dem Kennzeichen versehenen Produkte. Das Besondere: Die Informationen sind dynamisch und werden vom BSI nach Erkenntnislage und über die gesamte Laufzeit des IT-Sicherheitskennzeichens – in der Regel zwei Jahre – aktualisiert.

Marktaufsicht für aktiven Verbraucherschutz

Eine technische Prüfung durch das BSI, wie etwa bei einer Zertifizierung, erfolgt im Rahmen der Erteilung des IT-Sicherheitskennzeichens nicht. Während der Laufzeit des IT-Sicherheitskennzeichens kann die nachgelagerte Marktaufsicht eine solche Prüfung anlasslos, beispielsweise stichprobenartig, oder anlassbezogen, beispielsweise bei Bekanntwerden einer Sicherheitslücke, durchführen. Die Erkenntnisse aus der Marktaufsicht fließen in die dynamischen Sicherheitsinformationen auf der Produktinformationseite des BSI ein. Zum verstärkten Schutz der Verbraucherinnen und Verbraucher kann das BSI, insbesondere bei Verstößen gegen Sicherheitsstandards, die Freigabe des IT-Sicherheitskennzeichens widerrufen. Wird das IT-Sicherheitskennzeichen ohne Freigabe durch das BSI verwendet, stellt dies eine Ordnungswidrigkeit dar und kann mit einer Geldbuße von bis zu 500.000 Euro geahndet werden.

Ausblick: Der Weg zu einem europäischen Kennzeichen

Auch wenn es derzeit noch kein einheitliches und verpflichtendes IT-Sicherheitskennzeichen auf EU-Ebene gibt, sieht das BSI das nationale IT-Sicherheitskennzeichen als mögliche Blaupause und ersten Schritt in diese Richtung. Durch die angestrebte Verwendung von europäischen Normen, wie beispielsweise dem IoT-Basisstandard ETSI EN 303 645, arbeitet das BSI bereits jetzt auf einen Gleichklang mit europäischen Standards hin. Mit dem im Juni 2019 in Kraft getretenen Cyber Security Act existiert in der EU ein harmonisiertes Zertifizierungsrahmenwerk, das grundsätzlich auch die Möglichkeit einer europäischen Kennzeichnung eröffnet. Damit stellt der Cyber Security Act ein wichtiges Instrument bei der weiteren Regulierung des Internets der Dinge für den gesamteuropäischen digitalen Binnenmarkt dar. Mit Hilfe des Cyber Resilience Acts, der im vergangenen September angekündigt wurde, könnte ein solches Kennzeichen für die gesamte EU verpflichtend umgesetzt werden.

Allgemeine Hinweise zum IT-Sicherheitskennzeichen:
www.bsi.bund.de/IT-SIK

3 Der digitale Verbrauchermarkt 2021: Sicherheitsvorfälle und Schwerpunkte

Wie im vorherigen Kapitel gezeigt, sind Verbraucherinnen und Verbraucher beim Thema Informationssicherheit weiter in den Fokus gerückt. Neben den wesentlichen Anforderungen der Verbraucherbildung und -information, wie sie beispielsweise mit dem IT-Sicherheitskennzeichen angestrebt werden, bedarf es einer ausführlichen Betrachtung der Informationssicherheitslage von Verbraucherinnen und Verbrauchern. Die nachfolgend dargelegten Sicherheitsrisiken und -vorfälle bieten einen solchen Einblick für das Jahr 2021, können jedoch nicht die Bedrohungslage in ihrer Gänze erfassen.

Nahezu alle Themen aus dem Jahr 2020 ließen sich 2021 fortschreiben. Im Zuge der anhaltenden COVID-19-Pandemie wurden wiederholt zahlreiche Sicherheitslücken in Software von Corona-Testzentren bekannt. Zu den gängigsten Sicherheitsproblemen der Testzentren zählten Schwachstellen in der Zugriffslogik, zum Beispiel durch einfach hochzählbare Identifikationsnummern von Testergebnissen, schwache Passwortvorgaben oder unzureichend gesicherte Programmierschnittstellen (sog. APIs). Exemplarisch ist ein Fall, bei dem mehr als 136.000 Datensätze von getesteten Personen offen im Netz zugänglich waren (vgl. Tagesschau 2021; RBB24 2021).

Um zum Schutz sensibler Gesundheitsdaten beizutragen, verteilte das BSI über seine Meldewege eine Empfehlung zur Informations- und Datensicherheit in Corona-Testzentren und wies auf wesentliche Bestandteile des IT-Grundschutzes hin. Auf diesem Weg sollten Betreiber und Dienstleister der Testzentren sensibilisiert und präventive Maßnahmen gegen häufige Schwachstellen ergriffen werden.

Das Beispiel Smishing: Verbraucherinnen und Verbraucher im Fokus von Cyber-Kriminellen

Auch direkte Cyber-Angriffe auf Verbraucherinnen und Verbraucher blieben eine Herausforderung. Im Februar und Oktober 2021 warnte das BSI vor der erneuten Zunahme von Smishing-Wellen. Die Wortkombination besteht aus dem Nachrichtenservice „SMS“ und „Phishing“, dem Diebstahl von persönlichen Daten über gefälschte Nachrichten oder E-Mails. Hierbei versenden Angreifer massenhaft SMS, beispielsweise angebliche Paketbenachrichtigungen im Namen von Versanddienstleistern. In der SMS werden Empfängerinnen und Empfänger dazu verleitet, einen Link anzuklicken. Dieser verweist in der Regel auf schädliche Android-Apps oder präparierte Webseiten, auf denen weitere Angriffsvektoren genutzt werden. Sofern die Betroffenen das Installieren von Apps aus unbekannten Quellen bestätigen, können anschließend beispielsweise Daten auf dem Endgerät ausgespäht werden. Das stellt eine vollständige Kompromittierung des Geräts dar. Des Weiteren besteht die Möglichkeit, über die Schadsoftware einen erneuten Massenversand von SMS-Nachrichten vom infizierten Endgerät auszulösen. Dabei kann Betroffenen ein finanzieller Schaden durch eventuelle SMS-Entgelte entstehen. Auch andere persönliche Schäden sind nicht auszuschließen. Durch Rückrufe an die infizierte Rufnummer von einer größeren Personenzahl, die eine SMS-Nachricht erhalten hat, kann es zu Beeinträchtigungen und im Extremfall zur Unbenutzbarkeit des mit der Rufnummer verbundenen Endgeräts kommen.

Neben gefälschten Paketbenachrichtigungen per SMS hat das BSI im Laufe des Jahres vor weiteren Betrugsmaschen gewarnt. Hierbei wird Empfängerinnen und Empfängern von Nachrichten beispielsweise vorgetäuscht, dass es sich um eine Anleitung zum Download einer Sprachnachricht oder eine Warnung vor geleakten Privatfotos handele (vgl. Pressemitteilung vom 14.10.2021).

Vishing: Vorsicht vor Voice-Phishing-Anrufen des vermeintlichen IT-Supports!

Eine wiederkehrende Masche wurde auch in diesem Jahr von Kriminellen genutzt: Das Telefon klingelt und am anderen Ende der Leitung drängt ein vermeintlicher Kundensupport darauf, Zugang zum Computer zu erhalten, um ein Sicherheitsproblem zu lösen. Dabei besteht in Wahrheit gar kein IT-Problem – und ein echter Support würde solche Anrufe niemals tätigen. Die Betrügerinnen und Betrüger sitzen häufig in ausländischen Call-Centern und sind darauf aus, per Fernzugriff Schadsoftware auf den Geräten zu installieren. Anschließend verschaffen sie sich Zugang zu sensiblen Daten.

Bereits 2014 warnte das Unternehmen Microsoft vor derartigen Anrufen, bei denen sich Betrüger als Mitarbeiterinnen oder Mitarbeiter ausgaben. Seit Beginn des Jahres 2021 verzeichnen sowohl die Verbraucherschutzvereine als auch das Service-Center des BSI einen erneuten Anstieg von Anfragen und Warnungen zu solchen betrügerischeren Anrufen. Es werden dabei die Namen verschiedener Unternehmen für einen Täuschungsversuch ausgenutzt (vgl. vzbv 2021).

Betrugsmaschen im Kontext des Online-Shoppings greifen einen gesellschaftlichen Trend auf. Die Beliebtheit von Internet- und Versandhändlern unter Verbraucherinnen und Verbrauchern war 2021 weiterhin im Aufschwung. Dies lässt sich unter anderem an den steigenden Umsätzen des Internet- und Versandhandels ablesen (vgl. Statistisches Bundesamt 2021). Daraus ergibt sich, dass sowohl die Angriffsflächen für Kriminelle als auch die Anzahl potenzieller Opfer von Phishing-Attacken steigen. Die breitere Nutzung von Informations- und Warndiensten, wie etwa dem Phishing-Radar der Verbraucherzentrale NRW in Kooperation mit dem BSI, können zum Schutz vor unseriösen Angeboten beitragen (vgl. Verbraucherzentrale NRW 2022).

Hinzu kommen weitere Betrugsformen, die auf Social-Engineering-Techniken zurückgreifen und den Trend zum Online- und Versandhandel ausnutzen. Im Rahmen der andauernden pandemischen Lage nutzten Kriminelle die Herausforderungen bei der Umsetzung von Versand- und Zustellprozessen zu ihren Gunsten aus. So gelangten E-Mails in Umlauf, in denen sich die Angreifer unter anderem als Zollbeamte oder Zustelldienste ausgaben, um die Gebühren für die Zustellung einer Ware über anonyme Zahlungsdienste zu erlangen (vgl. Die Lage der IT-Sicherheit in Deutschland 2021: Seite 24).

