Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Bericht zum Digitalen Verbraucherschutz 2020

Sicher im
digitalen Alltag

Vorwort

In Deutschland gibt es eine lange Tradition des Verbraucherschutzes: Ernährung, Kosmetik, Konsumprodukte – auf vielen Wegen können sich Verbraucherinnen und Verbraucher über Vor- und Nachteile hierzu informieren. IT-Sicherheit ist hier immer noch ein Nischenthema. Wie lange wird mein Handy oder mein Smart TV mit Updates versorgt? Gab es früher bei dem Gerät schon Schwachstellen? Diese Fragen gehören für uns als BSI mit in das Portfolio an Informationen, die Verbraucherinnen und Verbraucher brauchen, um eine informierte und abgewogene Entscheidung zu treffen. Deshalb ist es gut und wichtig, dass das BSI mit dem IT-Sicherheitsgesetz 2.0 die gesetzlich verankerte Aufgabe des Digitalen Verbraucherschutzes bekommen hat.

Wir bauen dabei auf fast zwanzig Jahre Verbraucherinformation und -beratung auf. Wir arbeiten intensiv daran, die Informationssicherheit für alle Verbraucherinnen und Verbraucher zu gestalten und voranzutreiben. Daraus leiten wir eine Vielzahl von strategischen Zielen ab:
Künftig sollen so viele Consumer-Produkte wie möglich über ein IT-Sicherheitskennzeichen verfügen. Damit jeder auf einen Blick erkennen kann, über welche Sicherheitseigenschaften ein IT-Gerät verfügt. An unserem Standort in Freital richten wir einen eigenen Fachbereich ein, der sich ausschließlich um die Belange der Verbraucherinnen und Verbraucher kümmern wird. Wir initiieren zudem neue und intensivieren bestehende Informations- und Austauschformate und Kooperationen, haben einen “Beirat Digitaler Verbraucherschutz” gegründet und wenden uns mit der deutschlandweiten Informationskampagne “#einfachaBSIchern” an die Bürgerinnen und Bürger.

Mit diesem „Bericht zum Digitalen Verbraucherschutz“ gehen wir einen Schritt weiter. Wir wollen damit insbesondere jene Zielgruppen erreichen, die Verbraucherschutz aus professioneller Sicht in Deutschland gestalten. Nur mit ihnen zusammen können wir das Thema IT-Sicherheit in der öffentlichen Wahrnehmung verankern.

In diesem Bericht bündeln wir ab sofort jährlich die Expertise des ganzen BSI, analysieren entlang der integrierten Wertschöpfungskette im BSI von der Cyberabwehr bis zum Verbraucherschutz systematisch die Lage im Digitalen Verbraucherschutz und verknüpfen dies mit einem stets aktuellen Schwerpunktthema. In 2021 ist das das Thema “Cyber-Sicherheit im Gesundheitswesen”.

Für uns als BSI sind Digitalisierung und Informationssicherheit die zwei Seiten einer Medaille. Das eine gelingt nur mit dem anderen zusammen. In diesem Sinne bauen wir auf den Austausch und die Kooperation mit bewährten und neuen Partnern in Kommunen, Ländern, dem Bund, der Wirtschaft und Zivilgesellschaft. Es liegt noch einiges an Wegstrecke für einen umfassenden Digitalen Verbraucherschutz vor uns. Mit diesem ersten „Bericht zum Digitalen Verbraucherschutz“ ist wieder ein wichtiger Schritt getan.

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

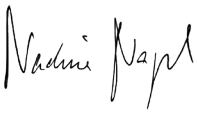
Die Vielfalt und Dynamik des digitalen Verbrauchermarktes

Schnell noch etwas via App bestellen, der Tochter beim Einloggen im neuen Schulportal helfen und der liebsten Freundin mit einem Videogruß zum Geburtstag gratulieren – die digitalen Möglichkeiten sind nahezu grenzenlos. Mit seiner Vielfalt und zugleich dynamischen Entwicklung wird der digitale Verbrauchermarkt jedoch zusehends zum Spielfeld krimineller Handlungen: Das Risiko von IT-Sicherheitsvorfällen und Cyber-Angriffen steigt.

Eine Auswahl an Daten und Fakten dazu haben wir in unserem neuen „Bericht zum Digitalen Verbraucherschutz" zusammengetragen und aufbereitet – mit informativen Mehrwerten. Er ordnet exemplarische und prägende Vorfälle und Entwicklungen des vorangegangenen Jahres ein und gibt passende Handlungsempfehlungen und Ausblicke. Ein Themenkomplex von besonderer gesellschaftlicher Relevanz wird einer fokussierten Betrachtung unterzogen. Zudem wird die Zielgruppe der Verbraucherinnen und Verbraucher stärker beleuchtet. Wir wollen so noch besser verstehen, auf welche Art und Weise mit digitalen Produkten, Daten und Dienstleistungen umgegangen wird, und daraus ableiten, welche spezifischen Bedarfe und Erwartungen hinsichtlich der IT-Sicherheit im privaten Alltag bestehen – stets mit Blick auf unsere drei Kernziele im Digitalen Verbraucherschutz:

- das Risikobewusstsein im digitalen Raum zu schärfen,
- die Beurteilungsfähigkeit zu stärken und
- die Lösungskompetenz zu steigern.

Mit dem „Bericht zum Digitalen Verbraucherschutz" wollen wir Orientierung in einem komplexen Handlungsfeld geben, das von vielen Beteiligten geprägt wird. Der Spannungsbogen reicht dabei vom Verbraucher über die Hersteller bzw. Dienstleister bis hin zu staatlichen und zivilgesellschaftlichen Akteuren. Dieses Spektrum an Stakeholdern wollen wir mit unserer neuen Publikation erreichen und damit auch für aktuelle Themen rund um die IT-Sicherheit des digitalen Verbrauchermarktes einen aktiven Dialog anregen.



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

Inhaltsverzeichnis

2 Einleitung

2 Einleitung

Die fortschreitende Digitalisierung unserer Welt zeigt sich in allen Lebensbereichen. Nicht nur in Wirtschaft, Politik und Wissenschaft - auch in der Gesellschaft steigen Relevanz und Bedeutung von sicheren IT-Diensten und IT-Produkten. So sind beispielsweise IT-Produkte wie Smartphones oder Sprachassistenzsysteme, aber auch IT-Dienstleistungen wie Onlineshopping fest im Alltag der meisten Menschen verankert.

Mit dem Thema „Digitaler Verbraucherschutz" gestaltet das Bundesamt für Sicherheit in der Informationstechnik (BSI) ein neues Handlungsfeld, das sich mit genau diesen Themenfeldern auseinandersetzt. Zweifelsohne bietet die Digitalisierung enorme Chancen für die Verbraucherinnen und Verbraucher. Und doch kann diese nur zu einer Erfolgsgeschichte werden, wenn IT-Sicherheit als Grundlage verstanden wird. Damit die Menschen für die damit verbundenen Herausforderungen und Risiken gewappnet sind, treibt das BSI den digitalen Verbraucherschutz weiter voran, um das Thema fest im Bewusstsein von Staat, Wirtschaft und Gesellschaft zu verankern.

Das BSI sammelt und erhebt eine Vielzahl von Daten zur Lage der IT-Sicherheit in Deutschland. Dafür werden vielfältige Quellen sowie Meinungen von Expertinnen und Experten herangezogen. Mit Fokus auf die Verbraucherinnen und Verbraucher sowie die zugrundeliegenden Märkte werden die zentralen Sachverhalte und Gegebenheiten aus dem Jahr 2020 erneut betrachtet und analysiert, um den folgenden Zielen nachzugehen:

Die Publikation legt ein Hauptaugenmerk auf die Frage, welche Schwerpunktthemen das digitale Verbraucherschutzjahr 2020 geprägt haben. Hierzu werden die wesentlichen **Sicherheitsvorfälle** am digitalen Verbrauchermarkt dargestellt und dahingehend erörtert, inwiefern insbesondere Verbraucherinnen und Verbraucher davon betroffen sein können.

Der Fokus dieser ersten Ausgabe des Berichts zum digitalen Verbraucherschutz liegt auf der **„Cybersicherheit im Gesundheitswesen"**. Da die **COVID-19-Pandemie** unsere Gesellschaft nachhaltig beeinflusst hat, wird vor diesem Hintergrund der Frage nach den Auswirkungen auf den digitalen Verbraucherschutz nachgegangen. Neben möglichen Sicherheitsrisiken durch die Veränderung des Konsumverhaltens der Verbraucherinnen und Verbraucher stellt die **Corona-Warn-App** ein weiteres Schlaglicht im Jahr 2020 dar. Darüber hinaus hat das BSI eine Untersuchung zum Thema **Gesundheits-Apps** initiiert. Sowohl die Vorstellung der Studienergebnisse als auch die Frage nach der genauen Ausgestaltung des digitalen Verbraucherschutzes an diesem spezifischen Markt werden nachfolgend diskutiert.

Um das digitale Verbraucherschutzjahr 2020 abzubilden, müssen zwei Perspektiven betrachtet werden: Welche Voraussetzung bringt der Markt mit? Ist dieses für Verbraucherinnen und Verbraucher nachvollziehbar? Anhand von Befragungsdaten zu Erwartungen und Handlungsweisen von Menschen im digitalen Raum werden **die Einstellungen, Erfahrungen und Herausforderungen von Verbraucherinnen und Verbrauchern** im digitalen Markt analysiert. Weiterführend werden die **Bedarfe** der Verbraucherinnen und Verbraucher im Umgang mit digitalen Produkten und Dienstleistungen identifiziert und erörtert. Ein starker Fokus liegt dabei auf der Zielsetzung, dass das BSI die Verbraucherinnen und Verbraucher zu aktivem Handeln in der IT-Sicherheit im privaten Kontext befähigen möchte. Auf diesem Weg können Anknüpfungspunkte gefunden werden, um das Risikobewusstsein der Verbraucherinnen und Verbraucher zu erhöhen, ihre Beurteilungsfähigkeit zu steigern und ihre Lösungskompetenz zu stärken.

