Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Die Lage der IT-Sicherheit in Deutschland 2021

Vorwort

Der rasante Fortschritt im Bereich der Informationstechnik verändert unsere Gewohnheiten im Beruflichen wie im Privaten in vielfältiger, oft auch sprunghafter Weise. Besprechungen finden zunehmend digital statt, Haushaltsgeräte werden mit dem Internet vernetzt, neue Orte erschließen wir uns nicht mehr mittels Stadtplan, sondern via Internet. Dies erleichtert unseren Alltag, die Vorteile können aber auch Nachteile mit sich bringen. Das verdeutlicht die steigende Anzahl an Cyber-Angriffen.

Die Angriffe auf Microsoft Exchange Server und SolarWinds haben uns eindrücklich vor Augen geführt, welche Reichweite Cyber-Angriffe in einer global vernetzten Welt haben können. Deutschland war von diesen Angriffen zwar in einem geringeren Ausmaß betroffen als einige andere Länder. Dennoch hat sich gezeigt, dass auch unsere Systeme in Deutschland verwundbar sind.

Zudem werden Cyber-Angriffe immer ausgefeilter. Sowohl im Bereich der Cyber-Kriminalität als auch in den Bereichen Cyber-Spionage und -Sabotage entwickeln Angreifer ständig neue Methoden und machen sich dabei auch aktuelle Umstände, wie zum Beispiel die Corona-Pandemie, zu Nutze.

Um unserer Verantwortung als Bundesregierung gerecht zu werden, Sicherheit auch im Cyber-Raum zu gewährleisten, müssen wir uns dieser dynamischen Gefahrenlage fortlaufend anpassen.

In dieser Legislaturperiode haben wir mit dem IT-Sicherheitsgesetz 2.0 den rechtlichen Rahmen für Cyber- und Informationssicherheit in Deutschland auf einen aktuellen Stand gebracht. Mit dem Gesetz wurde nicht nur das Bundesamt für Sicherheit in der Informationstechnik (BSI) als Deutschlands zentrale Cyber-Sicherheitsbehörde gestärkt und mit weiteren Kompetenzen bei der Detektion von Sicherheitslücken und bei der Abwehr von Cyber-Angriffen ausgestattet. Es wurde auch der digitale Verbraucherschutz ausgebaut und für mehr Sicherheit für Unternehmen gesorgt. Damit haben wir unsere Cyber-Sicherheit deutlich erhöht.

Mit der Cybersicherheitsstrategie 2021 haben wir unter Einbeziehung von Akteuren aus der Wirtschaft und Gesellschaft die Strategie aus dem Jahr 2016 neu aufgesetzt und treffen damit Vorsorge für künftige Herausforderungen im Cyber-Raum.

In einer global vernetzten Welt muss Cyber-Sicherheit grenzüberschreitend gedacht werden. Wir arbeiten daher eng mit internationalen Partnern sowie auf europäischer Ebene zusammen.

Der Bericht zur Lage der IT-Sicherheit in Deutschland 2021 zeigt, dass die Gefahren im Cyber-Raum weiter zunehmen und selbst Bereiche betreffen, die für unsere Gesellschaft elementar sind, wie etwa die Stromversorgung oder die medizinische Versorgung. Unsere Behörden stellen sich diesen Gefahren und arbeiten mit vollem Einsatz, um Bürgerinnen und Bürger, Unternehmen und Behörden bestmöglich zu schützen. Insbesondere die unverzichtbare Arbeit des BSI als zentrale Stelle für Informationssicherheit in Deutschland möchte ich in diesem Zusammenhang hervorheben.

Horst Seehofer
Bundesminister des Innern, für Bau und Heimat

Vorwort

Deutschland · Digital · Sicher · BSI

Im April 2021 wurde das IT-Sicherheitsgesetz 2.0 verabschiedet. Dies ist nicht nur ein wichtiger Meilenstein für das BSI. Vielmehr hat der Gesetzgeber damit ein klares und dringendes Upgrade der Cyber- und Informationssicherheit in Deutschland vollzogen und so die Voraussetzungen für eine sichere Digitalisierung geschaffen. Diese kann nur gelingen, wenn Informationssicherheit von Anfang an mitgedacht wird. Informationssicherheit darf nicht länger als Bremsklotz missverstanden werden. Sie ist vielmehr eine Investition in die Zukunft, denn sie macht eine erfolgreiche Digitalisierung erst möglich.

Das ist eine einfache Formel, die nicht immer einfach zu vermitteln ist. Denn erfolgreiche Cyber-Sicherheit ist unsichtbar. Nur wenn sie nicht funktioniert, wird sie sichtbar – als weltweiter Sicherheitsvorfall, als massiver Erpressungsversuch oder als Blockade und Ausfall von Systemen. Das schafft Aufmerksamkeit und macht Schlagzeilen, die eigentlich der Cyber-Sicherheit gehören sollten.

Es ist nicht nur die Anzahl von Sicherheitsvorfällen, die besorgniserregend ist, es ist auch die rasante Entwicklung neuer und angepasster Angriffsmethoden, die massenhafte Ausnutzung schwerwiegender Software-Schwachstellen und die teilweise gravierenden Folgen, die erfolgreiche Cyber-Angriffe auslösen. Zwar ist mit der Zerschlagung des Emotet-Netzwerkes der „König der Schadsoftware“ zunächst von der Bildfläche verschwunden, doch gibt es längst neue Angriffsmittel und Methoden.

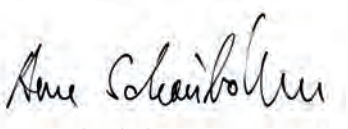
Schwachstellen in IT-Produkten ermöglichen diese neuen Angriffswege überhaupt erst. Dies ist gravierend, wenn Produkte mit großer Verbreitung und hoher Marktdurchdringung betroffen sind. Schwachstellen sind Ausdruck einer mangelhaften Produktqualität. Die Hersteller sollten daher in ihrem eigenen Interesse daran (mit)arbeiten, diese Mängel schnellstmöglich und konsequent zu beheben. Aber es muss auch den Anwenderinnen und Anwendern bewusst sein, dass sie ihre Netzwerke und Systeme jeden Tag aktiv schützen müssen. Wer dies nicht tut, geht enorme Risiken ein:

Produktionsausfälle können für Unternehmen existenzbedrohend sein. Blockierte digitale Bürgerdienste erschweren die Arbeit für Kommunen und Landkreise. Bürgerinnen und Bürger können Verwaltungsdienstleistungen nicht wie gewohnt in Anspruch nehmen. Krankenhäuser müssen sich von der Notfallversorgung abmelden und reihenweise OPs absagen. Dadurch werden Leben gefährdet, zudem leidet die hohe Qualität der medizinischen Versorgung in Deutschland insgesamt. Dies sind keine fiktiven Szenarien, sondern reale Konsequenzen von IT-Sicherheitsvorfällen im Berichtszeitraum. Diese Beispiele machen deutlich, wie sehr wir uns als Gesellschaft auf digitale Prozesse stützen und wie anfällig wir sind, wenn diese Prozesse ausfallen.

Die Corona-Pandemie hat den Alltag vieler Menschen in den vergangenen anderthalb Jahren erheblich verändert. Und sie hat gezeigt, dass wir bei der Digitalisierung in Deutschland Nachholbedarf haben. Als Gesellschaft haben wir Prioritäten neu gesetzt und viele unserer Gewohnheiten angepasst: Wir haben uns an die AHA-Regel gewöhnt, im Homeoffice und beim Homeschooling eingerichtet, Videokonferenzen und virtuelle Familientreffen abgehalten. Viele dieser Neuerungen werden uns auch nach der Pandemie begleiten. Daher ist es angebracht, sich auch mit den zugehörigen Herausforderungen auseinanderzusetzen, insbesondere im Bereich der Informationssicherheit. Der „Bericht zur Lage der IT-Sicherheit in Deutschland 2021“ zeigt auf, wo diese Herausforderungen liegen.

Die Digitalisierung mit all ihren Vorzügen wird weiter voranschreiten. Das ist gut so. Wenn wir dabei aber weiterhin die Informationssicherheit vernachlässigen, werden wir niemals das volle Potenzial der Digitalisierung ausnutzen können. Mehr noch: Im schlimmsten Fall werden viele Digitalisierungsprojekte scheitern.

Den Weg, den Deutschland mit der Verabschiedung des IT-Sicherheitsgesetzes 2.0 eingeschlagen hat, gilt es konsequent weiter zu beschreiten. Für eine sichere Digitalisierung in der Verwaltung, für digitale Innovationen in einer florierenden Wirtschaft, für zuverlässige IT-gestützte Anwendungen zum Nutzen der Bürgerinnen und Bürger. Als Cyber-Sicherheitsbehörde des Bundes sind wir bereit für die nächsten Schritte.



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

Inhaltsverzeichnis

Verzeichnis ausgewählter Vorfälle im Berichtszeitraum:

1 Gefährdungslage

1 Gefährdungen der Cyber-Sicherheit in Deutschland

Das BSI beobachtet als nationale Cyber-Sicherheitsbehörde kontinuierlich die Gefährdungslage der IT-Sicherheit in Deutschland. Im Fokus des BSI stehen Angriffe auf Unternehmen, staatliche sowie öffentliche Institutionen und Privatpersonen, aber auch Prävention und Bekämpfung dieser Lagen. In dem vorliegenden Bericht ziehen wir eine Bilanz für den Zeitraum vom 1. Juni 2020 bis zum 31. Mai 2021 (Berichtszeitraum). Damit greift der Bericht aktuelle und unter Umständen anhaltende Sicherheitslagen und Cyber-Bedrohungen auf. Dazu gehört unter anderem eine Bewertung der IT-Sicherheitslage aufgrund der Auswirkungen der COVID-19-Pandemie.

Anhand zahlreicher konkreter Beispiele aus vielen unterschiedlichen Bereichen zeichnen wir den Weg und die typischen Methoden von Angreifern nach, um zugleich aufzuzeigen, wie sich Menschen und Organisationen schützen können. Wir beginnen unsere Übersicht mit einer Zusammenfassung der allgemeinen Gefährdungslage und aktueller Cyber-Bedrohungen. Angriffe wirken sich nicht nur unmittelbar auf die betroffenen Menschen und Organisationen aus, sondern beeinträchtigen das Leben aller Menschen in einer digitalisierten Gesellschaft. Umso wichtiger ist es, jeden einzelnen Bereich mit seinen spezifischen Bedrohungen und Gegenmaßnahmen zu beleuchten. Ohne das Fazit dieses Berichts vorwegzunehmen: Die Gefährdungslage im Cyber-Raum bleibt auch im Berichtszeitraum angespannt. Cyber-Kriminelle nutzen alle modernen Methoden und Technologien für ihre Attacken auf Privatpersonen, Unternehmen und Institutionen. Um die Vorzüge einer digitalisierten Gesellschaft genießen zu können, müssen wir also weiter wachsam und wehrhaft sein. Sonst gerät das Ziel einer erfolgreichen Digitalisierung in Gefahr.

1.1 Zusammenfassung und Bewertung

Die IT-Sicherheitslage in Deutschland insgesamt war im aktuellen Berichtszeitraum angespannt bis kritisch. Dies war zum einen auf die Ausweitung der bekannten cyberkriminellen Lösegelderpressungen hin zu ergänzenden Schweigegelderpressungen (sogenannte Double Extortion) und Schutzgelderpressungen zurückzuführen. Zum anderen traten im aktuellen Berichtszeitraum jedoch auch Vorfälle auf, die eine Wirkung über die jeweils betroffenen Opfer hinaus entfalteten.

Zudem haben Angreifer die Produktion neuer Schadsoftware-Varianten im Vergleich zum vorigen Berichtszeitraum deutlich beschleunigt. Wurden im vorigen Berichtszeitraum noch durchschnittlich 322.000 neue Varianten pro Tag bekannt, so lag der Tagesindikator im aktuellen Berichtszeitraum bei durchschnittlich 394.000 Varianten pro Tag. Das entsprach einem Zuwachs von gut 22 Prozent. Insgesamt haben Angreifer im aktuellen Berichtszeitraum damit rund 144 Millionen neue Schadprogramm-Varianten produziert (vgl. Kapitel *Neue Schadprogramm-Varianten*, Seite 11).

Lösegeld, Schutzgeld, Schweigegeld: Cyber-Erpresser waren erfindungsreich

Der aktuelle Berichtszeitraum war geprägt von einer spürbaren Ausweitung cyber-krimineller Erpressungsmethoden.

Schutzgelderpressung: Bereits im Herbst 2020 war eine weltweite Kampagne von Cyber-Erpressern zu beobachten, die unter Androhung von Distributed-Denial-of-Service-Angriffen (*DDoS-Angriffen*) Schutzgelder von zahlungskräftigen Opfern erpressten (vgl. Vorfall *DDoS-Schutzgelderpressung,* Seite 34).