Cyber-Angriffe im Rahmen von Aktionstagen im Weihnachtsgeschäft

Das BSI warnte vor einem in diesem Jahr besonders starken Anstieg von cyber-kriminellen DDoS-Aktivitäten im Rahmen von saisonalen Shoppingevents wie dem Black Friday, dem Cyber Monday und dem Weihnachtsgeschäft insgesamt. Anlass zur Sorge bereiteten unter anderem die anhaltende globale DDoS-Schutzgelderpressungskampagne und ein massiver Anstieg von DDoS-Aktivitäten mit Rekordwerten, welche seit August im internationalen Umfeld beobachtet wurden. Bei diesen Aktivitäten wurden neue Rekorde aufgestellt. Beim Angriff auf Microsoft Azure Ende August 2021 wurde der Rekordwert von 2,4 Terabit pro Sekunde (Tbps) erreicht. Beim Angriff gegen Yandex mit dem Meris-Botnetz Ende August 2021 wurde der Rekordwert von 21,8 Millionen Anfragen pro Sekunde (Mrps) erreicht (vgl. bleepingcomputer 2022). Die Bewertung dieser Beobachtungen bestätigte sich, als in Deutschland zwischen dem Black Friday und Cyber Monday ein DDoS-Angriff mit 1,1 Tbps Spitzenbandbreite beobachtet wurde. Das entspricht ungefähr einer Verdoppelung des bisherigen deutschen Jahresrekordwerts. Sowohl bps als auch rps sind gängige DDoS-Angriffsparameter, welche unmittelbar das technische Bedrohungspotenzial von DDoS-Angriffen beschreiben.

Die Pressemitteilung sowie die technischen Daten der Cyber-Sicherheitswarnung finden Sie unter:

Auch auf die besondere Gefahrenlage für Verbraucherinnen und Verbrauchern beim Online-Shopping in den umsatzstarken Monaten machte das BSI aufmerksam. Unter anderem wurden sie über Indikatoren für Fake-Shops sowie sichere Bezahlweisen im Internet aufgeklärt. Diese finden Sie unter https://bsi.bund.de/onlineshopping.

Ransomware: Die Bedrohungslage nimmt weiter zu

Ein besonderes Augenmerk gilt dem Thema Ransomware, bei dem sich ein gleichbleibend hohes Gefahrenniveau zeigt. Unter diesem Begriff werden Schadprogramme verstanden, die den Zugriff auf Daten und Systeme einschränken oder unterbinden. Für die Freigabe wird dann ein Lösegeld (engl.: ransom) verlangt. Häufig werden einige Daten vor der Verschlüsselung von den Tätern ausgeleitet. Diese ausgeleiteten Daten werden anschließend zur Erhöhung des Handlungsdrucks bei den Opfern eingesetzt. Neben der dauerhaften Verschlüsselung der Daten drohen Kriminelle auch mit einer Veröffentlichung oder einem Verkauf der Daten, sollte das Lösegeld nicht gezahlt werden. Die Zahlung des Lösegeldes, das oftmals in einer Kryptowährung wie beispielsweise Bitcoin gefordert wird, gibt jedoch keine Garantie für die Freigabe verschlüsselter Daten und Systeme. Das BSI empfiehlt deshalb, einer Lösegeldforderung nicht nachzukommen und stattdessen sofort Anzeige zu erstatten (vgl. Ransomware: Bedrohungslage, Prävention & Reaktion 2021: Seite 5). Zusätzlich zu den Kosten für die Datenwiederherstellung beziehungsweise -rettung ist in der Regel auch die Bereinigung oder der Neuaufbau des betroffenen kompromittierten Unternehmensnetzwerks zeit- und kostenaufwendig.

Das Aufkommen von Ransomware lässt sich auf Ende der 1990er Jahre datieren, als zum ersten Mal Disketten mit einer derartigen Schadsoftware in Umlauf gebracht wurden (vgl. Kaspersky 2021). Seither entwickeln sich die Angriffe in ihrem Ausmaß und ihren Auswirkungen (Anzahl der Betroffenen, Höhe der Lösegeldforderungen) in eine besorgniserregende Richtung. Neben der zunehmend effektiveren Verbreitung von Schadsoftware beispielsweise durch das Ausnutzen von Sicherheitslücken, wie sie unter anderem durch WannaCry (2017) bekannt wurde, ist die Professionalisierung der Kriminellen eine Bedrohung. So etablieren sich zunehmend Geschäftsmodelle, bei denen Entwicklerinnen und Entwickler ihre Schadsoftware nicht mehr nur selbst anwenden, sondern diese an Dritte weiterverkaufen oder vermieten. Damit zeichnen sich gewisse kriminelle Serviceleistungen im Umgang mit Ransomware ab, die auch unter dem Begriff „Ransomware-as-a-Service“ diskutiert werden. Hierbei werden unter anderem die Ransomware und Anleitungen zur Verwendung an andere Cyber-Kriminelle vermarktet, aber auch die Infrastruktur für die Erpressung wie eine Leak-Seite oder Geldwäschemöglichkeiten. Es ist eine kriminelle Arbeitsteilung entstanden, bei der eine Gruppe etwa den Zugang zu einem kompromittierten Unternehmensnetz verkauft und eine andere die konkrete Ransomware. Der letztliche Angreifer fügt dann mehrere Puzzleteile zusammen (vgl. Ransomware: Bedrohungslage, Prävention & Reaktion 2021: Seite 8 ff.).

Wie stark und in welchem Verhältnis Lösegeldforderungen und -zahlungen seit 2019 gestiegen sind, unterscheidet sich von Quelle zu Quelle (vgl. Financial Crimes Enforcement Network 2021; Unit 42 2021). In jedem Fall konnte jedoch eine Zunahme der Höhe einzelner Lösegeldforderungen beobachtet werden. Das Unternehmen Coveware etwa berichtet quartalsweise über Lösegeldzahlungen aus Vorfällen, die von Coveware begleitet werden. Diese Quartalsberichte geben einen relativen Eindruck, wie die durchschnittliche Höhe der Lösegeldzahlungen angestiegen ist: Zahlten von Coveware betreute Opfer im ersten Quartal 2019 im Schnitt noch 12.700 US-Dollar, waren es im darauffolgenden Jahr bereits 111.600 US-Dollar. Der Anstieg setzte sich auch vergangenes Jahr fort und erreichte im dritten Quartal 2021 durchschnittlich 139.700 US-Dollar. Den durchschnittlichen Höchstwert verzeichnete Coveware ein Jahr zuvor im dritten Quartal 2020 mit 233.800 US-Dollar (vgl. Coveware 2019, 2020, 2020b, 2021).

Ransomware bei Verbraucherinnen und Verbrauchern: Betroffenheit von Einzelpersonen

Lange Zeit richtete sich Ransomware in der Fläche hauptsächlich gegen Individualpersonen. So wurde die Schadsoftware unter anderem über Spam-Mails direkt verbreitet, statt Teil einer längeren Infektionskette zu sein, wie es jetzt häufig beobachtet wird. Cyber-Kriminelle erpressten so vergleichsweise kleine Summen an Lösegeld von einer großen Anzahl an Betroffenen.

Für einen gemeinsamen Forschungsbericht von Malwarebytes, Digitunity und dem Cybercrime Support Network wurden vom 21. Juli bis zum 9. August 2021 insgesamt 5.000 Personen aus den Vereinigten Staaten, dem Vereinigten Königreich und Deutschland zu Themen der privaten IT-Sicherheit befragt. Zur Frage, welche verdächtigen Aktivitäten die Befragten selbst in ihrer Vergangenheit erlebt haben, gaben 16 Prozent aller Befragten an, bereits Opfer eines Ransomware-Angriff geworden zu sein, wobei hier vorwiegend Personen im Alter über 35 Jahren betroffen waren (vgl. Malwarebytes 2021).

Es ist anzunehmen, dass der Angriff auf eine breite Masse von Menschen mit Hilfe von Ransomware in der derzeitigen Lage keine Hauptangriffstechnik von Cyber-Kriminellen mehr ist. Jedoch kann von einer nicht unerheblichen Dunkelziffer an Vorfällen ausgegangen werden, die teilweise private Endgeräte sowie den privaten Lebensbereich von Verbraucherinnen und Verbrauchern betreffen. Eine Aufklärung über das Thema Ransomware ist weiterhin ein wesentlicher Bestandteil der Verbraucherbildung und wird vom BSI unter anderem durch aktuelle Formate wie den Podcast „Update verfügbar“ (vgl. Episode 14 und 15) oder den wöchentlich erscheinenden BürgerCERT-Newsletter umgesetzt.

Zum Botschafter für (mehr) Cyber-Sicherheit werden!

Nutzen Sie als öffentliche Organisation oder auch Unternehmen die kreativen Motive und Inhalte unserer aktuellen Informations- und Sensibilisierungskampagne: Unter www.einfachaBSIchern.de finden Sie zum Download ein „Digitales Informationspaket (DIP)“. Dort enthalten sind die vielfältigen Kampagnenmotive als druckfähige Plakate in verschiedenen Größen oder auch als Onlinebanner zum Einbinden auf Webpräsenzen. Werden Sie für die Verbraucherinnen und Verbraucher zum Botschafter für (mehr) Cyber-Sicherheit.