Mit dem Ziel, neue Erkenntnisse zum gesamtgesellschaftlichen Dialog in den Bereichen der Informationssicherheit und des Verbraucherschutzes beizutragen, schließt die Publikation mit potentiellen **Gestaltungsräumen** des digitalen Verbraucherschutzes für die Zukunft, die von Herstellern, Dienstleistern sowie Anwenderinnen und Anwendern wahrgenommen werden können. Hierzu werden zusammenfassend zu unterstützende **Handlungsfelder** sowie **Empfehlungen** dargestellt, die sich aus den Erkenntnissen des Verbraucherschutzjahres 2020 ableiten lassen.

3 Die digitalen Verbraucherinnen und Verbraucher

3 Die digitalen Verbraucherinnen und Verbraucher

Was sind digitale Verbraucherinnen und Verbraucher? Und wie digital machen diese Bürgerinnen und Bürger Deutschland? Allgemein gültige und eindeutige Antworten darauf können bisher nicht gegeben werden. Zudem unterliegen diese – wie auch die Digitalisierung selbst – einem steten Wandel.

Das BSI setzt sich mit dem vorliegenden, von nun an jährlich erscheinenden Bericht verstärkt dafür ein, diese Fragen zu beantworten. Denn die Kompetenzen, Erwartungen und Bedürfnisse dieser wichtigen Zielgruppe sind zentrale Bausteine für erfolgreiche Maßnahmen im digitalen Verbraucherschutz.

In diesem Kapitel werden grundlegende Anhaltspunkte vorgestellt, um die genannten Bausteine für die Zielgruppe der digitalen Verbraucherinnen und Verbraucher einzuordnen. Im Rahmen einer Web-Recherche wurden Studien und Statistiken zusammengetragen, die Informationen rund um die digitale Sicherheitslage der Verbraucherinnen und Verbraucher bieten. Für den Berichtszeitraum vom 01.01.2020 bis zum 31.12.2020 wurden wesentliche Aussagen aus dem Material zur aktuellen Situation und Bedrohungslage am digitalen Verbrauchermarkt 2020 erfasst. Gleichermaßen wurden Bedürfnisse sowie Nutzungsverhalten mitbetrachtet, um Kernaussagen über die digitalen Verbraucherinnen und Verbraucher im Jahr 2020 treffen zu können. Um ein möglichst aktuelles Bild von digitalen Verbraucherinnen und Verbrauchern im Erhebungszeitraum 2020 zu erhalten, wurde die Recherche um neue Veröffentlichungen der zugrundeliegenden Publikationsreihen aus dem 1. Quartal 2021 ergänzt.

Eine Bestandsaufnahme der digitalen Gesellschaft: Der D21-Digital-Index

Die Initiative D21 e. V. hat mit dem D21-Digital-Index Erkenntnisse darüber erhoben, wie die Bevölkerung den digitalen Wandel adaptiert. Beim D21-Digital-Index handelt es sich um eine jährliche Befragung mit dem Ziel, das digitale Lagebild in der Gesellschaft zu erheben. Basierend auf einer Zufallsstichprobe wurden im ersten Schritt Strukturbefragungen (20.322 Befragte im Zeitraum 2019/2020, 16.158 Befragte im Zeitraum 2019/2020) mit anschließenden Vertiefungsbefragungen (2.019 Befragte im Zeitraum 2019/2020, 2.038 Befragte im Zeitraum 2020/2021) durchgeführt. Digitale Trends zeichneten sich bereits im Berichtszeitraum 2019/2020 ab und wurden, wie im Folgebericht 2020/2021 deutlich wurde, durch die COVID-19-Pandemie verstärkt. So zeigte der Erhebungszeitraum 2019/2020, dass mit 82 Prozent bereits die deutliche Mehrheit der Bevölkerung das Internet für Recherchen mit Suchmaschinen nutzte. Weitere häufige Aktivitäten waren Onlineshopping mit 71 Prozent und Instant Messaging mit 70 Prozent. Etwas mehr als die Hälfte der Bevölkerung nutzte das Internet außerdem für Büroanwendungen (60 %), den Online-Kauf von Dienstleistungen (58 %) sowie für Online-Bezahlverfahren (55 %).

Die Zahlen machen deutlich, dass die Digitalisierung in den meisten Haushalten Einzug gehalten hat. Laut D21-Digital-Index gingen bereits im Erhebungszeitraum 2019/2020 viele Bürgerinnen und Bürger davon aus, dass die Digitalisierung in den nächsten drei bis fünf Jahren weitere Lebensbereiche stark verändern wird. Das Gesundheitswesen, E-Commerce und das Bildungswesen können hier als Beispiele benannt werden. Die erwartete Veränderung wurde dabei von der Mehrheit als (eher) positiv eingeschätzt. Im darauffolgenden Erhebungszeitraum gab die Hälfte der Bürgerinnen und Bürger an, dass sie sich bereits jetzt als Gewinner der Digitalisierung sehen.

Mit der verstärkten Nutzung von Online-Diensten und digitalen Endgeräten geht für die meisten Menschen auch der Wunsch nach digitaler Selbstbestimmtheit im Umgang mit diesen Dienstleistungen und Produkten einher. In den D21-Studien aus beiden Erhebungszeiträumen gab die Mehrheit der Befragten an, dass sie bezüglich ihrer Daten im Internet ein Ohnmachtsgefühl empfinden. Zum Beispiel gaben mehr als zwei von fünf Befragten im Erhebungszeitraum 2020/2021 an, dass sie das Gefühl haben, den Unternehmen nicht trauen zu können, obwohl sie deren digitale Anwendungen und Dienste in Anspruch nehmen.

Bedürfnisse der Verbraucherinnen und Verbraucher zum Thema Sicherheit

Weitere Erkenntnisse über die Herausforderungen der IT-Sicherheit für Verbraucherinnen und Verbraucher und den damit verbundenen Bedürfnissen veröffentlichten das Bundesministerium des Innern, für Bau und Heimat (BMI) und das BSI zum Safer Internet Day am 1. Februar 2020. In einer offenen Trendabfrage, umgesetzt

als Online-Befragung, mit mehr als 20.000 Teilnehmenden zeigte sich, dass sich rund drei Viertel der Befragten mehr Informationen für den Bereich digitale Sicherheit wünschen. Zu den Bereichen mit dem höchsten Informationsbedarf gehörten dabei Online- und Mobile-Banking mit 35 Prozent sowie der Schutz von digitalen Endgeräten mit 24 Prozent.

Bei der Veröffentlichung der Ergebnisse richteten BMI und BSI den Blick auf Themen wie die Nutzung von Smart Home-Technologien, obwohl Verbraucherinnen und Verbraucherinnen hier nur wenig Informationsbedarf äußerten. Das gleiche Phänomen zeigt sich bei stets aktuellen Themenfeldern wie beispielsweise Onlineshopping, soziale Netzwerke und Online-Kommunikation. Hier wünschten sich weit weniger als ein Viertel der Befragten Unterstützung oder äußerten Informationsbedarf. Das BSI machte vor diesem Hintergrund darauf aufmerksam, dass auch diese Bereiche der digitalen Lebenswelt trotz weniger explizit geäußertem Informationsbedarf nicht zu unterschätzen sind. Gerade am Beispiel der Smart Home-Technologien wird dies deutlich, da in diesem Bereich einheitliche Sicherheitsstandards noch keine flächendeckende Anwendung finden, wodurch das Risiko von Sicherheitslücken besonders groß ist. Hier gilt es, der Unwissenheit von Verbraucherinnen und Verbrauchern vorzubeugen und sie über die – gegebenenfalls auf den ersten Blick nicht sichtbaren – Sicherheitsrisiken solcher Endgeräte sowie sich weiterentwickelnden Angriffsmethoden von Cyberkriminellen aufzuklären. Wie im anschließenden Kapitel zu den Sicherheitsvorfällen am digitalen Verbrauchermarkt weiter veranschaulicht wird, entwickeln sich die angewandten Angriffsmethoden in allen technischen Bereichen weiter und bringen stets neue Sicherheitsrisiken mit sich. Aus diesem Grund sind aktuelle Informationen an Verbraucherinnen und Verbraucher über verschiedene Kanäle ein wesentlicher Baustein zur Prävention von Sicherheitsvorfällen im Verbraucherkontext.

Schadenslage durch Kriminalität und Schutzmaßnahmen im Cyber-Raum

Das Digitalbarometer 2020 mit seiner Bürgerbefragung zum Thema Cybersicherheit von BSI sowie der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK) umfasst eine Stichprobe von 2.000 Personen aus dem Ipsos Online-Access-Panel. Die als Web-Umfrage durchgeführte Studie zeigte, dass jede/jeder Vierte zum Opfer von Kriminalität im Internet geworden ist. Zu Schaden kamen dabei zirka zwei Drittel der betroffenen Personen. Ein besonderes Augenmerk liegt in diesem Kontext auf der Vielfalt an Schäden, die den Betroffenen zugefügt wurden: Neben monetären Schäden (32 %), spielten häufig auch der Verlust von Daten (23 %) und der Schaden durch das Wiederherstellen von Daten (23 %) eine Rolle. Auch emotionale Schäden, beispielsweise durch Cybermobbing, entstanden in einem Viertel der Fälle (25 %).