Lösegelderpressung: Zugleich waren im Herbst und Winter weitere Angriffswellen mit der Schadsoftware Emotet zu beobachten. Mit der im Anschluss an eine Emotet-Infektion bei ausgewählten Opfern nachgeladenen *Ransomware* versuchten Angreifer bis zum Takedown des *Botnetzes* im Januar 2021, im großen Stil Lösegeld von zahlungskräftigen Opfern zu erpressen (vgl. Vorfall *Emotet-Takedown*, Seite 21).

Schweigegelderpressung: Darüber hinaus erweiterten einzelne Angreifergruppierungen ihre Angriffsstrategie dahingehend, dass vor der Verschlüsselung von Daten diese zunächst unrechtmäßig abgespeichert wurden. Opfern, die über funktionierende *Backups* verfügten und sich insoweit nicht auf Lösegeldverhandlungen einlassen mussten, wurde zusätzlich mit der Veröffentlichung der erbeuteten Daten gedroht und ein Schweigegeld erpresst (vgl. Kapitel *Big Game Hunting mit Ransomware*, Seite 12). Dies bedeutet, dass im Fall eines *Ransomware*-Angriffs nunmehr grundsätzlich auch davon ausgegangen werden muss, dass die Daten dauerhaft kompromittiert sind; und zwar auch dann, wenn ein Lösegeld oder Schweigegeld gezahlt worden ist (vgl. Kapitel *Schadprogramme und Daten-Leaks*, Seite 25).

Zugleich traten im Berichtszeitraum auch weiterhin *Spam*-Kampagnen auf, die dem Bereich der Schweigegeld-

erpressung zuzuordnen waren. Sie richteten sich direkt gegen Endanwender und basierten nicht auf echten Datenabflüssen. Stattdessen gaben die Angreifer betrügerisch vor, über Daten der Opfer zu verfügen, und drohten die Veröffentlichung dieser vermeintlichen Daten an (vgl. Kapitel *Spam und Malware-Spam*, Seite 19).

Kritische Schwachstellen in Microsoft Exchange

Eine Schwachstelle im Exchange-Server sorgte Anfang März 2021 für Aufsehen: Microsoft schloss mit einem Sicherheitsupdate vier kritische Sicherheitslücken, die in Kombination bereits für gezielte Angriffe ausgenutzt worden waren. Unmittelbar nach Bekanntwerden der Schwachstellen konnten bereits großflächige Scans im Internet beobachtet werden, mit denen Angreifer nach verwundbaren Exchange-Servern suchten. Aufgrund der hohen Verbreitung angreifbarer Server einerseits sowie der leichten Ausnutzbarkeit mittels *Exploit-Kits* andererseits stufte das BSI die Lage als extrem kritisch ein. Dies ist die zweithöchste der möglichen Krisenstufen. Von den geprüften Systemen erwiesen sich zunächst 98 Prozent als verwundbar. Nach umfangreichen Warnungen durch das BSI und durch Microsoft sowie durch zügige Reaktion der Systembetreiber konnte dieser Anteil innerhalb einer Woche halbiert und nach weiteren zwei Wochen auf unter zehm Prozent gesenkt werden (vgl. Vorfall *Kritische Schwachstellen in MS Exchange*, Seite 27).

Spektakulärer Supply-Chain-Angriff

Als ein nur schwer zu kontrollierender Angriffsweg hat sich im Berichtszeitraum erneut die Kompromittierung von Software-Supply-Chains herausgestellt. Dabei greifen die Angreifer zunächst Software-Hersteller an und fügen dort Schadcode in legitime Software-Produkte ein. Eine besonders aufwändige Kampagne nutzte dafür die Software Orion von SolarWinds (vgl. Vorfall *SolarWinds,* Seite 30).

Cyber-Sicherheit unter Pandemiebedingungen

Weitreichende *Phishing*-Kampagnen unter Vorspiegelung falscher Tatsachen waren – wie schon im vergangenen Berichtszeitraum – unter inhaltlicher Bezugnahme auf die COVID-19-Pandemie zu beobachten (vgl. Kapitel *Phishing und weitere Betrugsformen*, Seite 24).

Außerdem setzte sich die Verlagerung von Geschäftsprozessen in den digitalen Raum im Berichtszeitraum fort (vgl. Kapitel *Gefährdungen der Cyber-Sicherheit durch die COVID-19-Pandemie*, Seite 38). Die Angriffsfläche vergrößerte sich dabei insbesondere durch die verstärkte Nutzung von Remote-Zugängen und *VPN*, durch Videokonferenzsysteme und Trends wie die dienstliche Nutzung privater Geräte (Bring Your Own Device, BYOD) oder ohne Kontrolle und Sicherheitsservice der IT-Abteilungen beschaffte Schatten-IT-Geräte. Beides stellt schon immer eine schwer zu kontrollierende Angriffsfläche dar. Unter Pandemiebedingungen dürfte die Nutzung solcher Geräte noch deutlich ausgeweitet worden sein.

Videokonferenzen waren im Berichtszeitraum immer wieder Angriffen ausgesetzt (vgl. Kapitel *Cyber-Angriffe auf Videokonferenzen*, Seite 25). So wurden beispielsweise Lauschangriffe beobachtet, bei denen sich Angreifer mittels zuvor erlangter Zugangsdaten unerkannt in Videokonferenzen einwählten und interne Informationen abgreifen konnten.

Angriff auf Institutionen des Gesundheitswesens

Bei einem Aufsehen erregenden Angriff auf die Europäische Arzneimittelagentur EMA erbeuteten Angreifer Daten über den Impfstoff der Hersteller BioNTech und Pfizer. Die Angreifer hatten sich gezielt über ein kompromittiertes Nutzerkonto eines EMA-Dienstleisters Zugang verschafft und anschließend Teile der erbeuteten Daten online veröffentlicht. Dabei waren die veröffentlichten Informationen so manipuliert, dass davon ausgegangen werden muss, dass deren Veröffentlichung Zweifel an dem Impfstoff auslösen sollte.

1.2 Schadprogramme

Zu Schadprogrammen zählen alle Computerprogramme, die schädliche Operationen ausführen können oder andere Programme dazu befähigen, dies zu tun. Schadprogramme gelangen u. a. im Anhang oder über Links in E-Mails auf einen Computer. Wenn die Nutzerin oder der Nutzer auf einen *maliziösen* Anhang oder auf einen Link klickt, der auf eine *maliziöse* Webseite führt, wird ein Schadprogramm installiert. Darüber hinaus zählen unbemerkte Downloads im Hintergrund (sogenannte *Drive-by-Downloads*) sowie *maliziöse* Erweiterungen von legitimen Programmen zu den typischen *Angriffsvektoren*. Für die Infektion angegriffener IT-Systeme nutzen Schadprogramme in der Regel Schwachstellen. Diese treten zum einen in Software- oder Hardware-Produkten auf, zum anderen aber auch an Netzwerkübergängen. Darüber hinaus wird, wie im Fall von *Social Engineering*, der Faktor „Mensch“ für Cyber-Angriffe immer bedeutsamer.

Die einzelnen Schadprogramme unterscheiden sich im Hinblick auf ihre Funktionalität, wobei ein Schadprogramm auch mehrere Funktionalitäten aufweisen kann. Als *Ransomware* bezeichnet man hierbei Schadprogramme, die etwa durch Verschlüsselung den Zugang zu Daten oder Systemen einschränken, damit der Angreifer anschließend ein Lösegeld erpressen kann (vgl. Kapitel *Big Game Hunting*

mit Ransomware, Seite 12). Schadprogramme, die sich als gutartige Software tarnen oder in legitimen Dateien verstecken, werden als Trojaner bezeichnet (vgl. zum Beispiel Vorfall *Ransomware-Angriff auf ein Universitätsklinikum in Nordrhein-Westfalen*, Seite 15, sowie Vorfall *Emotet-Takedown*, Seite 21) und solche, die zum Beispiel mit Hilfe von *Command-and-Control-Servern* fernsteuerbar sind, als *Bot* (vgl. Kapitel *Botnetze*, Seite 19).

Schutz gegen Angriffe mit Schadprogrammen bietet neben regelmäßigen Sicherheitsupdates unter anderem Antiviren-Software, die diese detektieren, an einer erfolgreichen Ausführung hindern und vom System wieder entfernen kann. Manche Angriffe nehmen aber auch tiefgreifende Veränderungen am infizierten System vor, die nicht einfach rückgängig gemacht werden können.

Durchschnittlicher täglicher Zuwachs neuer *Malware*-Varianten
Anzahl in Tausend

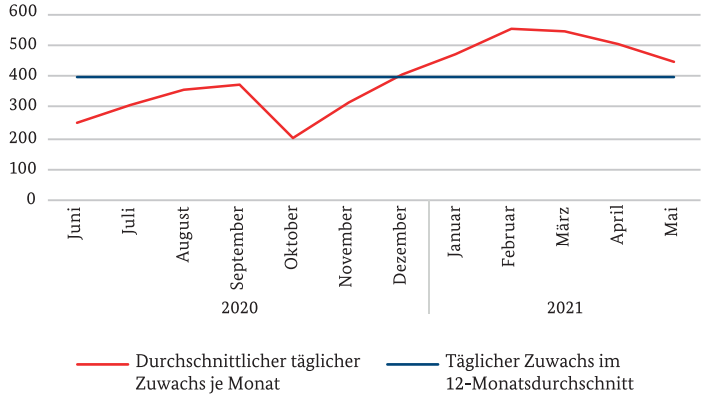


Abbildung 1: Täglicher Zuwachs neuer Schadprogramm-Varianten
Quelle: BSI-Auswertung von Rohdaten des Instituts AV Test GmbH

1.2.1 Neue Schadprogramm-Varianten

Eine neue Variante eines Schadprogramms entsteht, wenn im Programmcode Änderungen vorgenommen werden. Als neue Variante gilt daher jede Variante, die im Hinblick auf ihren *Hashwert* einzigartig ist. Während für bekannte Schadprogramm-Varianten Detektionsmethoden existieren, sind neue Varianten unmittelbar nach ihrem Auftreten unter Umständen noch nicht als Schadprogramme erkennbar und daher besonders bedrohlich.

Die Anzahl neuer Schadprogramm-Varianten hat im aktuellen Berichtszeitraum um rund 144 Millionen zugenommen (vgl. *Abbildung 1*; Quelle dieser und der folgenden Daten: BSI-Auswertung von Rohdaten des Instituts AV-Test GmbH).

Durchschnittlich nahm die Zahl neuer Schadprogramm-Varianten täglich um etwas mehr als 394.000 zu. Das entspricht einer Steigerung von 22 Prozent gegenüber dem vergangenen Berichtszeitraum (vgl. *Abbildung 2*). Allerdings waren erhebliche Schwankungen zu verzeichnen. So lag der Indikator im Juni 2020 bei 250.000 neuen Varianten, also 37 Prozent unter dem Durchschnittswert des Berichtszeitraums.

Um den Jahreswechsel haben Angreifer die Produktion neuer Schadprogramm-Varianten dann deutlich beschleunigt, sodass im Februar 2021 mit durchschnittlich 553.000 neuen Varianten pro Tag der höchste jemals gemessene

Neue Schadprogramm-Varianten
Anzahl in Millionen

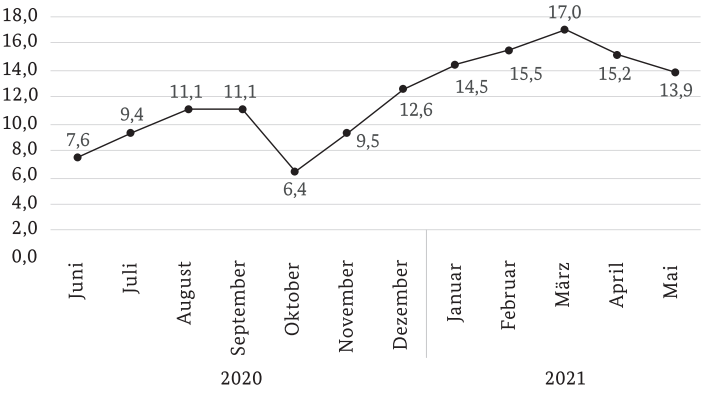


Abbildung 2: Neue Schadprogramm-Varianten
Quelle: BSI-Auswertung von Rohdaten des Instituts AV Test GmbH

durchschnittliche Tageszuwachs zu verzeichnen war (40 Prozent über dem Durchschnittswert des Berichtszeitraums).

Das Wachstum des Tagesindikators war insbesondere auf eine deutlich gestiegene Produktivität der Angreifer in der Kategorie der Windows-Schadprogramme zurückzuführen. In den Wintermonaten wurden regelmäßig neue Spitzenwerte in dieser Kategorie gemessen. Mit EvilQuest trat im September 2020 zudem auch erstmals eine Schadsoftware in nennenswerter Häufigkeit auf, die sich gegen Apples Betriebssystem MacOS richtet. Angreifer hatten die neuen Varianten der Schadsoftware massenhaft in illegalen Software-Kopien versteckt. Der Tagesindikator in der Kategorie der MacOS-Schadsoftware stieg daher binnen Monatsfrist auf sein 500-faches sprunghaft an, kehrte anschließend aber wieder auf sein übliches Niveau zurück. Da der Angriffsvektor im Wesentlichen über Produktpiraterie erfolgte, waren Geräte mit ausschließlich legaler Software von EvilQuest nicht betroffen.