Ransomware bei Herstellern und Dienstleistern: Erhebliche Schäden auch für Verbraucherinnen und Verbraucher

Seit 2017 beobachtet das BSI, dass Ransomware-Gruppen zunehmend Organisationen als Opfer auswählen, denen sie eine möglichst hohe Lösegeldsumme abverlangen können. Diese Vorgehensweise wird unter dem Namen Big Game Hunting, dem englischen Begriff für Großwildjagd, diskutiert und analysiert. Das Phänomen ist branchen- und länderübergreifend zu beobachten. Im Falle eines erfolgreichen Ransomware-Angriffs hat dieses Vorgehen ein enormes Schadenspotenzial für die Lieferketten und Dienstleistungen von Unternehmen, die oft auch auf Verbraucherinnen und Verbraucher durchschlagen. Nahezu alle digitalen Dienstleistungen für eine größere Zielgruppe sind auf die Funktionalitäten von Datenbanken angewiesen. Gerade deshalb sind diese ein beliebtes Angriffsziel für Cyber-Kriminelle, welche die Daten zu ihren Zwecken abrufen und anschließend die Systeme der Opfer verschlüsseln. Besonders erschreckend sind Angriffe auf Kundendatenbanken, da die hinterlegten Informationen außerhalb des Einflussbereichs der betroffenen Verbraucherinnen und Verbrauchern liegen. Kommt es zum Ransomware-Angriff mit Datenabfluss in einer Organisation, sind Verbraucherinnen und Verbraucher diesem hilflos ausgesetzt. Hier ist eine schnelle Reaktion der jeweiligen Unternehmen zur Schadensbegrenzung notwendig, zum Beispiel mittels Verbraucherinformation und Hilfestellungen für Kundinnen und Kunden, um den Schaden gering zu halten.

Das BSI hat weiterführende Informationen zum Thema Ransomware sowie konkrete Hilfen für die Prävention und die Reaktion im Schadensfall in Ihrer Institution zusammengestellt. Sie finden diese in unserer Publikation Ransomware: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall.

Im Mai 2021 stand das BSI in Kontakt mit einem deutschen Lebensmittel-Einzelhändler, der von einem Ransomware-Angriff mit anschließendem Datenleak betroffen war. Der Vorfall hatte zur Folge, dass sämtliche IT-Netzwerksysteme des Unternehmens gemäß einem Notfallplan heruntergefahren wurden. Unter anderem waren Warenwirtschaftsprogramme der Logistik betroffen, was zu Engpässen in der Warenverfügbarkeit führte. Im weiteren Verlauf der Vorfallsbearbeitung wurde bekannt, dass Daten aus Kundenbindungsprogrammen des Unternehmens im Darknet veröffentlicht wurden. Das Unternehmen reagierte auf die Schadenslage, indem Kundinnen und Kunden über den Vorfall informiert und deren Passwörter zurückgesetzt wurden. Des Weiteren hat das Unternehmen zusätzliche Maßnahmen zur Stärkung der Informationssicherheit sowie zum Schutz von Kundendaten angekündigt (vgl. hessenschau 2021).

Eine deutsche Elektronik-Fachmarktkette wurde Anfang November Opfer eines Ransomware-Angriffs der Gruppe Hive. Hier wurden laut Medienberichten mindestens 3.100 Server lahmgelegt und eine Lösegeldsumme von über 240 Millionen US-Dollar gefordert. Auch in diesem Fall waren Warenwirtschaftssysteme und teilweise Kassen betroffen. Dienstleistungen in den Filialen – wie Warenbestellungen, Rückgaben oder Abholungen – waren für Verbraucherinnen und Verbraucher nicht oder nur eingeschränkt nutzbar. Zwar sind nach bisherigen Erkenntnissen keine Kundendaten abgeflossen, der Vorfall zeigt jedoch die mögliche Tragweite einer sekundären Betroffenheit von Verbraucherinnen und Verbrauchern bei Ransomware-Attacken (vgl. Golem 2021).

Im Oktober 2021 gab ein internationaler Reisekonzern per Pressemitteilung bekannt, Opfer eines Cyber-Angriffs geworden zu sein. Die zuständigen Stellen identifizierten einen Ransomware-Angriff der Hacker-Gruppe Conti. Eine Systemverschlüsselung machte das Unternehmen nahezu geschäftsuntüchtig. Recherchen bestätigten, dass die verdächtigte Ransomware-Conti-Gruppe auf ihrer Darknet-Seite einen Teil der entwendeten Daten veröffentlicht hatte. Bei den Daten handelte es sich um Reisepässe, welche bei einer Tochtergesellschaft exfiltriert worden waren. Infolgedessen informierte der Konzern die betroffenen Verbraucherinnen und Verbraucher darüber, dass die Täter oder Dritte die Kopie des Reisepasses als Vorlage nutzen könnten, um rechtswidrig gefälschte Ausweiskopien zu erstellen, oder mit der Kopie des Reisepasses Identitätsdiebstahl begehen könnten. Ihnen wurde empfohlen, hinsichtlich möglicher Versuche von Phishing, Identitätsdiebstahl und Betrug besonders wachsam zu sein (vgl. t3n – digital pioneers 2021).

Die geschilderten Vorfälle aus der Wirtschaft stehen beispielhaft für die zunehmenden Ransomware-Angriffe. Sie verdeutlichen, dass in vielen Fällen Verbraucherinnen und

Verbraucher mittelbare Betroffene eines solchen Angriffs werden können, wenn Kundendaten entwendet werden, Produkte und Dienstleistungen nur eingeschränkt oder gar nicht funktionieren.

Das Jahr 2021 hat darüber hinaus gezeigt, dass auch Institutionen im öffentlichen Sektor sowie soziale Einrichtungen nicht von Angriffen Cyber-Krimineller verschont blieben. Mehrere Kommunen und Landkreise wurden Opfer von Cyber-Angriffen, welche den Ausfall von Dienstleistungen für Bürgerinnen und Bürger zur Folge hatten. Besonders der Angriff auf eine Landkreisverwaltung im Juli 2021 erreichte eine besorgniserregende Tragweite, die in der Ausrufung des Katastrophenfalls mündete. Die betroffene Verwaltung war über mehrere Wochen nicht arbeitsfähig, sodass auch Verwaltungsdienstleistungen für Bürgerinnen und Bürger nicht zur Verfügung standen.

Lösungsansätze: Die Zusammenarbeit von Staat, Wirtschaft und Gesellschaft

Im Rahmen des IT-Sicherheitsgesetzes 2.0 hat der Gesetzgeber eine intensivere Zusammenarbeit zum Schutz von Verbraucherinnen und Verbrauchern als einen zusätzlichen Schwerpunkt des BSI verankert. Dazu heißt es:

> *Aufnahme eines kontinuierlichen Verbraucherschutzdialogs zwischen BSI, Herstellern und Diensteanbietern, um einen frühzeitigen und steten Austausch zur Realisierung eines höchstmöglichen Schutzniveaus der IT-Sicherheit bei Verbraucherprodukten zu erreichen. Hierzu nutzt das BSI seine Erfahrungen aus der Marktbeobachtung, den Sicherheitstests und -analysen sowie dem Dialog mit den übrigen, im Verbraucherschutz tätigen Akteuren.*
>
> *(IT-SiG 2.0, Bundesrat Drucksache 16/21 vom 01.01.2021, S.65)*

Das übergeordnete Ziel ist die Realisierung eines höchstmöglichen Schutzniveaus für Verbraucherprodukte. Die Interpretation der Aufgabenstellung lässt auf folgende Punkte schließen: Der Verbraucherschutzdialog ist als eine regelmäßige Daueraufgabe für das BSI anzusehen. Es ist eine Kommunikation vom BSI mit den Herstellern und Diensteanbietern aufzubauen und sicherzustellen, dass diese in beide Richtungen funktioniert – von Unternehmen zum BSI und umgekehrt. Dies beinhaltet sowohl eine frühzeitige anlassbezogene Kommunikation als auch die Aufgabe, einen Kanal für den kontinuierlichen Austausch ohne konkreten Anlass aufzubauen und bereitzustellen. Die im Verbraucherschutz tätigen Akteure sind einzubeziehen. Sachlich und fachlich kann dies nur sinnvoll funktionieren, wenn die vorhandenen Strukturen und Kompetenzen des BSI eingebracht werden. Mit der Zusammenarbeit auf freiwilliger Basis tragen Unternehmen und das BSI gemeinsam dazu bei, die Cyber-Sicherheit für Verbraucherinnen und Verbraucher in Deutschland zu stärken.

Datenleaks sind die Folge mangelhafter Informationssicherheit. Im Vergleich zum vorherigen Berichtszeitraum hat sich gezeigt, dass vor allem die unzureichende Umsetzung des „Security by Design“-Prinzips und fehlende Update-Policies zu diesem Risiko beitragen. Des Weiteren besitzen Institutionen häufig einen nur unzureichenden Überblick über ihre eigene Infrastruktur sowie die enthaltenen Softwarekomponenten. Einen Lösungsansatz für dieses Problem bietet die "Software Bill of Materials", welche eine Übersicht über alle verwendeten Software-Komponenten eines Produkts darstellt. Gleichermaßen ist eine Übersicht über alle im Unternehmen verwendeten Softwareprodukte sinnvoll, damit auf bekannt gewordene Schwachstellen zeitnah reagiert werden kann. Im Sinne eines ganzheitlichen digitalen Verbraucherschutzes tritt das BSI gegenüber Herstellern und Anbietern für die Verbraucherbelange und die Sicherstellung von Informationssicherheit ein. Hierbei wird gegenüber Institutionen stetig die Umsetzung des IT-Grundschutzes empfohlen. Zudem werden weiterführende Sicherheitsempfehlungen zur Härtung der – teils branchenspezifischen – Infrastruktur zur Verfügung gestellt.