Straftat	Innerhalb der letzten 12 Monate	Straftaten die länger zurückliegen
Schadsoftware wie Viren und Trojaner	11 %	25 %
Phishing	17 %	15 %
Ransomware bzw. Erpressersoftware	6 %	10 %
Cybermobbing	10 %	6 %
Betrug beim Onlineshopping	44 %	28 %
Problematische Inhalte	8 %	6 %
Fremdzugriff auf einen Online-Account	30 %	23 %
Cyberstalking	8 %	6 %

Quelle:
Digitalbarometer: Bürgerbefragung zur Cybersicherheit. Kurzbericht zu den Umfrageergebnissen der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK) und des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

Info:
Die unterschiedlichen Schadensfälle zeigen, dass neben der materiellen auch die psychische Sicherheit der Verbraucherinnen und Verbraucher gestärkt werden muss. Selbsthilfeanleitungen sowie Orientierungshilfen tragen in diesem Umfeld zu einem digitalen Basisschutz bei.

Ein weiteres Ergebnis der Bürgerbefragung ist, dass sich trotz der Gefahrenlage für Verbraucherinnen und Verbraucher jede/jeder Zehnte ohne Schutzmaßnahmen im digitalen Raum bewegt. Ein aktuelles Virenschutzporogramm (57 %), sichere Passwörter (48 %) sowie eine aktuelle Firewall (47 %) waren bei den Personen, die sich vor Gefahren im Internet schützen wollten, die am häufigsten angewandten Maßnahmen. Auch die Verwendung von Zwei-Faktor-Authentisierung (33 %) und von sicheren Https-Verbindungen bei der Übertragung persönlicher Daten (31 %) waren Maßnahmen, die häufig zum Schutz ergriffen wurden.

Gleichermaßen konnten im Digitalbarometer Hinweise darauf gefunden werden, dass Verbraucherinnen und Verbraucher, die Sicherheitsempfehlungen direkt umsetzen, seltener Opfer von Kriminalität im Internet werden. Befragte, die bisher gar nicht oder nur einmalig Opfer wurden, gaben häufiger an, die Empfehlungen direkt umzusetzen (40 %).

Digitale Bedrohungen für Verbraucherinnen und Verbraucher durch COVID-19

Im Verlauf der COVID-19-Pandemie wurden einige analoge Angebote des Alltags, wie das Treffen mit Freunden, der Besuch von Veranstaltungen oder auch Shopping, durch digitale Formate ersetzt. Wie der Branchenverband Bitkom e. V. festgestellt hat, hielten seit dem Ausbruch der Pandemie digitale Freizeitangebote wie Onlineshopping, Videokonferenzen mit Freunden oder Musik- und Videostreaming-Dienste vermehrt Einzug in die Privathaushalte. Durch die telefonische Befragung von 1.003 Personen im April 2020 konnte Bitkom ermitteln, dass etwa die Hälfte der interviewten Internetnutzenden einen Musikstreamingdienst in Anspruch nahm (53 %) oder Online Games spielte (49 %). Etwa jeder dritte nutzte Streaming-Plattformen (37 %), um Videos oder Filme anzuschauen.

Das Bundeskriminalamt (BKA) wies im Bundeslagebild 2019 mit ihrer Sonderauswertung „Cybercrime in Zeiten der Corona-Pandemie“ nach, dass die gesellschaftlichen Veränderungen auch angepasste Formate von kriminellen Aktivitäten im Internet nach sich zogen. Im Beobachtungszeitraum von März bis August 2020 wurden zum Beispiel vermehrt gefälschte Webseiten und E-Mails in Umlauf gebracht, die mit einer „Corona-Soforthilfe“ warben. In weiteren Fällen gaben sich die Betrüger als Ärzte, Virologen aber auch Dienstleister, wie Paketlieferdienste, aus, um das hohe Informationsbedürfnis der Verbraucherinnen und Verbraucher zur Pandemie-Situation auszunutzen. So gingen laut Bericht allein bis Mitte September 2020 in Nordrhein-Westfalen mehr als 1.200 Strafanzeigen zu diesen Sachverhalten ein. Gestalterisch wurden die gefälschten Inhalte an Internetpräsenzen und Nachrichten staatlicher Stellen sowie wirtschaftlicher Akteure angelehnt. Zum Beispiel wurden Seitenlayouts von großen Banken nachgeahmt, um Seriosität bei Empfängerinnen und Empfängern der Nachrichten und Besucherinnen und Besuchern der Webseiten zu erwecken. Sofern betroffene Personen auf den Webseiten Schaltflächen betätigten oder Anhänge von E-Mails öffneten, führte dies zu einer Infektion ihres technischen Endgeräts mit Malware.

Die COVID-19-Pandemie zeigt, wie schnell und flexibel Cyberkriminelle agieren können. Die vielfältige Anwendung von Angriffswerkzeugen, darunter Phishing-Mails oder DDoS-Attacken auf digitale Angebote, bieten einen beispielhaften Einblick in die Gefahrenlage von Verbraucherinnen und Verbrauchern im virtuellen Raum.

4 Sicherheitsvorfälle auf dem digitalen Verbrauchermarkt

4 Sicherheitsvorfälle auf dem digitalen Verbrauchermarkt

Das Jahr 2020 ist ohne Zweifel von der COVID-19-Pandemie und den damit einhergehenden Veränderungen, Einschränkungen und Vorfällen geprägt. Doch auch abseits der Pandemie beobachtete das BSI zahlreiche Entwicklungen und Ereignisse im Bereich des digitalen Verbraucherschutzes, die bedeutende Auswirkungen auf die IT-Sicherheit von Verbraucherinnen und Verbrauchern hatten. Der digitale Verbrauchermarkt stellt sich dabei als durchweg komplex und hoch dynamisch dar. Stetiges Wachstum und eine kontinuierlich zunehmende Vernetzung prägen diese Entwicklung, die den digitalen Verbraucherschutz vor besondere Herausforderungen stellt: Zum einen gilt es, die zahlreichen Produkte und Dienstleistungen, die von Verbraucherinnen und Verbrauchern unmittelbar in Anspruch genommen werden, sicher zu gestalten. Desweiteren darf nicht übersehen werden, auch lediglich mittelbar dem digitalen Verbrauchermarkt zuzuordnende Produkte und Dienstleistungen abzusichern, wie beispielsweise die sogenannten „Kundendatenbanken". Nur eine derart integrierte Betrachtung aller relevanten Produkte und Dienstleistungen kann zu einer erfolgreichen Gestaltung des digitalen Verbraucherschutzes führen.

Es erfordert nur minimalen Rechercheaufwand, um hinsichtlich der Bedrohungslage für Verbraucherinnen und Verbraucher im digitalen Raum im Jahr 2020 fündig zu werden. Zu zahlreich waren die Vorfälle, die sich mittel- und unmittelbar auswirkten, wobei es starke Unterschiede in der Komplexität der Ursachen gab, jedoch fast immer schwerwiegende Folgen zu verzeichnen waren. Auf der einen Seite konnten, allein aufgrund vergleichsweise banaler Konfigurationsfehler am Server, online erreichbare Kundendatenbanken mit Millionen von Datensätzen ohne großen Aufwand abgerufen werden. Auf der anderen Seite befanden sich hoch komplexe Schwachstellen in Softwares, die einen Schaden für die Gesellschaft verursachten. Verbraucherinnen und Verbraucher waren diesen Vorfällen oftmals hilflos ausgeliefert, zumal aufgrund der technischen und teils komplexen Gegebenheiten keine Nachvollziehbarkeit erreicht werden konnte. Es ist folglich unerlässlich, Verbraucherinnen und Verbrauchern eine mögliche Betroffenheit bei derartigen Sicherheitsvorfällen verständlich darzulegen und zu erklären.

Neben den im Jahr 2020 ohnehin im Fokus stehenden Themen der digitalen Gesundheitsversorgung, die im nächsten Kapitel betrachtet werden sollen, gab es etliche Entwicklungen und Ereignisse auf dem digitalen Verbrauchermarkt. Zunächst konnte festgestellt werden, dass im Bereich der IoT-Anwendungen gehäuft über relevante Vorfälle berichtet wurde. Über Sicherheitslücken in konkreten Produkten hinaus wurden Schwachstellen in der zentralen Sicherheitsarchitektur von IoT-Geräten und Hardware im Allgemeinen entdeckt. An dieser Stelle wird bereits deutlich, welche Bedeutung dem Grundsatz „Security by Design" auch im digitalen Verbraucherschutz zukommt.

Die unter den Namen „Ripple20" und „Amnesia33" bekannt gewordenen Sammlungen von Sicherheitslücken in TCP/IP-Stacks stellen für Verbraucherinnen und Verbraucher eine besondere Herausforderung dar: Einerseits ist die technische Komplexität sehr hoch, was auch dazu führt, dass die eigene Betroffenheit selbst für versierte Nutzerinnen und Nutzer kaum erkennbar ist. Andererseits ist für viele der betroffenen Geräte nicht klar, wie diese das notwendige Update zur Schließung der Sicherheitslücken erhalten können. Hier liegt folglich ein schwerwiegendes Versäumnis im Sicherheitsdesign der Produkte vor, das Verbraucherinnen und Verbraucher letztendlich vor die Wahl zwischen der Nutzung unsicherer IoT-Geräte oder einem Neukauf potentiell sichererer Geräte stellt.

Ebenso stellt sich die Reaktionsbereitschaft der betroffenen Anbieter als problematisch dar: Im Dezember 2020 musste das BSI feststellen, dass sich von den 31 im September kontaktierten Unternehmen im Rahmen des Coordinated Vulnerability Disclosure (CVD)-Prozesses eine gewisse Anzahl gar nicht zurückgemeldet hat. Da nicht nur Verbraucherinnen und Verbraucher, sondern auch Unternehmen und kritische Infrastrukturen von den Sicherheitslücken betroffen waren, ist die mangelnde Kooperations- und Reaktionsbereitschaft hier von besonderer Tragweite. Nichtsdestotrotz zeigte der Vorfall, dass ein verantwortungsvoller Umgang mit Schwachstellen auch über Landesgrenzen hinweg funktionieren kann. Das BSI war dabei die federführende Behörde im europäischen Raum und konnte durch die vertrauensvolle Zusammenarbeit zwischen Staat und Wirtschaft in der Mehrzahl der Fälle den CVD-Prozess erfolgreich gestalten. Dieser Art von Kooperation bedarf es auch zukünftig, um Cybersicherheit und Verbraucherschutz in einem komplexen System wie dem europäischen Binnenmarkt wirksam umsetzen zu können.