1.2.2 Big Game Hunting mit *Ransomware*

Ransomware bezeichnet Schadsoftware, die klassischerweise den Zugriff auf lokale oder im Netzwerk erreichbare Daten und Systeme verhindert. Am häufigsten wird hierzu eine Verschlüsselung von Nutzerdaten (wie Office-, Bild-, Ton- und Videodateien) oder ganzer Dateninfrastrukturen wie Datenbanken durchgeführt. Das Opfer erhält anschließend eine Nachricht, dass der Zugriff nach Zahlung eines Lösegelds (engl. Ransom) wiederhergestellt wird. Dabei werden häufig sehr kurze Fristen gesetzt und mit der sukzessiven Löschung gedroht. Im aktuellen Berichtszeitraum setzten Angreifer *Ransomware* zudem zunehmend auch für neue Formen der Cyber-Erpressung ein (vgl. Kapitel *Diebstahl und Missbrauch von Identitätsdaten*, Seite 24). Dabei werden die Daten des Opfers nicht nur verschlüsselt, um ein Lösegeld zu erpressen, sondern zuvor ausgeleitet. Die Angreifer drohen dann nicht mit der Vernichtung, sondern mit der Veröffentlichung der Daten. Die Lösegeldzahlungen werden üblicherweise in digitalen (virtuellen) Währungen (zum Beispiel Bitcoin oder Monero) abgewickelt, um die Strafverfolgung zu erschweren. Neben der echten Gelderpressung können *Ransomware-Angriffe* aber auch zur Verschleierung bzw. Ablenkung von anderen Angriffen oder zur reinen Sabotage eingesetzt werden.

Cyber-Kriminelle verwenden in der Regel Angriffsstrategien, die leicht skalierbar sind und sich massenhaft gegen verschiedene Opfer anwenden lassen. Mit der im vergangenen Berichtszeitraum von Juni 2019 bis Mai 2020 beobachteten dreistufigen Angriffsstrategie, die sich aus dem ehemaligen Banking-Trojaner Emotet, der Schadsoftware Trickbot und der *Ransomware* Ryuk zusammensetzte, war es Angreifern beispielsweise gelungen, Angriffsstrategien massenhaft einzusetzen, die zuvor nur von strategisch ausgerichteten APT-Spionage-Angriffen bekannt gewesen waren (vgl. *Quellenverzeichnis*[1]). Dabei verbreitete sich im ersten Schritt der Trojaner Emotet über Outlook-Harvesting, indem er den E-Mail-Verkehr des Opfers analysierte und anschließend für besonders authentisch wirkende Social-Engineering-Angriffe auf Kontakte des Opfers verwendete. Zudem besaß er Downloader-Funktionalitäten, sodass die Angreifer im zweiten Schritt die Spionage-*Malware* Trickbot auf die infizierten Systeme aufspielen konnten. Trickbot ermöglichte den Angreifern weitreichende Spionageaktivitäten auf den infizierten Systemen. Bei ausgewählten, besonders lohnenswert erscheinenden Opfern wurde anschließend die *Ransomware* Ryuk ausgerollt und Lösegeld erpresst.

Wenn möglich, werden cyber-kriminelle Angreifer anhand der eingesetzten Schadsoftware und Vorgehensweise in Gruppen zusammengefasst und unterschieden. Beispielsweise wird die *Ransomware* Ryuk von einer anderen Angreifergruppe eingesetzt als die *Ransomware* Clop. Im aktuellen Berichtszeitraum beobachtete das BSI bei zahlreichen Angreifergruppierungen, die mit unterschiedlichen *Ransomware*-Varianten in Beziehung stehen, dass sich der Fokus ihrer Aktivitäten auf finanzstarke Opfer ausrichtete. So fokussierten die Angreifer ihre Bemühungen auf Organisationen, bei denen ein möglichst hohes Lösegeld gefordert werden kann. Die Höhe des Lösegelds machten die Angreifer dabei beispielsweise an öffentlich verfügbaren Informationen über ihre Opfer, wie etwa der Unternehmensgröße oder den Quartalszahlen, fest. Dieses Phänomen wird gemeinhin auch als Big Game Hunting bezeichnet, zu Deutsch: Großwildjagd. Das BSI sieht Big Game Hunting als einen Teilbereich der cyber-kriminellen Cyber-Angriffe und versteht darunter Angriffe, die sich mit *Ransomware* und damit in Verbindung stehenden Erpressungsmethoden gegen organisationsweite Netzwerke richten, um möglichst hohe Lösegelder zu erpressen.

Ransomware wird über die üblichen *Angriffsvektoren* als E-Mail-Anhang oder als Link verbreitet, der auf eine *maliziöse* Webseite führt. Einen *Angriffsvektor*, der speziell für Unternehmen und andere Einrichtungen mit größerer IT-Infrastruktur gefährlich ist, stellen Schwachstellen in Fernwartungs- und *VPN*-Zugängen dar. Diese Schwachstellen werden verwendet, um interaktiv beispielsweise auf zu wartende Systeme zuzugreifen. Gerade die Arbeit aus der Ferne ist in der COVID-19-Pandemie ein häufig benutztes und notwendiges Mittel für viele Organisationen geworden (vgl. *Gefährdungen der Cyber-Sicherheit durch die COVID-19-Pandemie*, Seite 38). Die Kompromittierung dieser Zugänge führt oft bereits im ersten Schritt dazu, dass der Angreifer mit weitgehenden Rechten ausgestattet ist. *Ransomware* wird zudem oftmals nicht mehr direkt geladen, sondern

Angreifer nehmen sich besonders bei zahlungskräftigen Organisationen die Zeit, das Netzwerk des Opfers vor der Ausführung der *Ransomware* auszukundschaften.
Weiterführende Informationen finden Sie hier:[a)]

Verbreitung von Schadsoftware und Methoden

Das BSI hat nachgewiesen, dass sich die genutzte Schadsoftware und Methoden im cyber-kriminellen Umfeld über Angreifergruppierungen hinweg ausbreiten. Insbesondere die Vorgehensweisen einer Angreifergruppe, die sich als erfolgreich erwiesen haben, werden zeitnah auch von anderen Gruppen übernommen. Diese Verbreitung von cyber-kriminellem Know-how und Technologien erfasst das BSI als *Proliferation* von Schadsoftware und Methoden.

Im aktuellen Berichtszeitraum beobachtete das BSI eine weitere Übertragung bekannter Erpressungsmethoden in den Cyber-Raum. Neben den bekannten Lösegelderpressungen mittels Verschlüsselungstrojaner traten Schweigegelderpressung unter Androhung der Enthüllung kompromittierender Informationen (sogenannte Double Extortion, vgl. auch Kapitel *Schadprogramme und Daten-Leaks*, Seite 25) sowie Schutzgelderpressungen unter Androhung eines *DDoS* (vgl. Kapitel *Distributed Denial of Service*, Seite 31) auf. Die Angreifer veröffentlichten diese Informationen in der Regel auf extra dafür eingerichteten sogenannten Leak-Seiten. Dies ist ein Beispiel für eine erfolgreiche Methode, die zeitnah von anderen Angreifergruppierungen übernommen wurde. Begünstigt wird diese *Proliferation* durch eine Arbeitsteilung und Auslagerung von Bestandteilen eines Cyber-Angriffs an darauf spezialisierte Angreifergruppen, vergleichbar zum Outsourcing von Dienstleistungen in der Privatwirtschaft. Dieses Phänomen wird als *Cybercrime-as-a-Service* (*CCaaS*; Cyber-Straftat als Dienstleistung) bezeichnet. *Cybercrime-as-a-Service* wurde vom BKA im Bundeslagebild Cybercrime 2020 detailliert dargestellt. (vgl. *Quellenverzeichnis*[2]).

Bedrohlichen Einfallsreichtum zeigten Cyber-Kriminelle im aktuellen Berichtszeitraum insbesondere bei der Schweigegelderpressung in Verhandlungssituationen mit dem Opfer. Allein die Zahl der monatlich aktiven Daten-Leak-Seiten, auf denen gestohlene Daten der Öffentlichkeit und anderen Angreifern für weitere Cyber-Angriffe angeboten werden, hat im Berichtszeitraum um fast 360% zugenommen. Und jede einzelne dieser Daten-Leak-Seiten enthält Millionen gestohlener Datensätze. Verschiedene Methoden haben die Angreifer angewendet:

1. Erregung öffentlicher Aufmerksamkeit: Einige Angreifer gehen aktiv auf Kundinnen und Kunden bzw. Partnerinnen und Partner des Opfers oder auch die Öffentlichkeit zu, um zusätzlichen Druck auf einen Betroffenen auszuüben. Dies betrifft Handlungen der Angreifer, die über die Veröffentlichung von Opferinformationen auf dafür eingerichteten Leak-Seiten hinausgehen. Das bedeutet, dass sich Angreifer beispielsweise per E-Mail an Kundinnen und Kunden oder Mitarbeitende eines Opfers wenden und diese darüber informieren, dass aufgrund eines nicht gezahlten Schweigegelds Daten über sie öffentlich wurden. Zudem wurde der Fall einer psychotherapeutischen Praxis bekannt, bei dem nicht nur die Praxisinhaber, sondern auch deren Patientinnen und Patienten erpresst wurden.

Insbesondere bei einem intransparenten Umgang des Opfers mit möglicherweise von dem Daten-Leak Betroffenen kann dies den Ruf des Opfers langfristig schädigen. Eine proaktive pflichtgemäße Meldung verhindert dies.

2. Versteigerung bzw. Verkauf sensibler Daten: Einige Angreifer versteigern bzw. verkaufen erbeutete Daten alternativ zum Veröffentlichen, sollte der Betroffene zu keiner Schweigegeldzahlung bereit sein (sogenannte Double Extortion). Im Gegensatz zu einer Veröffentlichung auf einer Leak-Seite können die Angreifer so zusätzlichen Profit aus den Daten generieren. Zudem können die Käuferinnen und Käufer der erbeuteten Daten diese ihrerseits erpresserisch gegen das Opfer nutzen. Dies gilt insbesondere, wenn es sich um wertvolle Geschäftsgeheimnisse oder kompromittierende Informationen über Einzelpersonen handelt. Im Fall eines Software-Herstellers erbeuteten Angreifer beispielsweise neuen Programmcode und drohten damit, diesen anschließend an den Höchstbietenden zu versteigern. An wen solche Daten schlussendlich versteigert werden, lässt sich in der Regel nicht mehr feststellen. Darüber hinaus müssen Daten, die einmal abgeflossen sind, auch im Fall einer Schweigegeld- oder Lösegeldzahlung grundsätzlich als kompromittiert betrachtet werden.

3. Androhen einer Meldung bei der zuständigen Datenschutz- oder Regulierungsbehörde: Im Zusammenhang mit einem Cyber-Angriff können vom Opfer Verstöße gegen die Datenschutzgrundverordnung oder andere begangen werden, wenn der Betroffene beispielsweise seiner Meldepflicht nicht nachkommt. Diese Verpflichtungen und die daraus ggf. resultierenden Ordnungsstrafen für den Betroffenen nutzten einige Angreifer als weiteres Druckmittel, indem sie androhten, die Regulierungsbehörde über den Verstoß zu informieren.

Durch die Veröffentlichung von Daten aus dem Netz des Opfers und dem mitunter gezielten Ansprechen der Presse und Öffentlichkeit können derartige Verstöße jedoch auch ohne das Zutun der Angreifer bei den zuständigen

Behörden bekannt werden. Eine proaktive pflichtgemäße Meldung verhindert dies.

4. Einsatz von *DDoS-Angriffen* in der Verhandlungsphase: Einzelne Angreifer setzen während der Verhandlung eines Lösegelds zusätzlich *DDoS-Angriffe* ein, um das Opfer weiter unter Druck zu setzen. Wenn beispielsweise ein Online-Versandhändler aufgrund eines *Ransomware*-Angriffs gezwungen wäre, auf eine weniger gegen *DDoS*-Angriffe widerstandsfähige Web-Präsenz auszuweichen, würde ein solcher *DDoS*-Angriff die Bewältigung des *Ransomware*-Angriffs noch zusätzlich erschweren.

Die Ausweitung der Erpressungsmethoden im Berichtszeitraum zeigt, dass die Verschlüsselung allein offenbar nicht mehr den von den Angreifern gewünschten Handlungsdruck bei Betroffenen erzeugt, da diese sich möglicherweise stärker auf ihre *Backups* verlassen können oder Lösegeldzahlungen gemäß der BSI-Empfehlung nicht leisten. Das BSI erwartet, dass cyber-kriminelle Angreifer ihre Vorgehensweisen weiterhin stetig ausbauen werden.