Die dargelegten Sicherheitsvorfälle und Schwachstellen stellen nur eine exemplarische Auswahl der Gefahren dar, denen Verbraucherinnen und Verbraucher, direkt und indirekt, im alltäglichen digitalen Umfeld ausgesetzt sind.

Kommunikation ist ein wesentlicher Schlüssel, um Gefahren der digitalen Welt zu begegnen. Dies gilt einerseits für die Aufklärung über potentielle Risiken der Digitalisierung sowie die Unterstützung von Verbraucherinnen und Verbrauchern mit Maßnahmen und Empfehlungen zur sicheren Nutzung digitaler Angebote. Andererseits betrifft dies die klare Kommunikation mit Verbraucherinnen und Verbrauchern bei Eintreten eines Sicherheitsvorfalls. So wird betroffenen Personen die Hilfe zur Selbsthilfe ermöglicht, zum Beispiel durch das Ändern von Passwörtern oder das Überprüfen von Zahlungsdaten und -vorgängen.

4 Fokusthema: Digitaler Verbraucherschutz im Automobilbereich

Die Digitalisierung nimmt im Automobilbereich kräftig an Fahrt auf. Moderne Fahrzeugmodelle verfügen mittlerweile über zahlreiche Funktionen, die auf eine Vernetzung beziehungsweise externe Datenverbindungen angewiesen sind. Es ist davon auszugehen, dass sich das Angebot an solchen Funktionen und darauf aufbauenden Dienstleistungen (auch von Drittanbietern) in den nächsten Jahren vervielfältigen wird. Damit wird das Fahrzeug nicht nur zum Empfänger, sondern zu einer Quelle von Daten und Informationen unterschiedlichster Art. Erfasst und zur Verfügung gestellt lassen sich diese zum Beispiel von externen Service-Anbietern für Dienstleistungen nutzen.

Vernetzte Fahrzeuge

Das Interesse der Verbraucherinnen und Verbraucher an solchen Angeboten ist vorhanden, fällt aber je nach Datenverwendung unterschiedlich aus. Zu dieser Erkenntnis kommt der TÜV-Verband in einer repräsentativen Umfrage aus dem Jahr 2020. Demnach würden 43 Prozent der Befragten einer Datenauswertung in einem voll- oder teilautomatisierten Fahrzeug zustimmen, wenn die Daten für die Verbesserung der Verkehrssicherheit genutzt werden. 41 Prozent würden es akzeptieren, wenn Daten der Aufklärung von Unfällen dienten, und 35 Prozent stimmten noch einer Auswertung zum Zwecke der Verbesserung der technischen Fahrzeugsicherheit zu. Nur 12 Prozent lehnen eine Speicherung und Auswertung von Daten generell ab. 18 Prozent aller Befragten haben sich dazu noch keine Meinung gebildet (vgl. TÜV-Verband 2020).

Für einen besseren Überblick und eine erste Systematisierung kategorisiert die Verbraucherzentrale Nordrhein-Westfalen datenbasierte Dienstleistungen im Fahrzeug wie folgt (vgl. Verbraucherzentrale NRW 2017):

- **Information:** Abruf von Kraftstoffpreisen, Hotelpreisen in der Umgebung oder E-Mails.
- **Entertainment:** Musik-Streaming, Videochats.
- **Fahrassistenzsysteme:** Warnung vor kritischen Verkehrssituationen und Gefahrenstellen, E-Call.
- **Dynamische Navigation:** Echtzeitverkehrsmeldungen, Informationen über freie Parkplätze und Geschwindigkeitsbegrenzungen.
- **Fahrzeug-/Wartungsmanagement:** Überwachung des Fahrzeugzustandes und Ferndiagnose im Pannenfall.

Darüber hinaus lassen sich im Fahrzeug anfallende Daten für die bereits oben erwähnte Analyse und Aufklärung von Unfällen verwenden, aber auch für Telematik-Versicherungstarife (vgl. Verbraucherzentrale NRW 2021b), für gesetzliche Zwecke wie Hauptuntersuchungen oder für die Forschung. Die Vernetzung ermöglicht es außerdem, Software-Updates zur Freischaltung neuer Funktionen oder zum Schließen von Sicherheitslücken per Funk (Over-the-Air-Updates) durchzuführen. Durch schnelle und skalierbare Updates seitens der Hersteller lassen sich bei Rückrufen in bestimmten Fällen aufwendige Werkstattbesuche für die Verbraucherinnen und Verbraucher vermeiden.

Alle oben genannten Funktionen und Dienstleistungen machen eine Betrachtung der Informationssicherheit erforderlich. Neben den grundsätzlichen Fragen der Datensicherheit, die auch in anderen Digitalisierungsbereichen von hoher Relevanz sind, kommt hierbei der Aspekt der Funktionssicherheit hinzu. Datenschnittstellen dürfen nicht zu einem Einfallstor für Cyberangriffe werden, die die Verkehrssicherheit gefährden. Dabei stellt der Schutz eines komplexen technischen Systems – wie eines Fahrzeugs – mit einer Vielzahl von Komponenten und internen wie externen Schnittstellen eine besondere Herausforderung dar.

> *Aktuelle Entwicklungen bei der Cybersicherheit in der Automobilbranche werden dabei regelmäßig durch das BSI im Branchenlagebild Automotive veröffentlicht.*
> *(vgl. BSI 2021, https://bsi.bund.de/dok/automotive)*

Den Bedarf an Maßnahmen für die Informationssicherheit hat auch der Gesetzgeber mit entsprechenden Regulierungsmaßnahmen aufgegriffen. Die United Nations Economic Commission for Europe (UNECE) hat 2020 Vorgaben zur Cyber-Sicherheit in der Typgenehmigung von Kraftfahrzeugen verabschiedet (vgl. UNECE 2021). Diese Regelungen sind ab Mitte 2022 durch Übernahme in EU-Recht auch in Deutschland verbindlich vorgeschrieben. Im Sinne einer ganzheitlichen Betrachtung über den Nutzungszyklus eines Fahrzeugmodells wird zunächst ein Cyber-Security-Management-System (CSMS) beim Hersteller gefordert. Dieses soll die Entwicklung, Produktion und Nutzung des Fahrzeugs abdecken sowie eine Vor- und Nachsorge in Bezug auf die Cyber-Sicherheit ermöglichen. Zur Umsetzung lässt sich der einschlägige ISO-Standard ISO/SAE 21434 heranziehen. Bereits bei der Fahrzeugentwicklung ist eine umfassende Risikobetrachtung gefordert. Bezogen auf den Fahrzeugtyp selbst müssen je nach Ergebnis der Risikobetrachtung angemessene technische Maßnahmen zur Verhinderung von Cyber-Angriffen getroffen werden.

Künstliche Intelligenz im Fahrzeug - Angriffe auf Sensorik und Bewertung

Zur Automatisierung von Fahrfunktionen kommen zunehmend Technologien wie Künstliche Intelligenz (KI) zum Einsatz. Diese KI-Systeme nutzen Eingabedaten, die zum Beispiel aus optischen Sensoren (unter anderem Kameras) stammen. Damit lassen sich unterschiedliche Funktionalitäten, wie zum Beispiel die Klassifikation von Verkehrsschildern oder die Detektion von Fußgängern, umsetzen. Die Ausgabe dieser KI-Systeme wird dann für die Steuerung von Lenkung, Bremse und Gaspedal genutzt. Auf dieser Basis lassen sich auch komplexe Fahrmanöver vornehmen, wie das Umfahren eines Hindernisses.

Den vielfältigen Möglichkeiten in der Automatisierung von Fahrfunktionen durch KI-Systeme stehen eine Reihe von Herausforderungen gegenüber. Für einen sicheren und robusten Einsatz von KI in Fahrzeugen sind gerade bei der IT-Sicherheit zahlreiche Besonderheiten zu berücksichtigen. Daher stellt das BSI mit der Publikation „Sicherer, robuster und nachvollziehbarer Einsatz von KI“ einen Überblick neuartiger Angriffe zur Verfügung. Kommt es beispielsweise im Trainingsprozess eines KI-Systems zu einer Manipulation der zugrundeliegenden Daten, dann handelt es sich um einen sogenannten Poisoning-Angriff. Die Wahrscheinlichkeit für einen erfolgreichen Angriff erhöht sich noch, wenn Daten oder bereits vortrainierte Modelle aus externen Quellen Verwendung finden. Auch im Betrieb des KI-Systems sind bei der Implementierung weitere Gefahren zu berücksichtigen, wie etwa gezielte Falscheingaben – sogenannte adversariale Angriffe. Ein Beispiel dafür sind Manipulationen an Verkehrsschildern, die durch das System falsch erkannt werden. Beide Arten von Angriffen können die KI-Systeme zu Fehlentscheidungen mit potenziell gravierenden Auswirkungen verleiten (vgl. ebenda).

KI-Systeme müssen weiterhin auch im Normalbetrieb unter unterschiedlichen oder sogar beliebigen Umweltbedingungen robust funktionieren, insbesondere auf höheren Automatisierungsstufen. Die komplexe Herausforderung dabei ist, dass Umweltbedingungen je nach Tages-, Nacht- oder Jahreszeit, Klima, Witterung, Straßenbelag und Umgebung stark variieren können. Auch mit sehr unterschiedlichem Lichteinfall und Reflexionen sowie mit teilweise verdeckter Sicht oder Beschädigungen (zum Beispiel von Verkehrsschildern) muss das KI-System zuverlässig umgehen können.