Hintergrund: Ripple20 und Amnesia33

Experten der israelischen Sicherheitsfirma JSOF veröffentlichten im Juni 2020 gleich 19 Sicherheitslücken in der Implementierung eines Netzwerk- bzw. TCP/IP-Stacks, die sie unter dem Titel „Ripple20" zusammenfassten. Die Lücken konnten von Angreifern missbraucht werden, um Schadcode in die Geräte einzuschleusen und auszuführen oder um kritische Daten auszulesen. Im Dezember 2020 veröffentlichte das Security-Unternehmen Forescout die Untersuchung „AMNESIA:33", die 33 Schwachstellen in vier verschiedenen Open Source Netzwerk-Stacks beinhaltete. In beiden Fällen vermuteten die Entdecker die Betroffenheit von Millionen Geräten. Die betroffenen Anwendungen kommen in einer Vielzahl von Geräten wie Routern, Druckern oder Smart Home-Systemen bei zahlreichen namhaften Herstellern zum Einsatz.

Im Bereich der IoT-Geräte konnten im Jahr 2020 zahlreiche weitere Vorfälle beobachtet werden. Regelmäßig fanden Expertinnen und Experten Sicherheitslücken in beispielsweise vernetzen Türklingeln oder in sogenanntem „smartem" (vernetztem) Spielzeug. So berichtete eine auf Sicherheitsanalysen von IoT spezialisierte Firma in der Vorweihnachtszeit von über 7.000 Schwachstellen in gerade einmal sechs zufällig ausgewählten Produkten, darunter auch Kinderspielzeug. Es waren hierbei sowohl die Intim- bzw. Privatsphäre als Ganzes (Beispiel: eigene Wohnung), als auch vulnerable Gruppen (Beispiel: Kinder) von flächendeckenden IT-Sicherheitsmängeln im IoT-Bereich betroffen.

Die IKT-Erhebung „Private Haushalte in der Informationsgesellschaft" des Statistischen Bundesamtes (Destatis) aus dem Jahr 2020 stützte diese Annahme. So gaben zwei Prozent der Internetnutzenden an, dass sie mit dem Internet verbundenes Spielzeug (zum Beispiel Roboterspielzeug oder intelligente Puppen) für private Zwecke nutzen, wobei das Spielzeug am häufigsten in der jüngsten Altersgruppe von 10 bis 15 Jahren genutzt wird. Hier liegt der Anteil bei vier Prozent aller Befragten dieser Altersgruppe. Das Statistische Bundesamt betrachtete mit dem Internet verbundene Spielekonsolen separat von den oben genannten Spielzeugen. Hier gaben 22 Prozent der Internetnutzenden an, dass sie diese zuhause nutzen. Neben jungen Erwachsenen zählen auch hier Kinder und Jugendliche zur stärksten Verbraucherzielgruppe. Eine mit dem Internet verbundene Spielekonsole wird demnach von 52 Prozent der Befragten im Alter von 10 bis 15 Jahren genutzt. In der Altersgruppe der 16 bis 24-Jährigen gaben 49 Prozent der Befragten an, eine solche Konsole zu nutzen. In Anbetracht der jungen Zielgruppe für vernetztes Spielzeug und Spielekonsolen handelt es sich hier um eine überwiegend vulnerable Gruppe von Verbraucherinnen und Verbrauchern. Diese müssen hinsichtlich der IT-Sicherheit von internetfähigen Spielwaren unterstützt werden.

Altersgruppe (von ... bis ... Jahren)	Mit dem Internet verbundene Spielekonsole
10 - 15 %	52 %
16 - 24 %	49 %
25 - 44 %	31 %
45 - 64 %	8 %
65 Jahre und älter	2 %

Quelle:
Statistisches Bundesamt, 2021: Wirtschaftsrechnungen 2020. Private Haushalte in der Informationsgesellschaft – Nutzung von Informations- und Kommunikationstechnologien.

Über 7.000 Schwachstellen in nur sechs Produkten

Die auf die Sicherheit von IoT-Geräten spezialisierte IoT Inspector GmbH berichtete im Dezember 2020 von 7.339 Schwachstellen in einem Smart Speaker, einem Messenger für Kinder, einer Drohne, einem Smart Home-Kamerasystem, einer Haustier-Überwachungskamera sowie einem Streaming-Gerät für Kinder. Durch veraltete Software mit bekannten Sicherheitslücken, unsichere Fernwartungszugänge und mangelhafte Verschlüsselung wurden laut IoT Inspector „nicht einmal grundlegende Sicherheitseigenschaften" erfüllt. Unabhängig von der persönlichen Betroffenheit der Verbraucherinnen und Verbraucher stellen unsichere IoT-Geräte durch die Einbindung in Botnetze eine zusätzliche Gefährdung der öffentlichen Sicherheit dar.

Doch auch häufig nicht im unmittelbaren Fokus der Verbraucherinnen und Verbraucher stehende Produkte, wie WLAN-Router, fielen durch Mängel in der IT-Sicherheit auf. Die Stiftung Warentest stellte im März 2020 fest, dass knapp die Hälfte der von ihr untersuchten Router dahingehende Mängel aufwiesen. Diese Einschätzung wurde vom Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE) im „Home Router Security Report 2020" bestätigt. In allen 127 untersuchten Geräten konnte das FKIE Fehler finden. Einige Router wiesen über 100 Schwachstellen auf. 46 Router hatten seit mindestens einem Jahr keine Sicherheits-Updates mehr erhalten. In einem Extremfall fanden die Forscherinnen und Forscher seit fast fünfeinhalb Jahren kein Update, obwohl die betrachteten Geräte zum Zeitpunkt des Reports noch im Handel erhältlich waren.

Als Herzstück eines jeden vernetzen Haushalts kommt den Routern eine besondere Bedeutung für die IT-Sicherheit zu. Sie stellen einerseits die zentralen Zugangspunkte zum Internet und andererseits die zentralen Verteilplattformen zu den netzinternen Endgeräten dar und sind damit das wichtigste Nadelöhrfür den gesamten Datenverkehr eines digitalen Haushalts. Es wäre folglich unsinnig, die Sicherheit von IoT-Geräten isoliert zu verbessern und den Router außer Acht zu lassen. Dieses Umstandes ist sich das BSI bewusst und veröffentlichte im Juli 2020 die Prüfspezifikation zur Technischen Richtlinie für Breitband-Router. Mit der Fertigstellung der Prüfspezifikation sind alle formellen Voraussetzungen für die Zertifizierung von Routern gemäß der Ende 2018 veröffentlichten Technischen Richtlinie erfüllt. Daneben haben auch Hersteller die Möglichkeit, ihre eigenen Produkte strukturiert auf die Konformität zu den Anforderungen der Technischen Richtlinie zu überprüfen und in Verbindung mit einer Herstellererklärung das geplante IT-Sicherheitskennzeichen zu nutzen. Auf diese Weise können die komplexen Sicherheitsanforderungen für Verbraucherinnen und Verbraucher transparent und sichtbar gemacht werden, so dass IT-Sicherheit eine gleichberechtigte Rolle beim Kauf eines Produktes spielen kann.

Home Router Security Report 2020

Das Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE) hat in 127 getesteten Routern für Privatnutzer von sieben großen Herstellern Sicherheitsmängel festgestellt. Nach Angaben der Forscherinnen und Forscher waren diese teilweise sehr erheblich und reichten von fehlenden Sicherheits-Updates, über einfach zu entschlüsselnde, hartkodierte Passwörter bis hin zu bereits bekannten Schwachstellen, die eigentlich längst behoben sein müssten.

Eine weitere im Jahr 2020 betrachtete IoT-Produktkategorie waren die Smart-TVs. Das Bundeskartellamt (BKartA) veröffentlichte im Juli eine Sektoruntersuchung, die insbesondere die Datennutzung und -verarbeitung bei vernetzten Fernsehgeräten ins Auge fasste. Doch auch die Sicherheitseigenschaften waren Teil der Publikation. So fand das BKartA heraus, dass die Mehrheit der Hersteller vor allem nach dem Verkauf des Produktes aktiv mit Sicherheitsmängeln umgeht. Deutlich weniger Hersteller sorgen vor und setzen bereits in der Produktentwicklung an, um Sicherheitsmängel zu verhindern. Umfassende Qualitätssicherungssysteme über alle Marktstufen sind die Ausnahme und die Maßnahmen der Hersteller zur Gewährleistung der IT-Sicherheit – was Aufwand, Intensität

und Regelmäßigkeit angeht – sehr unterschiedlich. Ferner fand das BKartA heraus, dass bei einem neu auf den Markt kommenden Smart-TV für ca. 27 Monate mit Sicherheits-Updates gerechnet werden kann. Folglich wäre ein TV-Modell des vorletzten Jahres bereits beim Kauf nach einer verhältnismäßig kurzen Zeit unsicher. Hinsichtlich der Verfügbarkeit von Updates soll die Umsetzung der Warenkaufrichtlinie zukünftig für einen besseren Verbraucherschutz sorgen. Nichtsdestotrotz bleibt der vom BKartA festgestellte Sachverhalt, dass IT-Sicherheit im Entwicklungsprozess häufig keine oder nur eine nachgeordnete Rolle spielt, eine große Herausforderung für den digitalen Verbraucherschutz.