Folgen eines *Ransomware*-Angriffs

Ransomware-Angriffe werden häufig erst dann detektiert, wenn bereits Daten verschlüsselt wurden und IT-gestützte Prozesse zum Erliegen kommen. Hieraus erwachsen verschiedene weitreichende Schäden, zum Beispiel finanzieller Art oder sogar für die Gesundheit von Patientinnen und Patienten, wenn beispielsweise deren Behandlung eingeschränkt werden muss. Von der Entdeckung einer Infektion bis zur Bereinigung der Systeme und vollständigen Wiederherstellung der Arbeitsfähigkeit vergehen in der Regel durchschnittlich 23 Tage (vgl. *Quellenverzeichnis*[3]). An diese unmittelbare Wirkung schließen sich in der Regel Folgekosten an, die sich bei der Bewältigung des Angriffs ergeben.

Zusätzliche Kosten entstehen bei der Bereinigung und Wiederherstellung von IT-Systemen. Um das Ausmaß der Schäden zu ermitteln, müssen oft spezialisierte Dienstleister hinzugezogen werden, da nach einer unvollständigen Bereinigung Hintertüren, so genannte *Backdoors*, zurückbleiben können. Diese *Backdoors* können Angreifer zu einem späteren Zeitpunkt wiederverwenden, um erneut Daten zu verschlüsseln und den Betroffenen zu erpressen. Wie in diesem Fall vorgegangen werden kann, beschreibt das BSI auf seiner Webseite:[b)]

Durch die inzwischen fast zur Normalität gewordene Ausleitung von Daten durch Angreifer vor einer Verschlüsselung muss bei einem *Ransomware*-Angriff mittlerweile grundsätzlich davon ausgegangen werden, dass diese Daten dauerhaft kompromittiert sind. Dieser Umstand verstärkt das Risiko weiterer Erpressungsversuche sowie eines Reputationsverlustes infolge eines *Ransomware*-Angriffs. Die Ausdehnung der Erpressungsmethoden bis hin zur Kontaktaufnahme der Angreifer mit Partnerinnen und Partnern und der Öffentlichkeit verschärft diese Wirkung weiter.

Zusammengenommen können die Schäden eines *Ransomware*-Angriffs für eine betroffene Organisation existenzbedrohend sein.

Empfehlungen

Die wichtigste Maßnahme zur Absicherung gegen *Ransomware*-Angriffe besteht in funktionierenden *Backups*. Die Rekonstruierbarkeit dieser *Backups* muss regelmäßig geprüft werden. Sie dürfen nicht aus dem Netzwerk heraus änderbar sein oder gelöscht werden können. Es sollten also Offline-*Backups* sein.

Um der häufiger werdenden Ausleitung von Daten und der Drohung einer Veröffentlichung (sogenannte Double Extortion) begegnen zu können, ist auch ein systematisches, regelgeleitetes Monitoring des Datentransfers erforderlich. So kann etwa der Abfluss ungewöhnlich hoher Datenmengen erkannt und frühzeitig unterbunden werden.

Zur Minimierung der Angriffsfläche ist außerdem die Zahl und Variabilität der von außen zugänglichen Systeme gering zu halten, Updates der Betriebssysteme und der Server- und Anwendungssoftware sind regelmäßig und zeitnah durchzuführen. Eine sachgerechte interne Segmentierung der Netze hilft, das Ausmaß der Schäden bei erfolgreichen Angriffen zu begrenzen.

Für Unternehmen und andere Institutionen sollten die umfassende und kontinuierliche Schulung aller Mitarbeiterinnen und Mitarbeiter zum Thema Informationssicherheit (Erhöhung der Aufmerksamkeit) und eine restriktive Auswahl der Personen mit administrativem Zugang zu den Systemen selbstverständlich sein. Bei den notwendigen Zugangsberechtigungen sind hohe Anforderungen an die *Authentisierung* und die verwendeten Protokolle zu stellen.

Den Auswirkungen eines frühzeitigen Ausfalls von IT-gestützten Prozessen kann zudem mit der Etablierung von alternativen oder auch redundanten digitalen Diensten begegnet werden. So können etwa Content Delivery Networks (CDN) die Aufrechterhaltung einer Web-Präsenz und darüber angebotene Services unterstützen. Der längerfristige Ausfall eines E-Mail-Servers kann beispielsweise über den Rückgriff auf von einem Dienstleister bereitgestellte E-Mail-Services kompensiert werden. Diese und ähnliche Maßnahmen sollen ermöglichen, einen IT-gestützten

geschäftskritischen Prozess so schnell wie möglich wiederherzustellen, um den aus einem Ausfall gegebenenfalls resultierenden Schaden so gering wie möglich zu halten. Entscheidend ist hierbei, Maßnahmen für den Fall zu berücksichtigen, dass ein IT-gestützter Prozess beispielsweise durch *Ransomware* längerfristig nicht regulär wiederhergestellt werden kann.

Um im Fall eines Angriffs vorbereitet zu sein, müssen Reaktionsszenarien schriftlich festgehalten werden, die alle beschriebenen Aspekte eines Angriffs, zum Beispiel Schäden an Produktionsanlagen, den Einsatz von Personal und Sicherheitsfirmen, alternative Geschäftsprozesse oder den Reputationsverlust, als Teil des Notfallmanagements mit einbeziehen. Weiterführende Informationen finden Sie hier:[c)]

Ransomware-Angriff auf ein Universitätsklinikum in Nordrhein-Westfalen

Am 10. September 2020 kam es an einem Universitätsklinikum in Nordrhein-Westfalen zu einem *Ransomware*-Angriff mit weitreichenden Folgen. Das Krankenhaus ist eine von sechs Universitätskliniken in NRW, die im bevölkerungsreichsten Bundesland die Grundpfeiler der Patientenversorgung darstellen sowie Forschung und Lehre vorantreiben. Das Klinikum weist eine Kapazität von mehr als 1.200 Betten auf, die sich auf 32 Kliniken verteilen, und behandelt jährlich etwa 50.000 stationäre Patientinnen und Patienten. Damit liegt das Universitätsklinikum in der medizinischen Versorgung oberhalb des Schwellenwertes von 30.000 stationären Fällen jährlich und ist somit als KRITIS-Betreiber gemäß BSI-Gesetz (BSIG) in Verbindung mit der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV) beim BSI registriert.

Sachverhalt
Gegen Mittag des 10. September 2020 wurde dem BSI bekannt, dass das Universitätsklinikum einem Angriff durch *Ransomware* zum Opfer gefallen war. Bereits am Abend des 9. September 2020 kam es zu ersten Auffälligkeiten auf einem Antivirus-Server im IT-Betrieb. Diese wurden jedoch zunächst als Betriebsanomalien klassifiziert, bis am darauffolgenden Morgen des 10. September 2020 erste verschlüsselte Dateien auf einigen Servern entdeckt wurden. Als Sofortmaßnahme trennte die Klinik die Internetverbindung und fuhr die meisten Windows-Server herunter, um Zugriffe auf das interne Netzwerk zu unterbinden und einer weiteren Verschlüsselung von Dateien entgegenzuwirken.

Als Einfallstor für den Angriff mit den *Ransomware*s DoppelPaymer und Dridex nutzten die Angreifer eine Schwachstelle auf dem Citrix NetScaler-Gateway des Klinikums, bei dem sie eine Kompromittierung durchgeführt hatten, und zwar bereits vor der Installation des zur Verfügung stehenden Sicherheitsupdates. Beim Citrix NetScaler handelt es sich um ein weit verbreitetes Netzwerkprodukt, das unter anderem für Fernzugriffslösungen eingesetzt wird. Die Angreifer hinterließen außerdem ein Erpresserschreiben, das allerdings nicht an das Klinikum direkt gerichtet war, sondern an die Universität. Als die Ermittlungsbehörden die Cyber-Kriminellen darauf aufmerksam machten, dass sie ein Krankenhaus angegriffen hatten, händigten diese einen digitalen Schlüssel zur Wiederherstellung der IT-Systeme und Daten aus. Dies legt die Vermutung nahe, dass die Angreifer nicht primär die ambulante und stationäre Patientenversorgung zum Ziel hatten, sondern vielmehr die Universität.

Bewertung
Infolge des Angriffs konnte die medizinische Versorgung am Universitätsklinikum für bereits stationär behandelte Patientinnen und Patienten sichergestellt werden, jedoch musste sich das Krankenhaus an dreizehn aufeinanderfolgenden Tagen aufgrund des Ausfalls zentraler Systeme von der Notfallversorgung abmelden. Planbare und ambulante Behandlungen wurden abgesagt bzw. verschoben und die Aufnahme neuer Patientinnen und Patienten wurde eingestellt. Die Kommunikation über E-Mail sowie die telefonische Erreichbarkeit des Klinikums waren eingeschränkt. Der Vorfall am Universitätsklinikum verdeutlicht noch einmal die Gefahren eines Cyber-Angriffs für Organisationen im Gesundheitswesen und deren IT-Infrastrukturen.

Reaktion
Das BSI war mit einem mobilen Einsatzteam (MIRT) auf Anforderung des Universitätsklinikums noch am selben Tag vor Ort, um erste Hilfe bei der Bewältigung des Vorfalls zu leisten. Das BSI unterstützte das Klinikum im gesamten Zeitraum sowohl lokal beim Wiederaufbau der IT-Infrastruktur als auch koordinierend aus dem Backoffice.

Passdatenabfluss

Sachverhalt
Die argentinische Einwanderungsbehörde Dirección Nacional de Migraciones wurde Opfer eines *Ransomware*-Angriffs, der einen massiven Abfluss von Daten auch deutscher Bürgerinnen und Bürger zur Folge hatte. Bei den Daten handelte es sich überwiegend um Passdaten von rund 100.000 ein- und ausreisenden Bürgerinnen und Bürgern, davon 12.000 aus Deutschland, einschließlich ranghoher deutscher Diplomaten. Die Angreifer erbeuteten persönliche Daten wie Name, Vorname, Passnummer, Geburtsdaten und Reiseinformationen sowie Informationen über das Reisedokument (zum Beispiel Diplomatenpass). Die erbeuteten Daten könnten für Identitätsdiebstahl genutzt werden.

Am 27. August 2020 informierte die argentinische Einwanderungsbehörde über technische Störungen, ergriff Maßnahmen und fuhr die IT-Systeme herunter. Die Hacker-Gruppe NetWalker übermittelte ein Erpresserschreiben mit der Aussage, dass die Daten auf den infizierten IT-Systemen im Netzwerk verschlüsselt worden seien, und forderten für die Wiederfreigabe der Daten ein Lösegeld in Höhe von ca. vier Millionen US-Dollar. Als die argentinische Einwanderungsbehörde dieser Forderung nicht nachkam, wurden die Daten etwa zwei Wochen später auf eine Webseite hochgeladen und der Link mit dem Passwort zu dieser Webseite in einem Blog im Darknet veröffentlicht.

Über Twitter teilte die argentinische Sicherheitsbehörde mit, dass es sich bei den erbeuteten Daten um ca. ein Prozent der jährlich anfallenden Daten zu Reisebewegungen handelt und die Datenbank der Einwanderungsbehörde nicht kompromittiert worden ist. Laut Medienberichten wurden zwei Gigabyte an Daten gestohlen, die in einem Ordner mit dem Namen Coronavirus gespeichert waren. In diesem Ordner befand sich eine Tabelle mit persönlichen Daten von rund 100.000 Reisenden aus verschiedenen Ländern wie Argentinien, Deutschland, Frankreich, Israel, der Schweiz und Kanada. Die Daten wurden auf Echtheit überprüft und bestätigt (vgl. *Quellenverzeichnis*[4], vgl. *Quellenverzeichnis*[5]).

Bewertung
Die *Ransomware* NetWalker, ursprünglich bekannt als Mailto, ist seit August 2019 im Umlauf. Seitdem wurden immer neuere Funktionalitäten in Zusammenhang mit dieser *Ransomware* entdeckt. NetWalker hat sich zuletzt zu einem *Ransomware*-as-a-Service-Modell entwickelt und ist in dieser Form seit März 2020 aktiv (vgl. *Quellenverzeichnis*[6]). *Ransomware*-as-a-Service-Angebote sind mittlerweile weit verbreitet. Aus Untergrundforen des Darknet leicht zu erzeugen, muss die Nutzerin oder der Nutzer der Dienste nicht mehr alle Details des *Angriffsvektors* selbst verstehen, sondern kann nach dem Baukastenprinzip individuelle *Ransomware*-Variationen für gezielte Angriffe bzw. Kampagnen erzeugen. Dabei etablieren sich arbeitsteilige Geschäftsmodelle (z. B. 40 Prozent des Lösegeldes für die Anbieterin oder den Anbieter und 60 Prozent für die Nutzerin oder den Nutzer) (vgl. *Quellenverzeichnis*[7]).