Auch bei Verschmutzung oder Beschädigung der Fahrzeugsensoren müssen die Systeme weiter robust arbeiten oder die Beeinträchtigungen rechtzeitig erkennen. Darüber hinaus lassen sich auch die Sensoren selbst angreifen. Vergleichsweise einfach kann dies beispielsweise mit einem Störsender (Jamming) erfolgen, um so die Bereitstellung der Umgebungsinformationen zu unterbinden. Der Sensorik können aber auch gezielt falsche Objekte vorgespiegelt werden (Spoofing). Drucke etwa, wie auf T-Shirts oder Häusern, lassen sich bewusst so gestalten, dass die Sensorik sie als Verkehrszeichen erkennt.

Kooperation mit dem Kraftfahrt-Bundesamt

Die zunehmende Digitalisierung des Automobilbereichs und die internationalen Aktivitäten zur Cyber-Sicherheit in Fahrzeugen auf Ebene der UNECE waren für das BSI und das Kraftfahrt-Bundesamt (KBA) Anlass, ihre Zusammenarbeit zu intensivieren. Im Oktober 2020 haben das BSI und das KBA daher eine Verwaltungsvereinbarung zur Zusammenarbeit im Bereich der Cyber-Sicherheit von Kraftfahrzeugen geschlossen. Das BSI unterstützt das KBA

Kraftfahrt-Bundesamt, Dienstsitz Flensburg

bei den Prozessen zur Typgenehmigung nach den neuen UNECE-Regelungen. Die ersten Verfahren zur Zertifizierung der Cyber-Security-Management-Systeme (CSMS) nach UNECE R155 (vgl. UNECE 2021) sowie der Software-Update-Management-Systeme (SUMS) nach UNECE R156 (vgl. UNECE 2021b) bei den Herstellern wurden vom BSI begleitet.

Das KBA ist die zuständige Marktüberwachungsbehörde, insbesondere für Kraftfahrzeuge und Kraftfahrzeuganhänger sowie Systeme, Bauteile und selbstständige technische Einheiten für diese Fahrzeuge. Ziel der Marktüberwachung ist der Schutz öffentlicher Interessen wie Gesundheit, Sicherheit und Umwelt. Einen wesentlichen Bestandteil bilden Produktprüfungen, die in gesetzlich vorgeschriebenem Umfang jährlich durchgeführt werden. Diese können auch bei konkretem Anlass – wie Hinweisen auf mögliche Mängel durch Dritte – erfolgen. Das BSI unterstützt im Rahmen der Verwaltungsvereinbarung das KBA ebenfalls bei Fragen der Cyber-Sicherheit in der Marktüberwachung. Derzeit werden die dafür erforderlichen gemeinsamen Prozesse für Cyber-Sicherheitsprüfungen in der Marktüberwachung abgestimmt. Dazu gehört die Bewertung von entdeckten und gemeldeten Schwachstellen sowie der notwendigen Abhilfemaßnahmen durch den Hersteller. Prüfobjekte im Fahrzeug und dazugehörige durchführbare Tests sind ebenso Inhalt der gemeinsamen Überlegungen. Konkret bereitet das BSI derzeit im Rahmen eines Projekts einen Leitfaden für Penetrationstests an Fahrzeugen vor, der auch in der Marktüberwachung zum Einsatz kommen kann und voraussichtlich 2023 fertiggestellt sein wird.

Gesetz zum autonomen Fahren

Am 21. Juni 2021 ist das Gesetz zum autonomen Fahren in Kraft getreten. Es ermöglicht den Einsatz von fahrerlosen Kraftfahrzeugen der Stufe 4 (siehe Abbildung: „Stufenmodell: Automatisierung von Fahrfunktionen“) in festgelegten Betriebsbereichen des öffentlichen Straßenverkehrs. Das Gesetz zielt in erster Linie auf autonome Shuttle-Dienste und sogenannte People-Mover ab, die Personen auf festgelegten Routen befördern. Es ist hierfür eine technische Aufsicht vorgeschrieben, die den Betrieb überwacht und gegebenenfalls alternative Fahrmanöver freigeben oder das autonome System deaktivieren kann. Im Gesetz werden unter anderem Anforderungen an die technische Beschaffenheit und Ausrüstung sowie Pflichten an die Beteiligten beim Betrieb der Systeme formuliert. Die Informationssicherheit der elektronischen Architektur und der erforderlichen Funkverbindungen wird explizit gefordert. In diesem Zusammenhang ist vom Betreiber unter anderem eine Risikobeurteilung des Systems zu erstellen. Außerdem besteht die Verpflichtung, erkannte Manipulationen und unerlaubte Zugriffsversuche an das KBA zu melden. Darüber hinaus sind im Gesetz Regelungen zur Prüfung und Erteilung der Betriebserlaubnis durch das KBA sowie zur Datenverarbeitung beim Betrieb der Fahrzeuge enthalten. Im Hinblick auf die Informationssicherheit wirkt das BSI bei der Erstellung, Umsetzung und Weiterentwicklung sowie bei der Bewertung der technischen Anforderungen mit.

Der Digitale Verbraucherschutz ist gefordert

Für den Digitalen Verbraucherschutz im BSI ist das Thema Automotive von sehr hoher Relevanz. Es lassen sich eine ganze Reihe von Themen ableiten, schon heute, aber vor allem auch zukünftig, die Schnittstelle von Informationssicherheit und Verbraucherschutz intensiv zu bearbeiten. Ob Sicherheits-Updates, die technischen Dimensionen des Datenschutzes oder KI-Fragestellungen – die Liste an Themenschwerpunkten ist lang:

Die neue UNECE-Regelung UNR155 ist ein wichtiger Schritt, um das Thema Cyber-Sicherheit im Fahrzeug zu verankern. Die Hersteller sollen hiernach zukünftig verpflichtet werden, die Informationssicherheit ihrer Produkte nachzuweisen und über den Nutzungszyklus hinweg zu gewährleisten. Neu entdeckte Schwachstellen und Vorfälle lassen sich auch dadurch nicht in Gänze verhindern. Mit den Vorgaben werden aber die organisatorischen und technischen Voraussetzungen geschaffen, auf solche Umstände zu reagieren und Schwachstellen schnell beheben zu können. Einen wesentlichen Baustein bilden dabei Software-Updates per drahtloser Verbindung.

Das BSI erachtet die dauerhafte Verfügbarkeit von sicherheitsrelevanten Updates als notwendig. Mit einem Durchschnittsalter von 9,8 Jahren aller zugelassenen Pkw (Stichtag: 1. Januar 2021) wird die besondere Relevanz allein für Deutschland deutlich (vgl. Kraftfahrt-Bundesamt 2021). Beispielsweise ist davon auszugehen, dass heute eingesetzte kryptographische Verfahren beziehungsweise Schlüssellängen durch stetige Fortschritte in der Kryptoanalyse langfristig nicht mehr ausreichend sind. Dieser sogenannte Kryptoverschleiß kann auf die gesamte elektrisch-elektronische Architektur (unter anderem das Bordnetzwerk mit den Kommunikationsbussen, Schnittstellen und elektronischen Steuereinheiten) des Fahrzeugs Auswirkungen haben. Zukünftige Youngtimer (20 bis 30 Jahre alte Fahrzeuge mit wenig Jahreslaufleistung, vgl. ADAC 2019) mit hochautomatisierten Fahrfunktionen können hier besonders betroffen sein. Die Tatsache, dass allein in Deutschland mehr als 18 Prozent des Fahrzeugbestands älter als 15 Jahre sind, verdeutlicht die Notwendigkeit für dauerhaft verfügbare Software-Updates (vgl. Kraftfahrt-Bundesamt 2021b). Die Verkehrssicherheit bildet dabei den Schwerpunkt, aber auch die ökologische Nachhaltigkeit von IT-Produkten spielt in der Betrachtung eine Rolle.

Für eine langfristige sichere Nutzbarkeit und die damit verbundene Reduzierung von Neuanschaffungen sind Sicherheits-Updates eine wichtige Voraussetzung zur Vermeidung unnötigen Ressourcenverbrauchs. Neben der ökologischen ist ebenso die wirtschaftliche Nachhaltigkeit zu betrachten.
Ein Fahrzeug muss auch hardwaretechnisch in der Lage sein, langfristig zur Verfügung gestellte Updates zu verarbeiten. Ist das nicht sichergestellt, dann müsste unter Umständen Hardware getauscht werden, deren Finanzierung nicht geklärt ist. Hier braucht es einheitliche und verbindliche Vorgaben, wozu auch die seit dem 1. Januar 2022 gültige Umsetzung der Warenkauf- und Digitale-Inhalte-Richtlinien in deutsches Recht beitragen könnte. In diesen wird erstmals eine Aktualisierungspflicht für „Digitale Inhalte" und „Waren mit digitalen Elementen“ geregelt. Konkrete Fristen für diese Verpflichtung werden nicht festgelegt, sondern auf einen Bereitstellungszeitraum beziehungsweise für die Verbraucherinnen und Verbraucher erwartbaren Zeitraum abgestellt.

Der Schutz der Daten der Verkehrsteilnehmerinnen und Verkehrsteilnehmer ist von großer Bedeutung. Fahrzeughersteller und berechtigte Dritte müssen entsprechend der einschlägigen Vorgaben Transparenz darüber schaffen, wer die im vernetzten Fahrzeug anfallenden (personenbezogenen) Daten verwendet beziehungsweise wofür diese verwendet werden. Fahrzeugnutzerinnen und Fahrzeugnutzer müssen eine einfache Möglichkeit haben, unerwünschte Datenabfragen technisch wirksam zu verhindern. Umgekehrt sollte Diensteanbietern und Betreibern, soweit von den Verbraucherinnen und Verbrauchern aktiv gewährt, ein fairer Zugang zu den Daten ermöglicht werden. Damit lässt sich die Entwicklung von Anwendungen zur Verbesserung der Verkehrssicherheit und -effizienz ermöglichen. Hierfür werden momentan in der Branche unterschiedliche Ansätze für den Datenzugriff diskutiert, mit denen sich die verschiedenen Anforderungen im Hinblick auf Datenschutz, Informationssicherheit und fairen Zugang vereinen lassen.