Laut IKT-Erhebung des Statistischen Bundesamtes (Destatis) nutzten im Jahr 2020 mehr als die Hälfte der Verbraucherinnen und Verbraucher mit Internetanschluss Smart-TVs im privaten Kontext (52 Prozent). Auffällig ist, dass die Produktkategorie unabhängig von Alter, Geschlecht und Bildungsstand in nahezu allen Bevölkerungsgruppen vertreten ist. Befragte im Alter über 65 Jahre machen mit rund einem Viertel die kleinste Gruppe der Nutzerinnen und Nutzer von Smart-TVs aus. Die Ergebnisse zeigen jedoch, dass die Geräte bereits tief in der privaten Nutzung verankert sind, wodurch der dringende Bedarf an IT-Sicherheitsmaßnahmen zum Schutz dieser vergleichsweise großen Zielgruppe deutlich wird.

Altersgruppe (von ... bis ... Jahren)	Mit dem Internet verbundene Fernsehgeräte (Smart-TV) für private Zwecke zuhause genutzt
10 - 15 %	60 %
16 - 24 %	63 %
25 - 44 %	64 %
45 - 64 %	47 %
65 Jahre und älter	28 %

Quelle:
Statistisches Bundesamt, 2021: Wirtschaftsrechnungen 2020. Private Haushalte in der Informationsgesellschaft – Nutzung von Informations- und Kommunikationstechnologien.

Die unzureichende Bedeutung von „Security by Design" zieht sich wie ein roter Faden durch das Themengebiet IoT, aber auch durch andere Gebiete der Informationstechnik. Die schiere Masse an gefundenen Sicherheitslücken zeigt, dass die IT-Sicherheit im Entwicklungsprozess keinesfalls die Berücksichtigung gefunden hat, die für ein ganzheitlich sicheres Produkt notwendig wäre. Damit wird auf der Anbieterseite ein grundlegender Mangel an Anreiz offenbar, einen durchgehenden IT-Sicherheitsaspekt im Produkt-Lebenszyklus systematisch zu verankern. Mitunter sind die Motive und Kompetenzen der Anbieter im Einzelnen intransparent oder schlichtweg nicht nachvollziehbar (Herstellungs- und Betriebskosten, geltende Haftungs- und Sanktionsregime, Wissen u. v. m.). Dies zeigen besonders profane Beispiele, in denen einfachste und aufwandsarme Maßnahmen vernachlässigt wurden. So fand die Stiftung Warentest bei einer Untersuchung der Software von Fotobuchanbietern heraus, dass in mehreren Fällen ein einziges Zeichen als Passwort akzeptiert wurde. Mit Blick auf die Sensibilität von privaten Fotoaufnahmen erscheint dieser Umstand untragbar, zeigt jedoch die digitale Sorglosigkeit, die an vielen Stellen noch vorherrscht. Diese Sorglosigkeit erstreckt sich sowohl auf Anbieter als auch Verbraucherinnen und Verbraucher. Ein weiteres Beispiel hierfür ist, dass mehr als 8 Prozent der eingesetzten Windows-Betriebssysteme in Deutschland Ende 2020 noch „Windows 7" verwenden. Dies entspricht in etwa 4 Millionen Systemen, die seit dem 14. Januar 2020 nicht mehr kostenfrei mit Sicherheits- oder Feature-Updates versorgt werden und somit fortschreitend verwundbarer werden, sofern dieser Support nicht zugekauft wird.

Ein in Teilen ebenfalls nachlässiger Umgang mit IT-Sicherheit lässt sich im zweiten großen Bereich feststellen, der im Jahr 2020 den digitalen Verbrauchermarkt geprägt hat: Kundendatenbanken. Eine Vielzahl von Vorfällen über alle Branchen hinweg sorgte für die millionenfache Veröffentlichung und Verbreitung von persönlichen oder personenbeziehbaren Daten, die gerade durch deren Verknüpfbarkeit über mehrere Datenquellen ein kaum kalkulierbares Schadensfeld aufspannen. Diese Datenbanken liegen in der Regel außerhalb des Einflussbereiches der Verbraucherinnen und Verbraucher, so dass diese den Anbietern und deren nicht regelmäßig nachprüfbaren Sicherheitsversprechen faktisch ausgeliefert sind, sobald sie eine Dienstleistung in Anspruch nehmen. Praktisch alle digitalen Dienstleistungen für eine größere Zielgruppe von Verbraucherinnen und Verbrauchern kommen nicht ohne Kundendatenbanken aus. Eben jene sind

jedoch häufig entweder per se mangelhaft oder aufgrund vergleichsweise einfacher Konfigurationsfehler angreifbar. Besonders problematisch ist hierbei die hohe Anzahl an Betroffenen durch einzelne Fehler: Während bei einem Angriff auf ein unsicheres IoT-Gerät i. d. R. einzelne Anwenderinnen und Anwender das Ziel sind und so der Schaden begrenzt wird, führt ein erfolgreicher Angriff auf eine Kundendatenbank zu teilweise millionenfacher Betroffenheit. Ferner ist die Art des Schadens zu unterscheiden, denn einmal entwendete Daten gelten quasi als dauerhaft und weltweit veröffentlicht und können nicht mehr in den vorherigen, geschützten Zustand überführt werden, so wie es durch die Bereinigung eines infizierten Systems ggf. möglich ist.

Die besondere Tragweite dieser Schadensart machen sich die Täter zunutze. Die Technischen Werke einer Stadt in Rheinland-Pfalz waren im April und Mai 2020 von einem Angriff betroffen, dem eine Forderung der mutmaßlichen Urheber im zweistelligen Millionenbereich folgte, ansonsten drohe eine Veröffentlichung der entwendeten Daten. Betroffen waren Kundinnen und Kunden sowie geschäftliche Kontakte der Stadtwerke in Form von personenbezogenen Daten (Namen, Adressen, Kontaktdaten). Es handelte sich demnach um einen gezielten Angriff, der trotz vorhandener Sicherheitsmaßnahmen zum Erfolg führte. Eine solche Vorgehensweise kann nie gänzlich ausgeschlossen werden, doch kann durch umfassende und ganzheitliche Sicherheitsmaßnahmen eine deutliche Risikominimierung auf ein vertretbares Maß erfolgen.

Weitaus vermeidbarer waren hingegen andere Vorfälle im Bereich der Kundendatenbanken. Durch einen falsch konfigurierten Server waren im Januar 2020 ca. 3 Millionen Kundendaten einer Autovermietung im Internet einsehbar - ein Vorfall, der mit der gebotenen Sorgfalt nicht hätte stattfinden müssen. Zu den Betroffenen zählten unter anderem zahlreiche Persönlichkeiten aus Politik und Verwaltung, so auch der Präsident des BSI, Arne Schönbohm.

BSI-Präsident Arne Schönbohm zum Vorfall bei einer Autovermietung gegenüber der Wochenzeitung "Die ZEIT":

> *„Der Fall zeigt leider, dass auch sehr sensible, personenbezogene Daten immer wieder nur unzureichend geschützt werden. Egal ob ich – wie in diesem Fall – persönlich betroffen bin oder nicht, solche Fälle ärgern mich sehr, weil sie vermeidbar wären."*

Ein Vorfall mit vergleichbarer Ursache wurde fast zeitgleich im Januar 2020 bekannt und zeigte, dass auch bei IT-affinen Unternehmen Nachlässigkeiten in der Konfiguration von Servern möglich sind. So waren im Dezember 2019 circa 250 Millionen Datensätze aus dem Supportbereich eines der weltweit größten Softwarekonzerne im Internet einsehbar. Im November des Jahres war es dann ein auf IT-Sicherheit spezialisiertes Unternehmen in Großbritannien, das versehentlich Kundendaten preisgab. Vorkommnisse wie diese stellen grundsätzlich das Vertrauen von Verbraucherinnen und Verbrauchern gegenüber den Unternehmen in Frage. Doch für die Erbringung von erwarteten und im Verbrauchermarkt nachgefragten digitalen Dienstleistungen ist eine vollständige Vermeidung sensibler Kundendatenbanken nicht möglich. Das Gebot der Datensparsamkeit und Zweckgebundenheit der Datenverarbeitung bleibt davon unbenommen. Folglich ist die Absicherung von Kundendatenbanken ein integraler Bestandteil des Erfolgs von digitalem Verbraucherschutz.

5 Schwerpunkt: COVID-19-Pandemie und Gesundheits-Apps

5 Schwerpunkt: COVID-19-Pandemie und Gesundheits-Apps

Zum Jahreswechsel 2018/2019 wurde ein finnisches Psychotherapiezentrum Opfer eines Cyberangriffs durch Unbekannte. Dieser Vorfall wurde erst im Oktober 2020 publik, als erste Datensätze von Patientinnen und Patienten veröffentlicht wurden. Die Täter wendeten sich mit einem Erpresserschreiben sowohl an das Zentrum, als auch an die Patientinnen und Patienten. Sollten die finanziellen Forderungen nicht erfüllt werden, drohten sie mit der Veröffentlichung weiterer hochsensibler Daten, unter anderem Kontaktinformationen, Diagnosen und Tagebücher. Unter den Betroffenen waren auch Minderjährige.