Laut der Telemetry Map von McAfee ist bei der globalen Verbreitung dieser *Ransomware* ein Anstieg zu verzeichnen (vgl. *Quellenverzeichnis*[8]). Fast zeitgleich erpresste die Hacker-Gruppe NetWalker Pakistans größtes privates Energieunternehmen K-Electric um 3,8 Millionen US-Dollar Lösegeld auf die gleiche Art und Weise wie die argentinische Einwanderungsbehörde. Als K-Electric dieser Forderung nicht nachkam, wurden auch deren Daten im Internet veröffentlicht (vgl. *Quellenverzeichnis*[9]). Weitere bekannte Fälle der Tätergruppe NetWalker sind der Angriff auf eine österreichische Stadtverwaltung am 24. Mai 2020 und der Angriff auf einen Gesundheitsdienstleister in Philadelphia am 20. Juni 2020 (vgl. *Quellenverzeichnis*[10], vgl. *Quellenverzeichnis*[11]).

Reaktion
Vorsorglich wurden im Fall der argentinischen Einwanderungsbehörde während des Angriffs die Systeme heruntergefahren, um das Ausmaß des Schadens zu begrenzen und den Angriff abzuschwächen. So konnten die Angreifer an weniger Daten gelangen als möglicherweise geplant. Zusätzlich wurde eine Strafanzeige gestellt und Ermittlungen durch die Strafverfolgung unter aktiver Beteiligung des BSI eingeleitet. Außerdem gab die argentinische IT-Sicherheitsbehörde an, den Schutz der Systeme zur Vermeidung künftiger Angriffe zu verstärken (vgl. *Quellenverzeichnis*[12], vgl. *Quellenverzeichnis*[13]).

Das BSI rät grundsätzlich davon ab, einer Lösegeldforderung nachzukommen, weil unklar ist, ob nach Zahlung des geforderten Lösegelds die Daten wieder entschlüsselt werden können. Außerdem verhindert die Zahlung auch nicht zuverlässig die Veröffentlichung der durch die Angreifer entwendeten oder technisch gesprochen kopierten Daten. Wichtige Hinweise, Empfehlungen und Dokumente zum Thema *Ransomware* stehen auf der BSI-Webseite zur Verfügung:[d)]

Darkside

Sachverhalt
Der US Pipeline-Betreiber Colonial Pipeline Company stellte am 7. Mai 2021 einen Cyber-Angriff auf seine IT-Infrastruktur fest. Am 8. Mai 2021 bestätigte der Betroffene gegenüber dem Federal Bureau of Investigation (FBI), dem United States Department of Energy (DOE/US-Energieministerium) und dem Weißen Haus, dass es sich bei dem Cyber-Angriff um einen *Ransomware*-Angriff handelte. Von dem Angriff war das Verwaltungsnetz betroffen (vgl. *Quellenverzeichnis*[14]).

Colonial Pipeline betreibt nach öffentlicher Darstellung das größte Pipeline-System für raffinierte Produkte in den USA. Das Pipeline-Netz hat eine Länge von ca. 8.800 Kilometern und ein Transportvolumen von bis zu ca. 2,5 Millionen Barrel täglich. Colonial Pipeline nimmt eine Schlüsselposition bei der Versorgung von Kunden entlang der Ostküste der USA mit raffinierten Produkten ein (vgl. *Quellenverzeichnis*[15]). Das FBI stellte fest, dass bei dem Angriff die *Ransomware* Darkside (a.k.a. DarkSide) von Cyber-Kriminellen eingesetzt wurde (vgl. *Quellenverzeichnis*[16]).

Bewertung
Darkside wird von Cyber-Kriminellen als *Ransomware*-as-a-Service angeboten. Zum Zeitpunkt des Cyber-Angriffs zählte Darkside zu einer der prominentesten und fortschrittlichsten *Ransomware*-Varianten. Cyber-Angriffe mit Darkside fallen in den Bereich des Big Game Hunting. In der Regel wird zusätzlich zur Lösegelderpressung mit Schweigegelderpressung gearbeitet, indem die Angreifer mit der Veröffentlichung der verschlüsselten und gestohlenen Daten drohen (sog. Double Extortion).

In Deutschland gehört die Mineralölwirtschaft zu den Kritischen Infrastrukturen. Betreibern Kritischer Infrastrukturen obliegen besondere Pflichten in Bezug auf ihre Cyber-Sicherheit sowie Meldepflichten gegenüber dem BSI bei Cyber-Sicherheitsvorfällen. Ein vergleichbarer Cyber-Angriff in Deutschland wird als möglich erachtet.

Betreiber von Energieversorgungsnetzen und Energieversorgungsanlagen in Deutschland müssen einen angemessenen Schutz der für die Erbringung der kritischen Dienstleistungen erforderlichen Telekommunikations- und elektronischen Datenverarbeitungssysteme gewährleisten (§ 11 a und b EnWG). Im Rahmen der Meldung von IT-Vorfällen (§ 8b BSIG) wurden vereinzelt IT-Angriffe auf Energieversorgungsunternehmen gemeldet, die jedoch bis dato lediglich deren Office-Systeme betrafen. Die kritischen Dienstleistungen konnten jeweils aufrechterhalten werden.

Reaktion
In der Folge des Angriffs schaltete der Pipeline-Betreiber sein Verwaltungsnetz ab und setzte vorsichtshalber den Betrieb der Pipeline aus. Diese Aussetzung sorgte für regionale Engpässe und Hamsterkäufe beispielsweise von Benzin. Auf der dedizierten Leak-Seite, die die Cyber-Kriminellen primär zur Veröffentlichung von gestohlenen Daten verwenden, gaben die Betreiber des *Ransomware*-as-a-Service-Angebots *(RaaS)* Darkside bekannt, dass der Angriff von einem Affiliate ausging und das Ausmaß des entstandenen Schadens nicht beabsichtigt gewesen war (vgl. *Quellenverzeichnis*[17]).

Seit dem 15. Mai 2021 berichteten mehrere Medien, dass die Cybercrime-Gruppe, die hinter der *RaaS* Darkside steht, offenbar die Kontrolle über weite Teile ihrer IT-Infrastruktur verloren habe. Die Medienberichterstattung bezog sich dabei auf eine Mitteilung der ehemaligen Darkside-Anbieter an ihre *Affiliates*. Der Entzug der Kontrolle über die IT-Infrastruktur soll auf Veranlassung einer Strafverfolgungsbehörde durch den *Provider* der Infrastruktur erfolgt sein. In der Mitteilung wurde abschließend bekannt gegeben, dass die *Ransomware*-as-a-Service Darkside eingestellt wird (vgl. *Quellenverzeichnis*[18]).

Über den Vorfall bei Colonial Pipeline und Darkside hinaus zeigten sich Auswirkungen auf *Ransomware*-as-a-Service im Allgemeinen. *RaaS*-Angebote wurden zuvor oftmals auf cyber-kriminellen Untergrundforen beworben und zur Schau gestellt. Eine Vielzahl etablierter Untergrundforen verbannte jedoch wenige Tage nach dem Vorfall sämtliche *Ransomware*-Themen von ihren Plattformen. In der Folge wurden vormals öffentlich beworbene *RaaS* in den privaten Raum gedrängt. Die Suche nach neuen *Affiliates* erfolgt seither bspw. über geschlossene Chat-Gruppen und „Mund-zu-Mund-Propaganda“ (vgl. *Quellenverzeichnis*[19]).

Einige *RaaS* wie REvil (a.k.a. Sodinokibi) oder Avaddon erlegten ihren *Affiliates* neue Bedingungen auf, die erfüllt sein müssen, bevor eine Organisation angegriffen werden darf. Hierzu zählen neben Ausschlusskriterien wie Organisationen aus dem Gesundheitssektor auch das Einholen einer Erlaubnis bei den Betreibern der *RaaS* (vgl. *Quellenverzeichnis*[19]). Es kann derzeit nicht abgeschätzt werden, inwieweit die angekündigten Restriktionen für *Affiliates* in einer tatsächlichen Abnahme oder Zunahme von Angriffen gegen einzelne Sektoren resultieren werden, da es jenseits der öffentlichen *RaaS*-Angebote etablierte Cybercrime-Gruppen gibt, die bislang keine derartigen Restriktionen verlautbart haben und wahrscheinlich auch nicht verlautbaren werden. Von *Ransomware* geht unverändert ein herausragendes Bedrohungspotenzial aus.

Ransomware-Angriff auf eine große Mediengruppe

Sachverhalt
In der Nacht zum 22. Dezember 2020 wurde eine große deutsche Mediengruppe Opfer eines *Ransomware*-Angriffs. Dieser Angriff beeinträchtigte die betrieblichen Abläufe massiv, wodurch zahlreiche Print- und Onlinemedien nicht wie gewohnt bereitgestellt werden konnten. Der Angriff ging von der *Ransomware* DoppelPaymer aus. Da der Angriff den Redaktions- und den Druckprozess störte, konnte nach dem Cyber-Angriff lediglich eine Notausgabe der jeweiligen Zeitungen veröffentlicht werden.

Bewertung
Die auch unter dem Namen Doppel Spider bekannten Angreifer hinter der *Ransomware* DoppelPaymer werden dem Big Game Hunting zugerechnet. Sie setzen bei ihren Angriffen zumeist eine Kombination aus Verschlüsselung und Veröffentlichung von im Vorfeld gestohlener Daten ein, um ihre Opfer zu erpressen (sog. Double Extortion). Dieselbe Angreifergruppe ist wahrscheinlich auch für den Angriff gegen ein nordrhein-westfälisches Universitätsklinikum verantwortlich (vgl. Vorfall *Ransomware-Angriff auf ein Universitätsklinikum in Nordrhein-Westfalen*, S. 15).

Reaktion
Das Medienhaus bemühte sich um eine zügige Wiederherstellung seiner Systeme. Die zuständige Polizei sowie das zuständige Landeskriminalamt übernahmen Ermittlungen in diesem Vorfall. Die zuständige Zentrale Ansprechstelle Cybercrime (ZAC) übernahm das Verfahren. Ende Januar 2021 wurden die Zeitungen wieder im gewohnten Umfang ausgeliefert.

Das BSI rät grundsätzlich davon ab, einer Lösegeldforderung nachzukommen, da einmal exfiltrierte und verschlüsselte Daten auch nach der Zahlung eines Lösegelds oder Schweigegelds grundsätzlich als kompromittiert betrachtet werden müssen.

1.2.3 *Spam* und *Malware-Spam*

Allgemein werden unerwünscht zugesandte E-Mails als *Spam* bezeichnet. Neben unerwünschten Werbe-E-Mails kann es sich dabei auch um Cyber-Angriffe wie *Malware-Spam* oder *Phishing*-E-Mails handeln. Der *Spam*-Versand erfolgt zum Beispiel über kompromittierte oder kommerziell angemietete Server, über von Angreifern gestohlene legitime E-Mail-Accounts, deren Zugangsdaten zuvor ausgespäht wurden (vgl. Kapitel *Schadprogramme und Daten-Leaks*, Seite 25), oder über infizierte Systeme, die zu *Botnetzen* zusammengeschlossen und dann für *Spam*-Dienstleistungen zur Verfügung gestellt werden (vgl. Kapitel *Botnetze*, Seite 19).

Im Berichtszeitraum waren insbesondere *Spam*-Wellen aus dem Bereich der Cyber-Erpressung zu verzeichnen. In den Mails einer ausgeprägten Sextortion-Kampagne im Oktober 2020 gaben die Angreifer beispielsweise vor, über intime Geheimnisse der oder des Adressierten sowie über deren oder dessen sämtliche Kontakte zu verfügen. Weiter behaupteten sie, Zugriff auf das Endgerät des Opfers und etwaige Peripheriegeräte wie zum Beispiel eine Webcam zu besitzen. Sie drohten mit umfänglicher Veröffentlichung der angeblichen intimen Geheimnisse und versuchten, ein Schweigegeld in Höhe von 1.000 US-Dollar in Bitcoin zu erpressen.

Spürbare Reichweite erzielten Angreifer mit Sextortion-Kampagnen im Januar, März und Mai 2021. Dabei gaben die Angreifer vor, über Videomaterial des Opfers zu verfügen, das dieses angeblich beim Besuch einer Webseite mit pornografischen Inhalten zeige. Dann forderten sie das Opfer auf, einen vierstelligen Euro-Betrag in Bitcoin zu zahlen. Andernfalls werde das kompromittierende Video an alle Kontakte des Opfers verschickt. Die *Spam*-Ratio, die die Anzahl an *Spam*-Mails je legitime, erwünschte E-Mail in der Wirtschaft in Deutschland misst, erreichte während dieser *Spam*-Wellen im Januar 2021 immer wieder hohe Werte und nahm im Mai 2021 Spitzenwerte von bis zu 34 *Spam*-Mails je legitime, erwünschte E-Mail an. Der Mittelwert im Mai 2021 lag demgegenüber bei 2,3 (vgl. *Abbildung 3*). Statistisch gesehen wurden die E-Mail-Postfächer der Wirtschaft in Deutschland während der genannten Kampagne also für jede legitime, erwünschte E-Mail zusätzlich mit 34 Cyber-Erpresser-Mails aus dem Sextortion-Bereich adressiert. Rund 80 Prozent davon waren allein auf die genannte Schweigegeld-Erpressungskampagne zurückzuführen.