Ein weiterer Punkt, der unter Umständen bei Verbraucherinnen und Verbrauchern für Verunsicherung sorgt, ist der Einsatz von KI unter anderem auch beim automatisierten Fahren. Wesentliche Ansatzpunkte bestehen hier in der Aufklärung im Umgang mit diesen Unsicherheiten. Nach einer Umfrage für die Mobility-Studie 2020 des TÜV-Verbandes sind 88 Prozent der Befragten (eher) der Ansicht, dass die Sicherheit und Funktionsfähigkeit von Fahrzeugen mit Künstlicher Intelligenz regelmäßig überprüft werden muss. 42 Prozent der Teilnehmenden halten eine jährliche Prüfung für sinnvoll, weitere zehn Prozent sprechen sich für eine monatliche Prüfung aus und 15 Prozent sind der Ansicht, dass sogar eine permanente Prüfung in Echtzeit angebracht ist (vgl. TÜV-Verband 2020). Im Regelbetrieb sind in Deutschland nach jetzigem Stand Systeme bis zur Stufe 3 (vgl. Grafik Seite 29) im Einsatz. Beim Erwerb eines Fahrzeugs mit automatisierten Fahrfunktionen sollten Verbraucherinnen und Verbraucher in Anlehnung an die beschriebene Skala präzise Informationen einholen, unter welchen Bedingungen welche Funktionen im Fahrzeug automatisiert ablaufen. Diese Informationen sind bei der Nutzung des Fahrzeugs unbedingt zu berücksichtigen. Verbraucherinnen und Verbraucher sollten sich bewusst sein, dass Fahrzeughersteller in ihren Produktbeschreibungen teilweise eigene Begriffe verwenden, die dazu verleiten können, von den Fahrzeugen einen höheren Grad an Automatisierung zu erwarten, als diese tatsächlich aufweisen.

Stufenmodell zum automatisierten Fahren

Bereits 2014 hat die Society of Automotive Engineers (SAE) ein Dokument (SAE J3016) mit Definitionen zur Automatisierung von Fahrfunktionen erstellt (vgl. ebenda). Dies soll einem einheitlichen Begriffsverständnis dienen sowie eine strukturierte Herangehensweise auf dem Weg zum vollautomatisierten Fahren ermöglichen. Dieses Dokument ist seitdem viel beachtet worden. Darin wird die Automatisierung von Fahrfunktionen anhand einer Skala mit fünf Stufen beschrieben:

In den Stufen 1 und 2 werden dabei die Lenkung und Beschleunigung des Fahrzeugs automatisiert. In Stufe 1 (Assistenzsysteme) betrifft dies nur eine dieser Funktionen, in Stufe 2 (Teilautomatisierung) hingegen beide. In Stufe 3 (Bedingte Automatisierung) übernimmt ein automatisiertes System alle Teile der Fahraufgabe, der Fahrer oder die Fahrerin muss jedoch bei Bedarf eingreifen. Die folgende Stufe 4 (Hochautomatisierung) erweitert Stufe 3 dahingehend, dass ein Eingreifen durch die Fahrerin oder den Fahrer nicht mehr erforderlich ist. Den Stufen 1 bis 4 ist gemein, dass die Automatisierung der Fahrfunktionen nur in bestimmten Fahrsituationen erfolgt. Dies kann zum Beispiel das Fahren mit niedriger Geschwindigkeit und bei guter Witterung auf der Autobahn sein. In der finalen Stufe 5 (Vollautomatisierung) sind schließlich ohne Einschränkung der Fahrsituation alle Teile der Fahraufgabe automatisiert.

In Ergänzung zum Stufenmodell der SAE hat die Bundesanstalt für Straßenwesen eine vereinfachte Abstufung in einen Assistierten Modus (Stufe 1 und 2), Automatisierten Modus (Stufe 3) und Autonomen Modus (Stufen 4 und 5) vorgenommen, die insbesondere in der Regulierung eine Rolle spielt (vgl. Bundesanstalt für Straßenwesen 2021).

Automatisierungsgrade des automatisierten Fahrens

STUFE 0	STUFE 1	STUFE 2	STUFE 3	STUFE 4	STUFE 5
Keine Automatisierung	Assistiert	Teilautomatisiert	Bedingt automatisiert	Hochautomatisiert	Vollautomatisiert
Fahrer führt dauerhaft Längs- **und** Querführung* aus.	Fahrer führt dauerhaft Längs- **oder** Querführung* aus.	Fahrer **muss** das System **dauerhaft** überwachen.	Fahrer **muss** das System **nicht** mehr **dauerhaft** überwachen. Fahrer muss potenziell in der Lage sein zu übernehmen.	Kein Fahrer erforderlich im spezifischen Anwendungsfall.	**Von „Start" bis „Ziel"** ist kein Fahrer erforderlich.
Kein eingreifendes Fahrzeugsystem aktiv.	System übernimmt die jeweils andere Funktion.	System übernimmt Längs- **und** Querführung* in einem spezifischen Anwendungsfall**.	System übernimmt Längs- und Querführung* in einem spezifischen Anwendungsfall**. Es erkennt Systemgrenzen und fordert den Fahrer zur Übernahme mit ausreichender Zeitreserve auf.	System **kann im spezifischen Anwendungsfall**** alle Situationen automatisch bewältigen.	Das System übernimmt die Fahraufgabe vollumfänglich bei allen Straßentypen, Geschwindigkeitsbereichen und Umfeldbedingungen.

* **Längsführung:** Geschwindigkeit halten, Gasgeben und Bremsen
Querführung: Lenken

**Anwendungsfälle beinhalten Straßentypen, Geschwindigkeitsbereiche und Umfeldbedingungen.

Interview mit Sven Paeslack, Abteilungsleiter „Typgenehmigung“ beim Kraftfahrt-Bundesamt (KBA)

Wie gelingt es, trotz steigender Anforderungen an die Cyber-Sicherheit, dass die Sicherheit der Autos auf den Straßen weiterhin gewährleistet ist und das Vertrauen der Verbraucherinnen und Verbraucher erhalten bleibt?

Die Grundlage sind robuste gesetzliche Regelungen, ein fordernder Typgenehmigungsprozess sowie eine intensive Überwachung des Marktes. Alle Beteiligten müssen über hohe Kompetenzen verfügen, die Cyber Security als Daueraufgabe kontinuierlich über den gesamten Lebenszyklus eines Fahrzeuges sicherstellen und bei Schwachstellen umgehend reagieren zu können.

Wie funktioniert die Zusammenarbeit mit dem BSI?

2020 haben das BSI und das KBA eine gemeinsame Verwaltungsvereinbarung unterzeichnet, um effizient die Aufgaben im Bereich der Automotive Cyber Security abzuarbeiten. Schon zuvor gab es eine intensive Zusammenarbeit, die durch die Vereinbarung nochmals gestärkt worden ist. Die Kooperation umfasst regelmäßige Treffen auf Arbeitsebene, die Erarbeitung von Anforderungen für Fahrzeughersteller und Technische Dienste sowie gemeinsame Audits bei diesen. Diese Zusammenarbeit von BSI und KBA war vom Beginn an ein Erfolgsmodell und soll international Maßstäbe setzen.

Auf welche Themenbereiche innerhalb der Cyber Security legen Sie besonders viel wert?

Die ganzheitliche Betrachtung der Cyber Security durch die am Genehmigungsprozess Beteiligten ist wesentlich, um Cyber-Angriffen auf Kraftfahrzeuge entgegenzuwirken. Dies muss durch Qualitätsmanagement-Systeme und Produkttests sichergestellt werden.

Hersteller müssen Maßnahmen über den gesamten Lebenszyklus (Entwicklung, Produktion, Außerbetriebsetzung) eines Fahrzeuges nachprüfbar darlegen. Das betrifft die Einhaltung des Rechtsrahmens und der sich aus der Natur der Cyber Security ergebenden, stetig anzupassenden Anforderungen.

Haben Sie ein Beispiel für ein konkretes Projekt?

Für die erste Genehmigung nach der neuen, harmonisierten UN-Regelung Nr. 155 zur Cyber Security haben wir sehr zeitnah Technische Dienste benannt und das Cyber-Security-Managementsystem eines Herstellers auditieren sowie die Produktprüfungen bewerten können. Dabei haben KBA und BSI während der Planungsphase, der Erarbeitung der Auditpläne, der Audits und für die Produktprüfung zusammengearbeitet. So waren wir in der Lage, die weltweit erste Genehmigung nach diesem Regelwerk zu erteilen, das Anfang 2021 in Kraft getreten ist.

Welche Vision verfolgt das KBA im Bereich der Cyber-Sicherheit?

Das KBA will mit seinen Kooperationspartnern international den Benchmark im Bereich der Automotive Cyber Security setzen, die Regelwerke weiter optimieren und die Erfahrungen zur Gewährleistung einer ganzheitlichen Verkehrssicherheit nutzen – dauerhaft und verlässlich.

Vielen Dank für das Gespräch!

KBA

Das Kraftfahrt-Bundesamt (KBA) ist die Bundesoberbehörde für den Straßenverkehr und unter anderem zuständig für die Typgenehmigung von Fahrzeugen und Fahrzeugteilen sowie die Benennung von Technischen Diensten. Zudem führt das KBA die Marktüberwachung für alle Produkte im Regelungsbereich des Straßenverkehrsgesetzes durch.