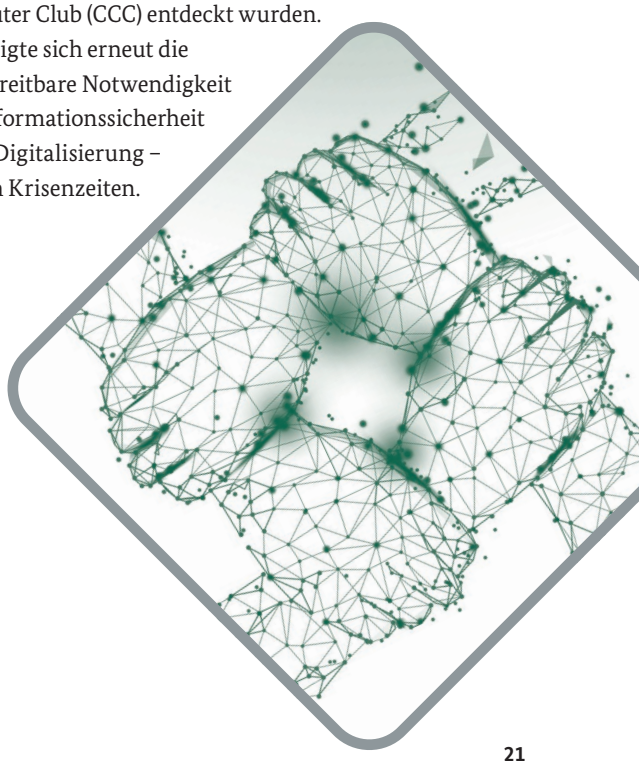
Fälle wie dieser stehen exemplarisch für die Gefahren, die mit unsicheren IT-Systemen im Gesundheitsbereich einhergehen. Anders als bei Vorfällen wie zum Beispiel im Finanzsektor können entstandene Schäden nicht einfach ersetzt werden. Die Daten werden unter Umständen durch Dritte unkontrolliert weiterverbreitet und können für weitere Straftaten verwendet werden. Häufig handelt es sich dabei um mehr als lediglich Kontaktinformationen – nämlich um persönliche Informationen aus der medizinischen und gesundheitlichen Intimsphäre der betroffenen Menschen.

Doch wie überall in der IT-Sicherheit ist nicht nur die Vertraulichkeit ein Schutzziel der besonders schützenswerten Daten und Dienste im Gesundheitsbereich, auch die Integrität und Verfügbarkeit spielen eine besondere Rolle. Allein die Vorstellung, gesundheitliche oder medizinische Daten würden durch äußere Einflussnahme verfälscht oder stünden im entscheidenden Moment nicht zur Verfügung, hebt die Bedeutung dieser Schutzziele der IT-Sicherheit hervor. Leider wurde diese Vorstellung im Berichtsjahr 2020 realisiert, so zum Beispiel bei der durch einen Cyberangriff eingeschränkten Arbeitsfähigkeit des Universitätsklinikums Düsseldorf im September 2020.

Die Relevanz verlässlicher und sicherer Informationstechnik im Gesundheitswesen und der medizinischen Infrastruktur dürfte auch vor der COVID-19-Pandemie unbestritten gewesen sein. Jedoch boten die mit der Pandemie einhergehenden Unsicherheiten und Veränderungen ein Einfallstor für Cyberangriffe und -kriminalität in zahlreiche Lebensbereiche der Verbraucherinnen und Verbraucher.

Das BSI beobachtete im Zuge der COVID-19-Pandemie unterschiedliche Kampagnen mit cyberkriminellem Hintergrund, die sich die komplexe Gesamtsituation rund um COVID-19 zunutze machten. Hierzu zählen beispielsweise Phishing- und Schadprogramm-Kampagnen, CEO-Fraud und Betrugsversuche mit IT-Mitteln, auch allgemein Scam genannt. Die von Ängsten, Sorgen und Unsicherheit geprägte Stimmung in weiten Teilen der Bevölkerung hätte die Erfolgsaussichten solcher Angriffe zwar begünstigen können, unerwartet große Häufungen traten jedoch nicht auf. Gleichzeitig sorgte der mit der Pandemie einhergehende Digitalisierungsschub für größere Angriffsflächen. Ausgangsbeschränkungen, Schul- und Geschäftsschließungen, Abstandsregeln – die politischen Maßnahmen gegen die COVID-19-Pandemie führten zu weitreichenden Einschränkungen der alltäglichen Lebensführung der Verbraucherinnen und Verbraucher. In vielen Fällen waren digitale Lösungen das Mittel der Wahl, um elementare Geschäftsprozesse und zwischenmenschliche Beziehungen aufrecht zu erhalten. Arbeiten im Home-Office, Online-Unterricht, Einkaufen im Internet und Video-Chats mit sozialen Kontakten führten zu einer beispiellosen Welle der Digitalisierung vieler Lebensbereiche. Die umfassende und plötzliche Mehrnutzung von digitalen Produkten und Diensten eröffnete Angreifern eine stark vergrößerte Angriffsfläche für ihre kriminellen Aktivitäten (siehe auch die BSI-Publikation „Die Lage der IT-Sicherheit in Deutschland 2020").

Deutlich wurden an dieser Stelle nochmals die hohe Dynamik der Digitalisierung und auch die sich kontinuierlich und schnell verändernden Anforderungen an den digitalen Verbraucherschutz. Wie bereits benannt, sind es oftmals längst bekannte Probleme, die nur unter anderen Rahmenbedingungen erneut auftreten. So zum Beispiel unzureichend gesicherte Kundendatenbanken zur Kontaktnachverfolgung in Gastronomiebetrieben, die durch den Chaos Computer Club (CCC) entdeckt wurden. Hier zeigte sich erneut die unbestreitbare Notwendigkeit von Informationssicherheit in der Digitalisierung – auch in Krisenzeiten.



CCC entdeckt Sicherheitslücken in digitalen Corona-Listen

Mitglieder des Chaos Computer Club (CCC) entdeckten im August gravierende Sicherheitslücken in einem Cloud-System, das zur Kontaktnachverfolgung während der COVID-19-Pandemie in gastronomischen Betrieben genutzt wurde. Der Zugriff auf die Datenbank erlaubte das Auslesen von Datensätzen zu 4,8 Millionen Personen und 5,4 Millionen Reservierungen, ferner Informationen zu Umsätzen und Bestellungen. Der Datenbestand reichte nach Angaben des CCC bis zu zehn Jahre zurück. In der jüngsten Vergangenheit konnten 87.313 COVID-19-Kontakterhebungen von 180 Restaurants gefunden werden. Ursächlich für die Sicherheitslücken waren ein mangelndes Rechtemanagement sowie unzureichend geschützte Passwörter, so der CCC.

Eine weitere Herausforderung für das BSI stellte die Entwicklung der Corona-Warn-App dar. Die Behörde begleitete die Entwicklung der App von Beginn an in beratender Funktion und führte unter anderem Code Reviews und Penetrationstests des zur Verfügung gestellten Codes von Frontend und Backend durch. Die Umsetzung von „Security by Design“ erhielt so, basierend auf der Technischen Richtlinie „Sicherheitsanforderungen an digitale Gesundheitsanwendungen" (BSI TR-03161), höchste Priorität. Die TR-03161 wurde bereits im April 2020 veröffentlicht und bildet die Grundlage für eine sichere Verarbeitung sensibler und besonders schützenswerter Daten in mobilen Anwendungen. Die Technische Richtlinie kann seit der Veröffentlichung genutzt werden, um die entsprechenden Anforderungen des Zulassungsverfahrens des Bundesinstituts für Arzneimittel und Medizinprodukte (BfArM) durch eine Selbsterklärung der Entwicklerinnen und Entwickler zu erfüllen.

Dass Gesundheits-Apps im Allgemeinen einen erhöhten Schutzbedarf haben, dürfte unbestritten sein. Aus diesem Grund untersuchte das BSI im Rahmen der Marktbeobachtung jene Art von Apps, die keiner besonderen Regulierung unterliegen, also kein Medizinprodukt sind bzw. nicht im DiGA-Verzeichnis gelistet werden. Ziel der Studie war es, einen Überblick über den Markt der Gesundheits-Apps zu erhalten sowie mögliche Trends zu identifizieren. Darüber hinaus sollten potentielle IT-sicherheitstechnische Risiken für Verbraucherinnen und Verbraucher aufgezeigt und darauf basierend Handlungsbedarfe und -empfehlungen für Staat, Wirtschaft und Gesellschaft abgeleitet werden.

Die hohe Dynamik des Digitalmarktes erforderte dabei zunächst eine genaue Marktanalyse, da es beispielsweise keine einheitliche Definition gibt, welche Anwendungen zu den Gesundheits-Apps zählen. Dazu analysierte das BSI in Zusammenarbeit mit der Cassini Consulting AG zunächst verschiedene Marktdaten sowie bereits veröffentlichte Studien und führte Interviews mit Branchenexpertinnen und Branchenexperten.

Zentrale Erkenntnisse waren dabei verschiedene Definitionsversuche der Gesundheits-Apps aus unterschiedlichen Marktperspektiven und eine funktionale Marktsegmentierung. Insgesamt konnte festgestellt werden, dass der Markt in diesem Bereich eine hohe Intransparenz und Dynamik aufweist. Stetige Veränderungen sowie Weiterentwicklungen von Angeboten gehen mit einer unklaren Lage für Verbraucherinnen und Verbraucher einher, wie es um IT-Sicherheit und auch Datenschutz bestellt ist. Ursächlich dafür dürften die hohen Potenziale des Marktes in Verbindung mit geringen Markteintrittshürden sein. Gleichzeitig kann jedoch ein kontinuierliches Wachstum des Marktes beobachtet werden, ebenso wie die stetige Erweiterung der Funktionen von Anwendungen. Diese technologische Entwicklung wird durch datengetriebene Lösungen und Künstliche Intelligenz weiter vorangetrieben.

Im Anschluss an diese Analyse folgte eine IT-sicherheitstechnische Betrachtung von konkreten Gesundheits-Apps. Dazu wurden insgesamt 84 Anbieter zwischen Ende 2020 und Anfang 2021 online befragt sowie eine technische Untersuchung von sieben ausgewählten Apps durchgeführt.