Im Durchschnitt des Berichtszeitraums lag die *Spam*-Ratio bei 1,7 *Spam*-Mails je legitime, erwünschte E-Mail. Die Bedrohung durch *Spam*-Mails war damit im Vergleich zu den Vorjahren durchschnittlich ausgeprägt. Moderne Spamfilter waren der Bedrohung gewachsen und konnten die meisten *Spam*-Mails abwehren, bevor sie die adressierten Postfächer erreichten.

Spam-Ratio in der Wirtschaft in Deutschland
Anzahl *Spam*-Mails je legitime, erwünschte E-Mail

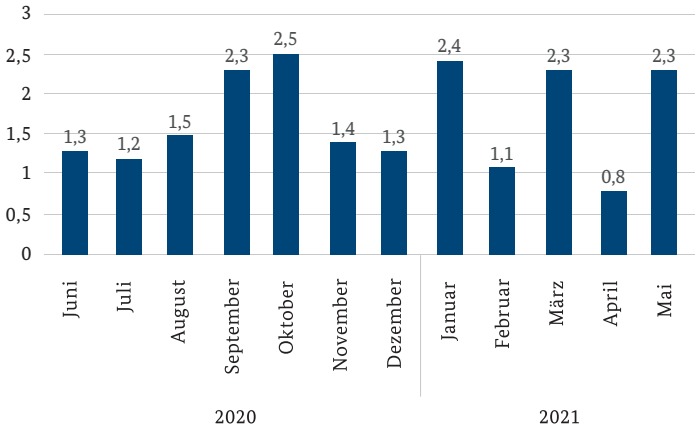


Abbildung 3: *Spam*-Ratio in der Wirtschaft in Deutschland
Quelle: BSI-Auswertung eigener Quellen

1.2.4 *Botnetze*

Unter einem *Bot* versteht man ein Schadprogramm, das einem Angreifer den Fernzugriff auf ein infiziertes System ermöglicht. Durch die großflächige Nutzung von *Bot*-Software haben Cyber-Kriminelle Zugriff auf eine große Anzahl fremder Systeme (Computer, Smartphones, Router, *IoT*-Geräte etc.) und können diese für eigene Zwecke missbrauchen. Den Zusammenschluss mehrerer *Bots*, die von einer zentralen Stelle gesteuert werden, bezeichnet man als *Botnetz*. Der modulare Aufbau aktueller *Bot*-Software ermöglicht dem Angreifer, die Funktionalität eines *Bots* flexibel für die jeweiligen Einsatzzwecke und Angriffsziele anzupassen. Neben dem Verursachen von Schäden auf dem infizierten System selbst (Abgreifen persönlicher Informationen, Onlinebanking-Betrug, Cryptomining, Datenverschlüsselung, etc.), können die übernommenen Systeme auch für den

Angriff auf Dritte genutzt werden (beispielsweise für *DDoS-Angriffe* (vgl. Kapitel *Distributed Denial of Service*, Seite 31) oder den *Spam*-Versand (vgl. Kapitel *Spam und Malware-Spam*, Seite 19).

Im aktuellen Berichtszeitraum wurden *Bots* überwiegend zum Ausspionieren persönlicher Informationen sowie zur Verbreitung weiterer Schadprogramme genutzt. Im Bereich der *Ransomware* ließ sich hier eine Fokussierung der Täter auf finanzstarke Ziele feststellen (vgl. Kapitel *Big Game Hunting mit Ransomware*, Seite 12). So wurden beispielsweise Emotet und Trickbot massiv eingesetzt, um bekannte Unternehmen sowie Institutionen auszuspionieren und deren Daten anschließend mit Ryuk zu verschlüsseln.

Wie in den Vorjahren nahm die Anzahl bekannter *DDoS-Botnetze* weiter ab, auch wenn weiterhin neue Varianten der Schadsoftware Mirai mit zusätzlichen Infektionsmechanismen für diverse Hardware-Plattformen erschienen. Grundsätzlich lässt sich im *Botnetz*-Bereich eine zunehmende Professionalisierung feststellen, was zur anhaltend hohen Gefährdung beiträgt. So wird der überwiegende Teil aktuell aktiver *Bot*-Software von professionellen Dienstleistern auf einschlägigen Plattformen als *Malware*-as-a-Service (*MaaS*) angeboten. Dadurch können auch technisch nicht versierte Cyber-Kriminelle die Funktionalitäten eines *Botnetzes* nutzen, ohne sich um die technischen Belange kümmern zu müssen.

Der Trend zur stärkeren Ausrichtung der Angreifer auf mobile Endgeräte ist auch im aktuellen Berichtszeitraum ungebrochen. Sieben der zehn größten im BSI-Sinkholing beobachteten *Botnetze* zielen auf Tablets und Smartphones, die mit Android laufen. Die Bedrohung hat zudem eine neue Qualität erreicht. So haben Angreifer seit Januar 2021 versucht, Nutzerinnen und Nutzer von Android-Smartphones im Rahmen umfangreicher SMS-*Spam*-Kampagnen zur Installation der MoqHao-Schadsoftware zu bewegen. Diese gliedert das betroffene Smartphone nach erfolgter Installation in ein *Botnetz* ein, um es für weitere Aktionen wie beispielsweise Informationsdiebstahl oder die Weiterverbreitung der Schadsoftware zu missbrauchen. Andere *Botnetze* wie beispielsweise ArrkiiSDK oder AndroidBauts verfolgen das Nutzerverhalten oder installieren ohne Wissen und Erlaubnis der Nutzerin oder des Nutzers zusätzliche Anwendungen. Zudem bringen sie Click-Fraud-Funktionalitäten mit. Die Angreifer können damit Klicks auf Werbebanner simulieren und so Provisionszahlungen pro Klick betrügerisch abrechnen.

Das BSI meldet regelmäßig Informationen über *Botnetz*-Infektionen an die deutschen *Provider*, die ihrerseits die betroffenen Kundinnen und Kunden ermitteln und benachrichtigen. Im Berichtszeitraum wurden täglich bis zu 40.000 infizierte Geräte in Deutschland erkannt und an die *Provider* gemeldet. Die Gesamtzahl der *Botnetz*-Infektionen ist dabei um einiges höher einzuschätzen.

Diese Daten stammen überwiegend aus *Sinkhole*-Datenbeständen, die von externen Quellen zugeliefert oder über BSI-eigene *Sinkhole*-Systeme erhoben werden. *Sinkhole*-Systeme nehmen anstelle der von den Angreifern gesteuerten *Command-and-Control-Server* die Kontaktanfragen von *Bots* entgegen und protokollieren diese ohne weitere Aktionen auszuführen.
Eine Beschreibung des Sinkholing-Verfahrens ist auf der Webseite des BSI zu finden:[e)]

Dort werden auch Steckbriefe von den am häufigsten gemeldeten Schadprogrammfamilien angeboten.

Wie auch in den Vorjahren ist die Bedrohungslage durch *Botnetze* anhaltend hoch. Die aus dem Sinkholing ermittelten Infektionszahlen stellen stets eine Untergrenze dar, da eine vollständige Erfassung aller *Botnetz*-Infektionen nicht möglich ist. Die Zahlen der sichtbaren Infektionen schwanken abhängig von der Auswahl der beobachteten *Botnetze* sowie der zugehörigen Domänen der Steuerungsserver (*C&C-Server*) quellenabhängig sehr stark. Die bisherigen Erfahrungen aus *Botnetz*-Abschaltungen zeigen, dass die Dunkelziffer deutlich höher liegt und die Anzahl infizierter Systeme in Deutschland sich mindestens in einem siebenstelligen Bereich bewegt. Die mit dem IT-Sicherheitsgesetz 2.0 eingeführte Befugnis, *maliziösen* Netzwerkverkehr seitens der Internetprovider umleiten zu lassen, bietet fortan die Möglichkeit, die Sichtbarkeit des bislang DNS-basierten Sinkholings deutlich auszubauen.

So wurden bereits im Jahr 2020 Schritte unternommen, um das Dunkelfeld weiter aufzuklären. Der Unique-IP-Index, der das Aufkommen und die Entwicklung der Infektionszahlen in den beobachteten *Botnetzen* anhand einzigartiger IP-Adressen misst, startete im Juni 2020 bei 884 Punkten. Gegenüber früheren Berichtszeiträumen (2019 lag er bei 100) hat sich das Hellfeld der beobachteten *Botnetz*-Aktivitäten nahezu verzehnfacht.

Da das BSI die Internetprovider und Netzbetreiber der betroffenen Systeme mittels regelmäßiger Reports warnt (vgl. Kapitel *Computer Emergency Response Team für Bundesbehörden*, Seite 71), konnten die Infektionszahlen bereits im ersten Jahr nach der Dunkelfeldaufklärung deutlich gesenkt werden (-31 % gegenüber Juni 2020). Im Durchschnitt des Berichtszeitraums lag der Unique-IP-Index bei 609 Punkten (vgl. *Abbildung* 4).

Unique-IP-Index[1)]
2019 = 100

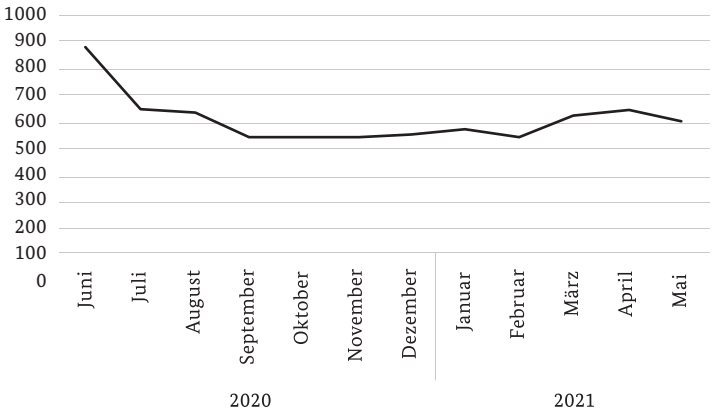


Abbildung 4: Unique-IP-Index
Quelle: BSI-Auswertung eigener Quellen

Aufgrund der stetig größer werdenden Angriffsfläche potentieller Opfersysteme, zum Beispiel durch unzureichend gesicherte *IoT*-Geräte und mobile Systeme, sowie einer zunehmenden Professionalisierung der Täter, ist künftig mit einer kontinuierlichen Zunahme von Infektionen zu rechnen.

Emotet-Takedown

Sachverhalt
Das BSI berichtete bereits im Lagebericht 2020 ausführlich über Emotet und warnte in den letzten Jahren mit mehreren Pressemitteilungen und Cyber-Sicherheitswarnungen immer wieder vor den von dieser Schadsoftware ausgehenden Gefahren. Bereits im Jahr 2019 wurden durch das BSI detaillierte Handlungsempfehlungen zum Schutz gegen Angriffe durch Emotet bereitgestellt (vgl. *Quellenverzeichnis*[20]). Dennoch kam es auch im vergangenen Jahr bei zehntausenden Privatnutzerinnen und -nutzern sowie in einer Vielzahl von Unternehmen, Behörden und anderen Organisationen zu neuen Infektionen mit Emotet.

Durch von Emotet nachgeladene Schadsoftware wie Trickbot wurden teilweise die Netzwerke der Betroffenen vollständig kompromittiert und mussten neu aufgebaut werden, was zu wochenlangen Einschränkungen der Arbeitsfähigkeit und Schäden in Millionenhöhe führte. Die in einigen Fällen von den Angreifern in den Netzwerken Betroffener zusätzlich ausgerollte *Ransomware* Ryuk zur Verschlüsselung von Daten mit anschließender Erpressung der Opfer verursachte weitere hohe Schäden.

Bewertung
Auf infizierten Systemen spähte Emotet die Zugangsdaten zu E-Mail-Konten sowie die Inhalte der Postfächer aus, um diese Informationen zur weiteren Verbreitung der Schadsoftware mit ausgefeilten Social-Engineering-Methoden zu missbrauchen. Allein im Jahr 2020 wurden dem BSI aus der Beobachtung von *Spam-Bots* mehr als 40.000 in Deutschland betriebene E-Mail-Konten bekannt, die durch Emotet kompromittiert worden waren. Diese wurden vom BSI an die zuständigen Betreiber gemeldet, damit Betroffene informiert und ein weiterer Missbrauch der E-Mail-Konten zur Verbreitung von Emotet unterbunden werden konnte. Dies stellt jedoch nur die Spitze des Eisbergs dar - die Gesamtzahl der von Emotet kompromittierten E-Mail-Konten in Deutschland liegt vermutlich deutlich höher.