5 Der Blick nach vorne: Was jetzt zu tun ist

> *Ich denke viel an die Zukunft,*
> *weil das der Ort ist,*
> *wo ich den Rest meines Lebens zubringen werde.*
> *(Woody Allen)*

Die dargestellten Herausforderungen und Themen im Digitalen Verbraucherschutz werfen die Frage auf: „Was ist zu tun?“ Wir erleben eine fortschreitende Digitalisierung der Gesellschaft. Mit Blick auf die Potenziale sowie die heute erst angedachten Anwendungen der Zukunft müssen wir uns eingestehen, dass wir weiterhin am Anfang komplexer Entwicklungen sind. Der im Bericht skizzierte Automotive-Bereich (Kapitel 4) ist dabei ein gutes Beispiel für die Metamorphose einer Old Economy in die digitale Moderne – mit weiterhin hohem Entfaltungspotenzial.

Digitalisierung und Informationssicherheit sind zwei Seiten derselben Medaille. So gilt es insbesondere für den Digitalen Verbraucherschutz, alle relevanten Akteure einzubinden, um das IT-Sicherheitsniveau grundsätzlich zu erhöhen und zukunftstauglich zu machen. Es bedarf einer ganzheitlich gedachten Sicherheitsinfrastruktur, um Prävention, Detektion und Reaktion effektiv miteinander zu verknüpfen. Die Analyse der Entwicklungen im Jahr 2021 (Kapitel 3) zeigt, dass die Gefahren des Cyber-Raumes nach wie vor einer enormen Dynamik unterliegen. Cyber-Kriminalität in all ihren Ausprägungen ist zum globalen, lukrativen und stetig wachsenden Geschäft geworden. Dem müssen wir uns als Verbraucherschützerinnen und Verbraucherschützer stellen. Die elementaren Herausforderungen sind:

- Die Etablierung technischer Schutzmöglichkeiten in den Alltag der Verbraucherinnen und Verbraucher.
- Die Kompetenzbildung und Wissensvermittlung für die sichere Nutzung von Online-Anwendungen und -Produkten.
- Stärkere Anstrengungen von Wirtschaft und weiteren Institutionen für sichere Angebote.

Der „Faktor Mensch“ spielt, wie in Kapitel 2 intensiv beleuchtet, eine gewichtige Rolle bei nahezu allen Überlegungen für einen effizienten Digitalen Verbraucherschutz. Das weite Feld der Informationssicherheit kann jedoch aufgrund der Komplexität sowie aufwendiger technisch-organisatorischer Anforderungen bei Teilen der Verbrauchergruppe zur Überforderung führen. Schlimmstenfalls mündet diese in Desinteresse oder Ablehnung. Auch dieser Herausforderung muss sich der Digitale Verbraucherschutz weiterhin stellen.

Es gilt, die Verbraucherperspektive einzunehmen.

Das Wissen um spezifische Bedürfnisse und Trends, das Nutzungsverhalten, differenzierte Lebenswelten oder auch psychografische Aspekte sind Grundvoraussetzung, um geeignete Handlungsmaximen und Kommunikationsmaßnahmen für Verbraucherinnen und Verbraucher zu entwickeln.

Zusammenfassend lassen sich für die verschiedenen Akteure im Bereich des Digitalen Verbraucherschutzes folgende gemeinsame Handlungsfelder festhalten:

AKTEURE	HANDLUNGSFELDER
Wirtschaft und Staat	• **„Usable Security“**, das heißt, die einfache beziehungsweise eingängige Umsetzung von IT-Sicherheitsmaßnahmen für Kundinnen und Kunden beim Gebrauch von digitalen Produkten und Diensten (siehe Verbraucherperspektive und -bedarfe) • Fokussierung auf die **Nachhaltigkeit** von Produkten/Angeboten im Kontext der Informationssicherheit, zum Beispiel durch eine langfristige Update-Policy • Verbraucherschutz ist auch der **Schutz von Kundendaten in Unternehmen vor potenziellen Angriffen und Datenleaks**, etwa mit Maßnahmen wie dem IT-Grundschutz • Weiterentwicklung von **IT-Sicherheit-Mindeststandards, Zertifizierungen** und Maßnahmen zur **Transparenzbildung** auf nationaler wie internationaler Ebene
Gesellschaft und Verbraucher	• Die Informationssicherheit als hohes, **schützenswertes Gut gesellschaftlich verankern** und dafür sensibilisieren • Die **Kompetenzbildung** und **Wissensvermittlung** in der Bevölkerung vorantreiben • Die verschiedenen handelnden Akteure als **Multiplikatoren** für eine breite Aufklärungsarbeit einbinden • Aufnehmen von **Trendthemen**, Berücksichtigung von **Verbraucherinteressen** und **Bündelung von Interessen** durch institutionelle Akteure der Zivilgesellschaft

Die Gefahren, welche die Digitalisierung mit sich bringt, kennen keine territorialen Grenzen. Daher sind internationale Bestrebungen auch im Digitalen Verbraucherschutz notwendig. Das in Kapitel 2 thematisierte IT-Sicherheitskennzeichen bietet dazu beispielhaft eine entsprechende europäische Perspektive für mehr Transparenz im internationalen Verbrauchermarkt.

Aufgrund seiner Komplexität und Vielfalt ist und bleibt der Digitale Verbraucherschutz eine gesamtgesellschaftliche Herausforderung. Er bedarf ganzheitlicher und gemeinsamer Anstrengungen. Nur so kann der digitale, private Alltag für Verbraucherinnen und Verbraucher sicher gestaltet werden. Heute und in Zukunft.

6 Literaturverzeichnis/ Quellen

ADAC (2019):
Ab wann sind Autos, Motorräder & Co. Oldtimer?
Einzusehen unter:
https://www.adac.de/rund-ums-fahrzeug/oldtimer-youngtimer/recht-tipps/oldtimer-definition/,
zuletzt eingesehen am: 25.01.2022.

Adams A and Sasse MA (1999):
Users are not the enemy.
Communications of the ACM 42(12): 40–46.

Bundesamt für Sicherheit in der Informationstechnik (2021):
Ransomware: Bedrohungslage, Prävention & Reaktion 2021.
Einzusehen unter:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.html,
zuletzt eingesehen am: 21.01.2022.

Bundesamt für Sicherheit in der Informationstechnik (2021):
„Smishing" - SMS-Phishing im Herbst 2021 mit neuen Betrugsmaschen. Pressemitteilung vom 14.10.2021.
Einzusehen unter:
https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/Smishing_SMS-Phishing_141021.html,
zuletzt eingesehen am: 21.01.2022.

Bundesamt für Sicherheit in der Informationstechnik (2021):
Die Lage der IT-Sicherheit in Deutschland 2021.
Einzusehen unter:
https://www.bsi.bund.de/Lagebericht,
zuletzt eingesehen am: 21.01.2022.

Bundesamt für Sicherheit in der Informationstechnik (2021):
Sicherer, robuster und nachvollziehbarer Einsatz von KI: Probleme, Maßnahmen und Handlungsbedarfe.
Einzusehen unter:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Herausforderungen_und_Massnahmen_KI.pdf?__blob=publicationFile&v=5,
zuletzt eingesehen am: 25.01.2022

Bundesamt für Straßenwesen (2021):
Selbstfahrende Autos – assistiert, automatisiert oder autonom?
Einzusehen unter:
https://www.bast.de/DE/Presse/Mitteilungen/2021/06-2021.html,
zuletzt eingesehen am 25.01.2021

Bundeskanzleramt (gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik) (2020):
Zwischenbericht: Schutz von Online-Konten.
Ergebnisse der ersten Projektphase.
Online verfügbar unter:
https://www.bundesregierung.de/resource/blob/975272/1732446/4c4377ce98f697a94011955fdc9a1f62/de-passwort-download-zwischenbericht-data.pdf?download=1

Bleepingcomputer (2022):
Microsoft mitigates largest DDoS attack 'ever reported in history'.
Einzusehen unter:
https://www.bleepingcomputer.com/news/security/microsoft-mitigates-largest-ddos-attack-ever-reported-in-history/,
zuletzt eingesehen am: 01.02.2022

Chong I, Xiong A and Proctor RW (2019):
Human Factors in the Privacy and Security of the Internet of Things. Ergonomics in Design:
The Quarterly of Human Factors Applications 27(3): 5–10.

Coverware (2019):
Ransomware Recovery Blog. Quarterly Report:
Ransom amounts rise 90% in Q1 as Ryuk increases.
Einzusehen unter:
https://www.coveware.com/blog/2019/4/15/ransom-amounts-rise-90-in-q1-as-ryuk-ransomware-increases,
zuletzt eingesehen am 31.01.2022.

Coverware (2020):
Ransomware Recovery Blog. Quarterly Report:
Ransomware Payments Up 33% As Maze and Sodinokibi Proliferate in Q1 2020.
Einzusehen unter:
https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report,
zuletzt eingesehen am 31.01.2022.

Coverware (2020b):
Ransomware Recovery Blog. Quarterly Report:
Ransomware Demands continue to rise as Data Exfiltration becomes common, and Maze subdues.
Einzusehen unter:
https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report, zuletzt eingesehen am 31.01.2022.