Inhalt der Befragung waren die Maßnahmen, die seitens der Anbieter zur Gewährleistung der IT-Sicherheit ihrer Anwendungen durchgeführt wurden. Dabei konnte festgestellt werden, dass der Grundsatz „Security by Design“ nur in Teilen Einzug in den Entwicklungsprozess der betrachteten Gesundheits-Apps gefunden hat. Fehlende Prozesse für Updates und den Umgang mit Schwachstellen gingen einher mit einer unzureichenden Umsetzung technischer und organisatorischer Maßnahmen. Zwar gaben alle Befragten an, gewisse grundlegende Maßnahmen der IT-Sicherheit umzusetzen, in Anbetracht der Kritikalität der verarbeiteten Daten in Gesundheits-Apps muss aber davon ausgegangen werden, dass im Regelfall kein ganzheitlicher und somit angemessener Schutz gewährleistet werden kann.

Diese Annahme wurde in der technischen Untersuchung von sieben ausgewählten Apps bestätigt. Obwohl nur eine oberflächliche Prüfung der Sicherheitseigenschaften vorgenommen wurde, konnten die Anbieter lediglich eine Auswahl grundsätzlicher Anforderungen erfüllen. Sie deckten diese somit in keinem der Fälle in einer Art und Weise ab, wie es nach dem Stand der Technik zu erwarten gewesen wäre. So wurden beispielsweise bei sechs der Anwendungen die Passwörter nicht in gehashter Form, sondern als Klartext übertragen. Auch „Man in the Middle-Angriffe“ waren durch in fast allen Fällen fehlendes „Certificate Pinning“ möglich, was das Abfangen, Auslesen und Manipulieren der Kommunikation zwischen App und dem Cloud Backend ermöglichte.

Die vollständigen Analysen und Ergebnisse sind in der Studie „IT-Sicherheit auf dem digitalen Verbrauchermarkt: Fokus Gesundheits-Apps“ auf der Webseite des BSI nachzulesen.

Zusammenfassend lässt sich feststellen, dass trotz der hohen Schutzbedürftigkeit sensibler Daten im Gesundheitsbereich an zahlreichen Stellen noch Nachholbedarf in Fragen der IT-Sicherheit besteht. Es muss an dieser Stelle Anliegen von Staat, Wirtschaft und Gesellschaft sein, diese Missstände zu beseitigen. Der Ansatz von „Security by Design“ stellt dabei eine der zentralen Komponenten zur erfolgreichen Digitalisierung des Gesundheitsbereichs dar, da nur so ganzheitliche IT-Sicherheit gewährleistet werden kann.

6 Gestaltungsräume und Ausblick

6 Gestaltungsräume und Ausblick

Wie sich bereits in den vorherigen Kapiteln abgezeichnet hat, war das Jahr 2020 von gesundheitlichen, gesellschaftlichen und wirtschaftlichen Herausforderungen geprägt, die sich nachhaltig in der digitalen Lebenswelt der Verbraucherinnen und Verbraucher abzeichneten. Mit Blick auf das Jahr 2021 und die bereits sichtbaren gesellschaftlichen Entwicklungen kann davon ausgegangen werden, dass die hohe Komplexität des digitalen Verbrauchermarktes zukünftig weiter zunehmen wird. Der technologische Fortschritt und das immer größer werdende Angebot an neuen digitalen Verbraucherprodukten und -diensten trägt genauso zu dieser Entwicklung bei, wie die weiterhin angespannte Pandemiesituation und der daraus resultierende Bedarf nach technologischen Hilfsmitteln zur Gestaltung des Alltags. Um diesen hoch dynamischen Markt mit seinen schnelllebigen Trends zukünftig sicherer gestalten zu können, wurden aus den Vorfällen und Studienergebnissen des Jahres 2020 zentrale Handlungsfelder und Vorgehensweisen abgeleitet, die zur zukünftigen Ausgestaltung des digitalen Verbraucherschutzes beitragen.

Die Gestaltung einer sicheren Digitalisierung zum Nutzen der Verbraucherinnen und Verbraucher verfolgt das BSI u. a. durch den Austausch mit den Herstellern in Richtung sichere Produkte aber auch durch den Dialog mit Verbraucherzentralen. Weitere Kooperationen innerhalb von Staat, Wirtschaft und Gesellschaft tragen zur Erhöhung der IT-Sicherheit Einzelner sowie zur öffentlichen Sicherheit im Allgemeinen bei. Gleichzeitig adressiert das BSI Verbraucherinnen und Verbraucher unmittelbar und bietet umfangreiche Informationen zur Umsetzung von Schutzmaßnahmen im Alltag an.

6.1: Handlungsfelder des digitalen Verbraucherschutzes aus dem Jahr 2020

Die zunehmende Digitalisierung und Vernetzung des Gesundheitswesens trägt dazu bei, Abläufe zu optimieren. Vor allem im medizinischen Kontext fallen hochsensible Daten einzelner Personen an, die einen erhöhten Schutzbedarf mit sich bringen. Doch auch außerhalb des professionellen Gesundheitssektors, beispielsweise bei der Verwendung von privaten Gesundheits-Apps, fallen Daten von gleicher Wertigkeit an. Laut Digitalbarometer sind ein Drittel aller durch Kriminalität im Internet entstandenen Schäden monetärer Art, die durchschnittlich um die 100 Euro betragen und im Einzelfall durch Versicherungen ersetzt werden. Darüber hinaus lässt sich die Veröffentlichung von personenbezogenen Gesundheitsdaten nicht einfach rückgängig machen. Beispielsweise können sensible Daten wie Medikationspläne, Pulsfrequenz-, Schlafrhythmus- oder Tagebuchdaten bei Veröffentlichung oder unbemerkter Manipulation zu erheblichen Schäden führen. Aus diesem Grund sollten technische Endgeräte von Verbraucherinnen und Verbrauchern sowie die laufenden Anwendungen der Anbieter von Gesundheitsdienstleistungen ein gehobenes Maß an Sicherheit vorweisen. Es ist essentiell, dass Betreiber solcher Systeme, sowohl im medizinischen als auch im wirtschaftlichen Sektor, die für ihre Dienstleistungen notwendigen Systeme und Prozesse bestmöglich absichern.

Auch die Sicherheit von (Kunden-) Datenbanken muss erheblich gestärkt werden. Verbraucherinnen und Verbraucher unterliegen hier einer gewissen Handlungsohnmacht, da sie nur bedingt Einfluss darauf haben, auf welche Art und Weise Hersteller und Dienstleister die bereitgestellten Kundendaten speichern und absichern. Die Sicherheitsvorfälle aus dem Jahr 2020 in diesem Themenspektrum zeigen, dass Dienstanbieter die Daten ihrer Kunden besser schützen müssen, und auch der Zugangsschutz zu Online-Diensten aus Kundenperspektive verstärkt werden sollte. Oftmals ist das Bekanntwerden von Kundendaten ein Einfallstor für weitere kriminelle Aktivitäten im Cyber-Raum, da persönliche Daten wie E-Mail-Adressen für Identitätsdiebstahl oder Kontaktadressen für die Verbreitung von Phishing und Schadprogrammen genutzt werden. Auch wenn Verbraucherinnen und Verbraucher mit Maßnahmen wie Datensparsamkeit solchen Vorfällen vorbeugen können, obliegt die sichere Verwahrung der Kundeninformationen den Organisationen, die diese erhalten.

Die Gestaltung von sicheren IoT-Produkten und -Diensten wurde bereits als zusätzliches Handlungsfeld im Rahmen der Sicherheitslage in den vorherigen Kapiteln identifiziert. Hier bedarf es der Umsetzung eines angemessenen Sicherheitsniveaus seitens der Hersteller, um beispielsweise dem Aufbau von Botnetzen über IoT- und IT-Geräte entgegenzuwirken. Wie bereits in den vorangegangenen Kapiteln benannt wurde, dient die Router-TR als Wegbereiter auf diesem Gebiet. Aber auch der im vergangenen Sommer veröffentlichte IoT-Basisstandard (ETSI EN 303 645) stellt einen wichtigen Meilenstein zur Erhöhung der I(o)T-Sicherheit und eine Richtschnur für die Hersteller dar. Er gilt als international anerkannte Messlatte zur Beurteilung, ob IoT-Geräte für den Verbrauchermarkt

über ein Mindestmaß an Cybersicherheit verfügen. Für eine korrekte Anwendung legt die Prüfspezifikation ETSI TS 103 701 fest, wie eine Konformitätsbewertung von IoT-Produkten für Verbraucherinnen und Verbraucher anhand der Anforderungen von EN 303 645 durchgeführt werden kann, um die Vergleichbarkeit der Bewertungsergebnisse, z. B. durch Herstellererklärungen in Verbindung mit dem geplanten IT-Sicherheitskennzeichen, zu gewährleisten. Ein weiteres Beispiel aus dem alltäglichen Gebrauch sind Smartphones, die als zentrales Steuerelement für Alltagsabläufe genutzt werden können. Auch hier wird anhand des BSI-Anforderungskataloges über mehr Sicherheit beim Handy ab Werk diskutiert. Unter dem Schlagwort „Security by Design" wird diese Vorgehensweise im Folgenden weiter ausgeführt. Dennoch ist gerade im Bereich der smarten Endgeräte zu berücksichtigen, dass zahlreiche Daten über die unterschiedlichen Produkte und Apps geteilt werden. Die Vernetzung einzelner Geräte und Dienste untereinander durch die Verbraucherinnen und Verbraucher ist eine weitere Herausforderung bei der sicheren Gestaltung von privaten IoT-Lösungen. Die Bereitstellung von praxisbezogenen, verständlichen Informationen für Verbraucherinnen und Verbraucher zum sicheren Umgang mit dem Internet of Things spielt hierbei eine zentrale Rolle.