Reaktion
Am 26. Januar 2021 gelang der Generalstaatsanwaltschaft Frankfurt am Main - Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) - und dem Bundeskriminalamt (BKA) gemeinsam mit Strafverfolgungsbehörden in anderen Ländern im Rahmen einer international koordinierten Maßnahme, die Infrastruktur der Schadsoftware Emotet erfolgreich zu übernehmen und zu zerschlagen (vgl. *Quellenverzeichnis*[21]).

[1)] Ohne infizierte IP-Adressen, die nicht im Sinkholing erfasst wurden.

Im Rahmen dieses Takedowns gelang es den Strafverfolgungsbehörden durch die Auslieferung eines angepassten Binary, die Schadsoftware Emotet auf einer Vielzahl betroffener Opfersysteme unbrauchbar zu machen. Die Kommunikationsparameter von Emotet wurden so angepasst, dass die infizierten Systeme fortan nicht mehr Kontakt zu den Kontrollservern der Täter aufnahmen, sondern sie sich stattdessen bei mehreren vom BKA betriebenen sogenannten „*Sinkhole*-Servern" meldeten. Diese *Sinkholes* protokollierten zur Beweissicherung die Kontaktaufnahmen infizierter Systeme mit Zeitstempel, IP-Adresse und dem von Emotet übermittelten Windows-Computernamen.

Die Protokolldaten wurden vom BKA täglich an das BSI übermittelt. Das *CERT-Bund* des BSI leitete die Informationen an die für die IP-Adressen jeweils zuständigen Netzbetreiber bzw. *Provider* in Deutschland weiter, um Betroffene über die Infektion ihrer Systeme mit Emotet benachrichtigen zu können. Daten zu IP-Adressen ausländischer Netzbetreiber wurden an das jeweils zuständige nationale *CERT* weitergeleitet.

Auch wenn die Schadsoftware Emotet auf infizierten Systemen durch den Takedown keinen weiteren Schaden verursachen kann, bleibt die bereits zuvor nachgeladene Schadsoftware wie Trick oder Qakbot weiterhin aktiv. Ein schnelles Handeln der Betroffenen war daher erforderlich, um infizierte Systeme nach einer Benachrichtigung zu bereinigen und weitere Schäden zu verhindern.

Das angepasste Binary deinstallierte sich am 25. April 2021 selbstständig. Bis dahin konnten drei Monate lang Betroffene weltweit benachrichtigt werden.

Auf infizierten Systemen spähte Emotet die von Nutzerinnen und Nutzern bei der Anmeldung zu Onlinediensten im Webbrowser eingegebenen Zugangsdaten aus. Im Rahmen der weiteren Ermittlungen nach dem Takedown wurde von Strafverfolgungsbehörden eine Datenbank mit mehr als 35 Millionen Datensätzen über von Emotet weltweit auf infizierten Nutzersystemen ausgespähte Zugangsdaten sichergestellt. Mehr als 700.000 Datensätze betrafen Benutzerkonten von über 80.000 verschiedenen, in Deutschland betriebenen Onlinediensten - unter anderem Onlinebanking, Onlineshops, Buchungsportale für Hotels und Flüge, Kundenportale von Internet- und Mobilfunkprovidern sowie Portale für Dienstleistungen von Behörden, wie Wirtschaftsförderungsprogramme und BAföG-Anträge. Das *CERT-Bund* des BSI informierte die Betreiber der Onlinedienste bzw. deren *Provider* zu den betroffenen kompromittierten Benutzerkonten.

SMS-*Phishing* („Smishing")

Sachverhalt

Phishing-Angriffe werden nicht nur per E-Mail, sondern ebenfalls über SMS-Nachrichten durchgeführt. Für diese Variante hat sich das Kunstwort „Smishing" gebildet, die Kombination aus SMS und *Phishing*. Dieses Phänomen ist nicht neu, es trat bislang allerdings überwiegend außerhalb Deutschlands auf. Die nachfolgend beschriebenen Angriffsvarianten haben zum einen das Ziel, eine großflächige Verbreitung durch infizierte Android-Smartphones zu erlangen und zum anderen *Phishing*-Angriffe durchzuführen.

Im Februar 2021 waren in Deutschland SMS-*Phishing*-Nachrichten in größerem Ausmaß festzustellen, die auf das Android-Schadprogramm MoqHao zurückzuführen waren. MoqHao verwendete für die Verbreitung deutschsprachige SMS-Nachrichten, die vermeintlich im Kontext einer Paketbenachrichtigung stehen. Neben dem Benachrichtigungstext war ein Link enthalten, wie z. B. „Ihr Paket wurde verschickt. Bitte überprüfen und akzeptieren Sie es. <Link>". Der Link führte auf eine Webseite, die Android-Anwenderinnen und -Anwender dazu verleiteten sollte, etwa ein vermeintliches Update einer Chrome-Browser-*App* zu installieren. Dahinter verbirgt sich die schädliche MoqHao-*App*. Unmittelbar nach der Installation kommt es zu einem massenhaften SMS-Versand über infizierte Android-Smartphones, um MoqHao weiter zu verbreiten. Darüber hinaus kann MoqHao auf infizierten Android-Smartphones *Phishing*-Angriffe, z. B. durch die Einblendung von Formularfeldern, durchführen. Command-and-Control-Server ermittelt MoqHao über kodierte Inhalte auf Social-Media-Profilen.

Seit März 2021 wurden die MoqHao-Nachrichten in Deutschland zunehmend durch SMS-Nachrichten des Android-Schadprogramms „FluBot“ verdrängt. Hierbei kam ebenfalls eine vermeintliche Paketbenachrichtigung als thematischer Aufhänger zum Einsatz. Für die Paketverfolgung sei die Installation der FluBot-*App* erforderlich, die sich in Deutschland als FedEx- oder DHL-*App* tarnte. Mit Installation der Android-*App* kommt es wie bei MoqHao zum massenhaften SMS-Versand. Die SMS-Texte weisen allerdings eine höhere Varianz und seit Anfang April 2021 in manchen Fällen eine persönliche Anrede auf. Diese Informationen rühren daher, dass FluBot nach der *App*-Installation die lokalen Smartphone-Kontakte ausliest und an einen Command-and-Control-Server übermittelt. Diese Informationen werden wiederum für den SMS-Versand über infizierte Android-Smartphones genutzt. Neben der Verbreitung per SMS führt FluBot wie MoqHao auf infizierten Android-Smartphones *Phishing*-Angriffe durch.

FluBot weist eine robustere *Botnetz*-Infrastruktur als MoqHao auf. So kommen in den SMS-Nachrichten häufig wechselnde Link-Adressen zum Einsatz. Die FluBot-*Apps* werden über eine Vielzahl an unterschiedlichen Download-Webseiten angeboten, bei denen es sich um kompromittierte Webseiten handelt. Für die Adressierung von *Command-and-Control-Servern* nutzt FluBot einen Algorithmus für die Erzeugung von potenziellen Domain-Namen (Domain Generation Algorithm, kurz DGA). Durch tausende potenzielle Domains soll die Beeinträchtigung des FluBot-*Botnetzes* durch die Stilllegung einzelner Domains verhindert werden.

An den FluBot-Mechanismen orientiert sich das Android-Schadprogramm „TeaBot“, das ebenfalls die lokalen Smartphone-Kontakte ausliest, sich über SMS-Nachrichten verbreitet und in Form von vermeintlichen Android-*Apps* wie VLC Media Player, TeaTV, DHL oder UPS in Erscheinung tritt. Wie FluBot führt TeaBot auch *Phishing*-Angriffe auf infizierten Android-Smartphones durch und zielt dabei u. a. auf installierte Banking-*Apps* von deutschen Banken ab.

Bewertung
Die genannten Android-Schadprogramme MoqHao, FluBot und TeaBot haben gemein, dass sie aus unbekannten Quellen und nicht aus legitimen *App*-Stores installiert werden müssen. Diese Funktion ist unter Google Android standardmäßig deaktiviert, unter Apple iOS ist dies grundsätzlich nicht möglich. Durch *Social Engineering* wie z. B. der persönlichen Anrede, dem gestiegenen Paketversand während der COVID-19-Pandemie sowie einer Schritt-für-Schritt-Anleitung für die notwendigen Android-Konfigurationsänderungen und der *App*-Installation, ist den SMS-*Phishing*-Akteuren allerdings eine umfangreiche Ausbreitung in Deutschland gelungen.

Mit Installation einer der genannten schädlichen Android-*Apps* gilt das Smartphone als vollständig kompromittiert. Neben dem SMS-Versand können auch SMS-Inhalte und je nach Schadprogrammversion zudem Tastatureingaben und *App*-Inhalte ausgespäht werden. Damit sind neben *App*-Daten auch potenziell Zwei-Faktor-Authentifizierungsmechanismen betroffen.

Anwenderinnen und Anwender von Apple iOS sind grundsätzlich nicht durch die schädlichen Android-*Apps* gefährdet, sie können allerdings über die Links in den SMS-Nachrichten auf *Phishing*-Webseiten umgeleitet werden.

Reaktion
Seit dem verstärkten Aufkommen der SMS-*Phishing*-Wellen im Februar 2021 arbeitet das Cyber-Abwehrzentrum mit den deutschen Mobilfunkprovidern zusammen, um die SMS-*Phishing*-Wellen einzudämmen und öffentlich zu sensibilisieren, z. B. über Pressemitteilungen und Social Media. Ein weiterer Austausch erfolgt in der internationalen IT-Sicherheits-Community, um Verhaltensänderungen in den SMS-*Phishing*-Kampagnen rasch zu erkennen und Gegenmaßnahmen abzuleiten.

Das BSI hat neben Sensibilisierungsmaßnahmen außerdem Maßnahmen zur Erkennung infizierter Android-Smartphones mithilfe des Sinkholings, d. h. der Registrierung von *Command-and-Control-Server*-Domains ergriffen. Mit dem Sinkholing verbinden sich infizierte Smartphones nicht zu einem legitimen, sondern zu einem *Command-and-Control-Server* von IT-Sicherheitsanalysten. Diese Informationen wurden wiederum zur Information deutscher Netzbetreiber über infizierten Android-Smartphones in den jeweiligen Netzen verwendet.

Weiterhin erfolgte eine Zusammenarbeit mit Google, um die Erkennung der o. g. schädlichen *Apps* auf Android-Smartphones z. B. mithilfe von Google Play Protect zu verbessern.

1.3 Diebstahl und Missbrauch von Identitätsdaten

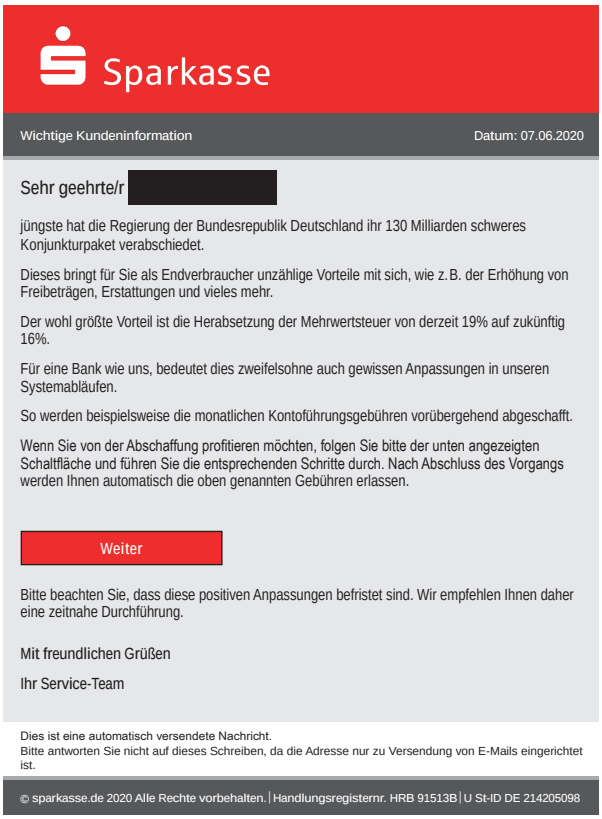
Unter einer Identität wird im Kontext der Informationssicherheit die Menge von Merkmalen verstanden, die die Echtheit einer Person oder Sache nachweist. Die Identität einer Person oder Sache kann sowohl durch ein einziges Merkmal oder aber durch die Kombination diverser Merkmale bestimmt werden. Im Internet wird auf die Identität einer Person meist aus Identifikations- und Authentisierungsdaten geschlossen, wie zum Beispiel aus der Kombination von Benutzername und Passwort. Solche Daten beinhalten Wissen über eine Person, weshalb diese auch als Wissensfaktoren bezeichnet werden. Als Identitätsdiebstahl wird die rechtswidrige Aneignung bzw. Verwendung solcher Daten bezeichnet. Insbesondere bei der elektronischen Kommunikation und der Nutzung von Diensten im Internet hängt das Vertrauen der Internetnutzer in ihr Gegenüber häufig davon ab, ob dieses solche Wissensfaktoren vorweisen kann. Dies macht jede Form vertrauenserweckender Daten zu einem begehrten Ziel für verschiedenste Angreifer.