Coverware (2021):
Ransomware Recovery Blog. Quarterly Report:
Ransomware attackers down shift to 'Mid-Game' hunting in Q3 2021.
Einzusehen unter:
https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts,
zuletzt eingesehen am 31.01.2022

Dourish P and Anderson K (2006):
Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena. *Human-Computer Interaction 21(3): 319–342.*

Fox D and Titze C (2021):
Phishing Awareness durch Gamification. *Datenschutz und Datensicherheit - DuD 45(11): 727–732.*

Fridrich, Christian, Renate Hübner, Karl Kollmann, Michael-Burkhard Piorkowsky, and Nina Tröger. 2017.
"Grundüberlegungen Zu Einer Kritischen Verbraucherforschung." In Abschied Vom Eindimensionalen Verbraucher, edited by Christian Fridrich, Renate Hübner, Karl Kollmann, Michael-Burkhard Piorkowsky, and Nina Tröger, 1-22. Kritische Verbraucherforschung. *Wiesbaden, Germany: Springer VS.*

Fridrich, Christian, Renate Hübner, Rainer Hufnagel, Mirjam Jaquemoth, Karl Kollmann, Michael-Burkhard Piorkowsky, Norbert F. Schneider, Nina Tröger und Stefan Wahlen.
2014. Bamberger Manifest für ein neues Verbraucherverständnis. Journal für Verbraucherschutz und Lebensmittelsicherheit. *Online first (27. April): 1–6.*

Financial Crimes Enforcement Network (2021):
Financial Trend Analysis. Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021.
Einzusehen unter:
https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf, zuletzt eingesehen am: 01.02.2021.

Golem (2021)::
Ceconomy Ransomware verlangt Millionen Dollar von Media Markt.
Einzusehen unter:
https://www.golem.de/news/ceconomy-ransomware-verlangt-240-millionen-dollar-von-media-markt-2111-160941.html, zuletzt eingesehen am: 28.01.2022.

Hessenschau (2021):
Cyberangriff und die Folgen. Tegut warnt nach Kundendaten-Klau vor Betrügern.
Einzusehen unter:
https://www.hessenschau.de/wirtschaft/tegut-warnt-nach-kundendaten-klau-vor-betruegern,kundendaten-tegut-darknet-100.html, zuletzt eingesehen am: 16.02.2022.

Kaspersky (2021):
Die Ransomware-Saga.
Einzusehen unter:
https://www.kaspersky.de/blog/history-of-ransomware/26487/, zuletzt eingesehen am: 28.01.2022.

Kraftfahrt-Bundesamt (2021):
Fahrzeugstatistik: Durchschnittsalter der Personenkraftwagen wächst.
Einzusehen unter:
https://www.kba.de/DE/Statistik/Fahrzeuge/Bestand/Fahrzeugalter/2021/2021_b_kurzbericht_fz_alter_pdf.pdf;jsessionid=87C7B1D59A4D9E582FAE5856573D56B3.live11294?__blob=publicationFile&v=2,
zuletzt eingesehen am: 25.01.2022

Kraftfahrt-Bundesamt (2021b):
Personenkraftwagen am 1. Januar 2021 nach ausgewählten Merkmalen.
Einzusehen unter:
https://www.kba.de/DE/Statistik/Fahrzeuge/Bestand/Jahrebilanz_Bestand/2021/2021_b_jahresbilanz_tabellen.html?nn=3532350&fromStatistic=3532350&yearFilter=2021&fromStatistic=3532350&yearFilter=2021,
zuletzt eingesehen am: 25.01.2022.

Malwarebytes (2021):
Demographics of Cybercrime.
Einzusehen unter:
https://www.malwarebytes.com/resources/2021-demographics-of-cybercrime-report/index.html,
zuletzt eingesehen am: 21.01.2022.

Neumann L (2017):
Menschliche Faktoren in der IT-Sicherheit. In: Abolhassan F (ed) *Security Einfach Machen: IT-Sicherheit als Sprungbrett für die Digitalisierung.* Wiesbaden: Springer Gabler, 85-97.

Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) und Bundesamt für Sicherheit in der Informationstechnik (BSI) (2021):
Digitalbarometer.
Online verfügbar unter:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Digitalbarometer/Digitalbarometer-ProPK-BSI_2021.html

RBB24 (2021):
Corona-Schnelltests. Schwere Sicherheitslücke bei sensiblen Daten Tausender Berliner.
Einzusehen unter:
https://www.rbb24.de/politik/thema/corona/beitraege/2021/03/berlin-datenleck-schnelltests-21dx-medicus-ai.html,
zuletzt eingesehen am: 01.02.2022.

SAE International (2021):
Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles J3016_202104.
Einzusehen unter:
https://www.sae.org/standards/content/j3016_202104/,
zuletzt eingesehen am: 25.01.2021.

Sasse MA and Smith M (2016):
The Security-Usability Tradeoff Myth [Guest editors' introduction]. *IEEE Security & Privacy* 14(5): 11–13.

Statistisches Bundesamt (2021):
Umsätze im Onlinehandel haben auch nach Wiedereröffnung der Geschäfte weiter zugenommen. Pressemitteilung Nr. N 067 vom 24. November 2021.
Einzusehen unter:
https://www.destatis.de/DE/Presse/Pressemitteilungen/2021/11/PD21_N067_45.html,
zuletzt eingesehen am: 21.01.2022.

SVRV - Sachverständigenrat für Verbraucherfragen. (2021):
Gutenachten zur Lage der Verbraucherinnen und Verbraucher 2020. BMJV. Berlin.
Online verfügbar unter:
https://www.svr-verbraucherfragen.de/wp-content/uploads/SVRV_Gutachten_2020.pdf,
zuletzt geprüft am 22.04.2021.

t3n – digital pioneers (2021):
Hacker-Angriff auf Reiseveranstalter FTI:
So groß ist der Schaden.
Einzusehen unter:
https://t3n.de/consent?redirecturl=%2Fnews%2Fhacker-angriff-fti-conti-1429780%2F,
zuletzt eingesehen am: 01.02.2021.

Tagesschau (2021):
Tausende Menschen betroffen. Datenleck bei Corona-Tests.
Einzusehen unter:
https://www.tagesschau.de/investigativ/ndr/datenleck-corona-test-101.html,
zuletzt eingesehen am: 01.02.2022.

Thorun C and Diels J (2020):
Consumer Protection Technologies: An Investigation Into the Potentials of New Digital Technologies for Consumer Policy. *Journal of Consumer Policy* 43(1): 177–191.

TÜV-Verband (2020):
Mobility-Studie 2020.
Einzusehen unter:
https://www.tuev-verband.de/?tx_epxelo_file[id]=824708&cHash=ffdd97d1d1e007adc980dc629d0ecf06,
zuletzt eingesehen am: 25.01.2022.

Unit 42 (2021):
Highlights form the 2021 Unit 42 Ransomware Threat Report.
Einzusehen unter:
https://unit42.paloaltonetworks.com/ransomware-threat-report-highlights/, zuletzt eingesehen am: 01.02.2022.

United Nations Economic Commission for Europe, UNECE (2021):
Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system. UN Regulation No. 155.

United Nations Economic Commission for Europe, UNECE (2021b):
Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system. UN Regulation No. 156.

Verbraucherzentrale Bundesverband (2021):
Warnung: Abzocke durch angebliche Microsoft-Mitarbeiter.
Einzusehen unter:
https://www.verbraucherzentrale.de/wissen/vertraege-reklamation/abzocke/warnung-abzocke-durch-angebliche-microsoftmitarbeiter-24641,
zuletzt eingesehen am: 21.01.2021.

Verbraucherzentrale NRW (2017):
Connected Car nimmt Fahrt auf – Wohin steuert das Auto der Zukunft? Trendbericht Marktwächter Digitale Welt – Nutzergenerierte Inhalte.
Einzusehen unter:
https://www.verbraucherzentrale.de/sites/default/files/2019-11/trendbericht-connected-car.pdf,
zuletzt eingesehen am: 25.01.2022.

Verbraucherzentrale NRW (2021):
Phishing-Radar.
Einzusehen unter:
https://www.verbraucherzentrale.nrw/wissen/digitale-welt/phishingradar,
zuletzt eingesehen am: 21.01.2022.

Verbraucherzentrale NRW (2021b):
Telematik-Versicherung: Geld sparen möglich, aber es gibt Kehrseiten.
Einzusehen unter:
https://www.verbraucherzentrale.de/wissen/geld-versicherungen/weitere-versicherungen/telematikversicherung-geld-sparen-moeglich-aber-es-gibt-kehrseiten-38399,
zuletzt eingesehen am: 25.01.2022.

Weirich D and Sasse MA (2001):
Pretty good persuasion. In: Proceedings of the 2001 workshop on New security paradigms: (eds V Raskin, SJ Greenwald, B Timmerman and D Kienzle), Cloudcroft, New Mexico, 9/10/2001 - 9/13/2001, p. 137. New York, NY: ACM.

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
März 2022

Druck
Appel & Klinger Druck und Medien GmbH, Schneckenlohe

Gestaltung
Faktor 3 AG

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

Bildnachweis
Titel, S. 8, S. 10, S. 18, S. 24, S. 32, S. 34: AdobeStock ©Roman;
Titel: AdobeStock ©mimagephotos; S. 2, S. 26, S. 30, S. 39: BSI;
S. 8: AdobeStock ©Soloviova; S. 9: AdobeStock ©Olivier Le Moal;
S. 10: AdobeStock ©TimeStopper; S. 15: AdobeStock ©SFIO CRACHO;
S. 18: AdobeStock ©Drobot Dean; S. 24: AdobeStock ©Andrey Popov;
S. 28: AdobeStock ©Olivier Le Moa; S. 32: AdobeStock ©rh2010;
S. 34: AdobeStock ©pikselstock

Grafiken
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Artikelnummer
BSI-DVS22/001

www.bsi.bund.de