6.2: Vorgehensweisen zur Stärkung des digitalen Verbraucherschutzes

Um die sichere Ausgestaltung der geschilderten Handlungsfelder anzugehen, müssen alle für den digitalen Verbraucherschutz relevanten Akteure aus Staat, Wirtschaft und Gesellschaft zusammenarbeiten. Zur Schaffung eines sicheren digitalen Privatumfelds müssen Verbraucherinnen und Verbraucher Cyberkriminialität nicht mehr als abstraktes Konstrukt, sondern als konkrete Bedrohung wahrnehmen. Gleichermaßen sollten die Bemühungen zu sicherheitsorientiertem und selbstbestimmten Handeln in der digitalen Welt etabliert, und entsprechende Unterstützungsmaßnahmen bereitgestellt werden. Die Empfehlungen sollten so formuliert sein, dass diese niedrigschwellig kommuniziert und direkt umgesetzt werden können. So wird Einzelpersonen und Haushalten ein leichter Einstieg in den Aufbau eines sicheren IT-Umfeldes ermöglicht. Zum Beispiel müssen die Fragen, welche Sicherheitsmaßnahmen priorisiert und im Zusammenspiel genutzt werden sollten, in der Kommunikation zwischen Institutionen sowie im Dialog mit Verbraucherinnen und Verbrauchern beantwortet werden. Die Bereitstellung von Selbsthilfe-Anleitungen und Orientierungsmöglichkeiten, wie einem IT-Sicherheitskennzeichen, durch wirtschaftliche und staatliche Akteure bietet die Chance, Verbraucherinnen und Verbrauchern bei der Umsetzung von IT-Basisschutz für den privaten Gebrauch zu unterstützen.

Die Bereitstellung von verlässlichen, geprüften und verständlichen Informationen von IT-Expertinnen und -Experten, auf die sich Verbraucherinnen und Verbraucher verlassen können, ist zentraler Bestandteil des digitalen Verbraucherschutzes.

Die sorgfältige Handhabung und konsequente Umsetzung von IT-Sicherheitsmaßnahmen ist für Hersteller und Privatpersonen gleichermaßen äußerst relevant. Hersteller müssen im Rahmen der Qualitätssicherung von Geräten und Diensten schnellstmöglich auf Sicherheitslücken reagieren. Zentrales Element bei diesen Vorgehensweisen ist die Zeitkomponente, sodass nach Bekanntwerden von Sicherheitsvorfällen und -risiken schnellstmöglich weitere Handlungsschritte ergriffen werden können, um größere Schäden und Gefährdungslagen zu vermeiden. Ziel sollte sein, flächendeckende Maßnahmen zur Problembehebung und Updates für betroffene Produkte bereitzustellen, um die aktive Ausnutzung von Schwachstellen durch Kriminelle zu verhindern. Gleichermaßen müssen Verbraucherinnen und Verbraucher über potentielle Risiken aufgeklärt werden. So ist zum Beispiel bekannt, dass Sicherheits-Updates in manchen Fällen über lange Zeiträume hinweg ignoriert werden, wodurch unbewusst erhebliche Risiken eingegangen werden. Besonders Sicherheitslücken, die über das Internet zugänglich sind, können leicht von Angreifern ausgenutzt werden. Daher sollten Verbraucherinnen und Verbraucher entsprechende Informationen von Herstellern und Providern ernst nehmen und frühzeitig handeln.

Das Mitdenken von Sicherheitsanforderungen an Soft- und Hardware während der Entwicklungsphase eines Produktes, ist eine weitere Vorgehensweise, die zur Stärkung des digitalen Verbraucherschutzes beiträgt. Unter dem Stichwort „Security by Design" wird Sicherheit von Anfang an mitgedacht, so dass Sicherheitslücken gar nicht erst entstehen. Die zunehmende Vernetzung von Geräten und der verstärkte Einsatz von Sensortechnik in Privathaushalten und bei tragbaren Endgeräten bieten vielzählige und teils neuartige Angriffspunkte für Cyberkriminelle. Wie bereits in Bezug auf das Handlungsfeld IoT veranschaulicht wurde, müssen grundlegende Anforderungen der IT-Sicherheit bereits während der Produktentwicklung mitgedacht werden, um die Angriffsfläche für Täter bei Verbraucherprodukten und zugehörigen Schnittstellen möglichst gering zu halten. Eine mögliche Grundlage dafür bietet die ETSI EN 303 645, an deren Entwicklung das BSI maßgeblich beteiligt war. So sollten IT-Geräte mit bestimmten Hardwareeigenschaften aus-

gestattet sein und bereits im Auslieferungszustand eine sichere Softwarelösung beinhalten.

Die Digitalisierung sorgt dafür, dass sich der Alltag von Verbraucherinnen und Verbrauchern an einigen Stellen einfacher und komfortabler gestaltet. Diese Chancen können jedoch nur dann sicher genutzt werden, wenn die Sicherheitsrisiken des digitalen Umfeldes mitbetrachtet und -berücksichtigt werden. Im Rahmen des digitalen Verbraucherschutzes bleibt daher weiterhin das Ziel, durch eine in der Öffentlichkeit breit angelegte Aufklärungsarbeit, durch lebenswelt- und zielgruppenorientierte Kommunikationsangebote sowie durch technische Anforderungen und Standards die notwendigen Rahmenbedingungen zu schaffen, die den Verbraucherinnen und Verbrauchern selbstbestimmtes Handeln ermöglichen. Dafür ist auch in der Zukunft eine gesamtgesellschaftliche Anstrengung für eine ganzheitliche Begegnung der Herausforderungen notwendig.

7 Literaturverzeichnis und weiterführende Links

7 Literaturverzeichnis und weiterführende Links

Bitkom e.V., 2020:
Seit Corona-Ausbruch: Online-Dienste gefragt wie nie.
Einzusehen unter:
https://www.bitkom.org/Presse/Presseinformation/Seit-Corona-Ausbruch-Online-Dienste-gefragt-wie-nie

Bundeskartellamt, 2020:
Sektoruntersuchung Smart-TVs.
Einzusehen unter:
https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2020/01_07_2020_SU_Smart-TVs.html

Bundeskriminalamt, 2020:
Sonderauswertung Cybercrime in Zeiten der Corona-Pandemie.
Einzusehen unter:
www.bka.de/Lagebilder.

Bundesministerium des Innern, für Bau und Heimat (2020):
BMI und BSI: Informationskampagne zur IT-Sicherheit.
Umfrage zum Safer Internet Day:
Bürger wünschen sich Hilfe beim sicheren Umgang mit Computern.
Einzusehen unter:
https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2020/02/safer-internet-day.html

Europäische Institut für Telekommunikationsnormen (ETSI), 2021:
Consumer IoT Security.
Einzusehen unter:
https://www.etsi.org/technologies/consumer-iot-security

Initiative D21, 2021:
Digital-Index Deutschland 2020/ 2021. Jährliches Lagebild der Gesellschaft. Gefördert durch das Bundesministerium für Wirtschaft und Energie.
Einzusehen unter:
www.initiatived21.de/studien-und-publikationen/

Initiative D21, 2020:
Wie digital ist Deutschland? Gefördert durch das Bundesministerium für Wirtschaft und Energie.
Einzusehen unter:
www.initiatived21.de/studien-und-publikationen/

Statistisches Bundesamt, 2021:
Wirtschaftsrechnungen 2020. Private Haushalte in der Informationsgesellschaft – Nutzung von Informations- und Kommunikationstechnologien.
Einzusehen unter:
https://www.destatis.de/DE/Service/Bibliothek/_publikationen-fachserienliste-15.html

StiftungWarentest, 2020:
Fotobücher im Test. Ärgerliche Sicherheitslücken.
Einzusehen unter:
https://www.test.de/Fotobuecher-im-Test-Wer-macht-die-schoensten-Bildbaende-4932482-0/

StiftungWarentest, 2020:
WLAN-Router im Test. Die besten DSL-Router für Ihr Heimnetz.
Einzusehen unter:
https://www.test.de/DSL-WLan-Repeater-Router-im-Test-4733659-0/

Weiterführende Links vom Bundesamt für Sicherheit in der Informationstechnik

BSI Magazin „Mit Sicherheit" (5/2020 & 12/2020).
Einzusehen unter:
https://www.bsi.bund.de/BSI-Magazin

Digitalbarometer 2020:
Bürgerbefragung zur Cybersicherheit (09/2020). Kurzbericht zu den Umfrageergebnissen der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK) und des Bundesamts für Sicherheit in der Informationstechnik (BSI).
Einzusehen unter:
https://www.bsi.bund.de/Digitalbarometer

Die Lage der IT-Sicherheit in Deutschland 2020 (10/2020).
Einzusehen unter:
https://www.bsi.bund.de/Lagebericht

BSI TR-03148:
Sichere Breitband-Router.
Einzusehen unter::
https://www.bsi.bund.de/router-tr

BSI TR-03161:
Sicherheitsanforderungen an digitale Gesundheitsanwendungen.
Einzusehen unter:
https://bsi.bund.de/dok/tr-03161

Pressemitteilungen und Kurzmeldungen unter:
https://www.bsi.bund.de/Presse

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
Mai 2021

Druck
Appel & Klinger Druck und Medien GmbH, Schneckenlohe

Gestaltung
Faktor 3 AG

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

Bildnachweis
Titel: AdobeStock ©neonshot; S. 3, 5: BSI; S. 8: AdobeStock ©jayzynism;
S. 9: AdobeStock ©tetxu; S. 10: AdobeStock ©Monkey Business;
S. 13: AdobeStock ©alphaspirit; S. 14: AdobeStock ©Halfpoint;
S. 19: AdobeStock ©zapp2photo; S. 20: AdobeStock ©Drazen;
S. 21: AdobeStock ©pickup; S. 23: AdobeStock ©Pixel-Shot;
S. 24: AdobeStock ©Antonioguillem; S. 28: AdobeStock ©fizkes

Grafiken
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Artikelnummer
BSI-DVS21/001

www.bsi.bund.de