1.3.1 Phishing und weitere Betrugsformen

Eine prominente Form für Angreifer, an solche Daten zu gelangen, ist das sogenannte *Phishing*. Mithilfe ausgefeilter Techniken des *Social Engineering* versucht ein Angreifer, das Opfer zur Herausgabe sensibler Informationen zu bewegen. Hierbei stehen in Deutschland neben Bankkundinnen und -kunden insbesondere auch Kundinnen und Kunden von Online-Versandhändlern wie Amazon oder Bezahlsystemen wie PayPal im Fokus.

Wie das BSI beobachten konnte, orientieren sich auch aktuelle *Phishing*-Kampagnen an gesellschaftlichen Ereignissen und aktuellen Themen, wie etwa Steuerrückzahlungen oder auch die COVID-19-Pandemie. Die Unsicherheit und Überforderung im Umfeld aktueller Entwicklungen der COVID-19-Pandemie, der reale und empfundene Zeitdruck und die gesellschaftliche und mediale Dominanz des bestimmenden Themas wurden von Angreifern ausgenutzt. Hierbei wurde gezielt mit Emotionen gespielt, und die Angriffe konnten eine breite Masse erreichen.

So machten sich die Angreifer im Rahmen der Pandemie die erschwerte Umsetzung logistischer Prozesse zunutze. Angreifer gaben sich etwa als Zollbeamte aus und verlangten via E-Mail vor der Zustellung einer Ware die Entrichtung einer Gebühr, zu zahlen über einen anonymen Zahlungsdienst wie Paysafecard. Da pandemiebedingt immer mehr Menschen online bestellten, vergrößerte sich auch der Kreis potenzieller Opfer entsprechend. Immer weitere Betrugsszenarien wurden um aktuelle Themen herum aufgebaut: Angreifer nutzten die Gewährung von Soforthilfen mit Hilfe von Fake-Webseiten aus, nahmen die Senkung der Mehrwertsteuer als Vorwand, Änderungen der Kontoführungsgebühren vorzutäuschen, und entwickelten angesichts drohender Ausgangssperren oder vorübergehender Schließung von Bankfilialen immer neue fiktive Online-Systeme. Die Angreifer reagierten stets schnell auf aktuelle oder kurz bevorstehende Entwicklungen in der Pandemie (vgl. *Abbildung 5*).



Sparkasse

Wichtige Kundeninformation — Datum: 07.06.2020

Sehr geehrte/r [redacted]

jüngste hat die Regierung der Bundesrepublik Deutschland ihr 130 Milliarden schweres Konjunkturpaket verabschiedet.

Dieses bringt für Sie als Endverbraucher unzählige Vorteile mit sich, wie z. B. der Erhöhung von Freibeträgen, Erstattungen und vieles mehr.

Der wohl größte Vorteil ist die Herabsetzung der Mehrwertsteuer von derzeit 19% auf zukünftig 16%.

Für eine Bank wie uns, bedeutet dies zweifelsohne auch gewissen Anpassungen in unseren Systemabläufen.

So werden beispielsweise die monatlichen Kontoführungsgebühren vorübergehend abgeschafft.

Wenn Sie von der Abschaffung profitieren möchten, folgen Sie bitte der unten angezeigten Schaltfläche und führen Sie die entsprechenden Schritte durch. Nach Abschluss des Vorgangs werden Ihnen automatisch die oben genannten Gebühren erlassen.

Weiter

Bitte beachten Sie, dass diese positiven Anpassungen befristet sind. Wir empfehlen Ihnen daher eine zeitnahe Durchführung.

Mit freundlichen Grüßen

Ihr Service-Team

Dies ist eine automatisch versendete Nachricht.
Bitte antworten Sie nicht auf dieses Schreiben, da die Adresse nur zu Versendung von E-Mails eingerichtet ist.

Abbildung 5: Beispiel einer Phishing-E-Mail
Quelle: *Phishing-Radar der Verbraucherzentrale NRW* in Kooperation mit dem BSI

Das Wissen der Angreifer über ihre Opfer und/oder das Agieren im Namen eigentlich vertrauenswürdiger Institutionen oder Personen nahm dabei eine besondere Rolle für den Erfolg oder Misserfolg eines Angriffes ein. So wurden dem BSI Vorfälle gemeldet, bei denen sich Angreifer Zugriff auf Online-Bankkonten von Opfern verschaffen konnten und durch gezielte fingierte Anrufe die für eine Transaktion notwendige TAN in Erfahrung bringen konnten. Zudem wurden Fälle bekannt, bei denen Twitter-Accounts bekannter Persönlichkeiten wie Barack Obama, Jeff Bezos und Bill Gates verwendet wurden, um Angebote im Zusammenhang mit der Kryptowährung Bitcoin zu lancieren, verbunden mit dem Versprechen, die eingezahlten Bitcoins in doppelter Höhe zurückzuzahlen.
Weitere Informationen finden Sie hier:[f)]

1.3.2 Schadprogramme und Daten-Leaks

Neben dem Einsatz von *Phishing* stellen aber auch immer wieder spezielle schädliche Skripte oder komplexe Schadprogramme eine weitere Möglichkeit dar, Identitätsdaten zu entwenden. So stehen Online-Händler aufgrund der immensen Anzahl an Kundendaten immer wieder im Fokus gegenwärtiger Angriffsbemühungen durch Skimming. Bei Web-Skimming-Angriffen werden legitime Webseiten von Online-Händler kompromittiert, teils ohne dass die Betreiber der Plattformen dies direkt bemerken. Solche Skimming-Angriffe auf Webshops sind im Berichtszeitraum erneut unter dem Stichwort Magecart bekannt geworden. Hierbei konnten Angreifer durch das Einbinden von maliziösem JavaScript Kreditkartendaten sowie Liefer- und Rechnungsadressen aus dem Bezahlprozess des Webshops erbeuten.

Zusätzlich wurde die allgegenwärtige Bedrohung durch die Verschlüsselung elementarer Daten durch *Ransomware* im Berichtszeitraum zunehmend begleitet durch den Diebstahl und die Veröffentlichung dieser Daten (vgl. Kapitel *Big Game Hunting mit Ransomware*, Seite 12). Waren es anfangs nur ausgewählte Angreifergruppen, die die Erfolgsaussichten der Lösegelderpressung auf diese Weise verbesserten, so haben mittlerweile zahlreiche Angreifergruppen diese Vorgehensweise (Modus Operandi) adaptiert und der Trend konnte sich verstetigen. Dies hat zur Folge, dass bei einem Angriff mit einer *Ransomware* mittlerweile auch immer mit dem Risiko eines Daten-Leaks gerechnet werden muss; beide Themen verschwimmen mehr und mehr. Hinzu kommt, dass Daten, die einmal auf eine dedizierte Leak-Seite (DLS) gestellt wurden, auch nach Zahlung eines Schweigegelds und anschließender Entfernung der Daten als kompromittiert angesehen werden müssen. Die Daten werden wahrscheinlich von den unterschiedlichsten Akteuren gesammelt und können für zukünftige Angriffe weiterverwendet werden.

Die Ursachen für Daten-Leaks sind jedoch in vielen Fällen nicht nur in fortschrittlichen Angriffen zu suchen. Sensible Daten gelangten auch im aktuellen Berichtszeitraum aufgrund mangelnder Schutzmaßnahmen von (Online-) Datenbanken in unbefugte Hände. Dies hat immer wieder zur Folge, dass sensible (oft personenbezogene) Daten ohne Beteiligung oder sogar in vielen Fällen auch ohne Kenntnis der Betroffenen in die Öffentlichkeit geraten.

Allgemein von einem Daten-Leak betroffen waren im Berichtszeitraum unter anderem namhafte Technologieunternehmen, Arztpraxen und Krankenhäuser, Unternehmen aus dem Bereich Transport und Logistik sowie öffentliche Einrichtungen und soziale Netzwerke. Besondere Aufmerksamkeit erweckte ein Vorfall in Finnland. Im Rahmen eines Cyber-Angriffs auf den Betreiber eines finnischen Psychotherapie-Zentrums konnten Unbekannte zehntausende Patientenakten entwenden. Die Angreifer forderten Schweigegeldzahlungen und sagten im Gegenzug die Löschung der Patientenakten zu. Opfer können in solchen Fällen jedoch niemals sicher sein, dass die Daten wirklich gelöscht werden. Diese müssen deshalb grundsätzlich als kompromittiert betrachtet werden. Der Vorfall erweckte aufgrund des schwerwiegenden Eingriffs in die besonders schützenswerte Intimsphäre der Patientinnen und Patienten internationales Aufsehen.

Ein zentrales Thema bei der Betrachtung von Identitätsdiebstählen war die weltweite COVID-19-Pandemie. Die durch die COVID-19-Maßnahmen bedingte Verschiebung analoger Prozesse in den digitalen Raum, aber auch die Bekämpfung der Pandemie bildeten die Ausgangslage für zahlreiche Vorfälle, die im Berichtszeitraum auftraten (vgl. *Gefährdungen der Cyber-Sicherheit durch die COVID-19-Pandemie*, Seite 38). Weltweit kam es vermehrt zu Abflüssen sensibler Informationen, die im Zusammenhang mit der Pandemie und deren Bekämpfung standen und durch mangelhafte Sicherheitsmaßnahmen oder gezielte Angriffe entwendet wurden. Auch in einigen deutschen Testzentren war der Zugriff auf persönliche Daten zeitweise möglich.

In Deutschland konnte mithilfe des BSI die Sicherheit der nationalen Corona-Warn-*App* nachhaltig gestärkt werden. Das BSI begleitet den Entwicklungsprozess durch permanente Schwachstellenanalysen und Penetrationstests. Detektierte Schwachstellen konnten so in Kooperation mit den Herstellern der *App* geschlossen werden, bevor die jeweilige Version produktiv zum Einsatz kam. Dem BSI sind im Berichtszeitraum keine Vorfälle bekannt, bei denen es im Zusammenhang mit der deutschen Corona-Warn-*App* zu einem Abfluss von personenbezogenen Daten gekommen ist (vgl. Kapitel *Corona-Warn-App*, Seite 52).

1.3.3 Cyber-Angriffe auf Videokonferenzen

Insgesamt führte die Corona-Krise zu einer massiven Verlagerung diverser Lebensbereiche in den digitalen Raum. Diese Veränderung bot die Möglichkeit, innovative Konzepte und neue Möglichkeiten zu schaffen, jedoch gingen mit der Auslagerung analoger Prozesse in den digitalen Raum auch neue Risiken einher. Kommunikationsplattformen gewannen im Berichtszeitraum durch die verhängten Kontaktverbote stark an Bedeutung. Weltweit wickelten Unternehmen und staatliche Institutionen ihre interne Kommunikation zu großen Teilen über Videokonferenzplattformen ab. Durch die stark ansteigende Verwendung und der damit einhergehenden öffentlichen Aufmerksamkeit wurden solche Videokonferenzplattformen zu einem attraktiven Ziel für Cyber-Angriffe.

Ein Interesse für Angreifer bestand dabei in der Beschaffung von Informationen aus privaten Konferenzen. Beim sogenannten Credential Stuffing werden bspw. Nutzerdaten aus vorangegangenen Daten-Leaks automatisiert bei verschiedenen Diensteanbietern ausprobiert, um zu testen, ob auch dort eine Anmeldung möglich ist. So konnten sich Dritte mittels zuvor abgeflossener Login-Daten getarnt als legitime Teilnehmer Zugang zu geschlossenen Sitzungen verschaffen. Das Eindringen in interne Sitzungen kann fatale Folgen für die betroffenen Institutionen haben. Die Möglichkeiten, entwendete Informationen zu instrumentalisieren, sind zahlreich. Inhalte von Videokonferenzen geben mitunter tiefgehende Einblicke in interne Prozesse, eingesetzte Tools und nicht zuletzt vertrauliche Informationen einer Institution. Neben Erpressung und Wirtschaftsspionage können so auch weitere Cyber-Angriffe aus Lauschangriffen resultieren.

Im Berichtszeitraum erfolgte eine Vielzahl von Angriffen auf Nutzerinnen und Nutzer, bei denen Login-Daten entwendet wurden. Die Angreifer verwendeten dabei oftmals *Phishing*-Mails, die als Sitzungseinladungen gekennzeichnet waren und die Zielpersonen auf gefälschte Webseiten weiterleiteten. Dort wurden die Nutzerinnen und Nutzer dann zur Passworteingabe aufgefordert. Die entwendeten Informationen standen anschließend teilweise auf illegalen Plattformen im Internet zum Verkauf. Neben Login-Daten wurden darüber hinaus *Zero-Day-Exploits* für bekannte Videokonferenzplattformen angeboten.

Ein weiteres Phänomen, das mit der vermehrten Nutzung von Videokonferenzplattformen in den Vordergrund trat, war das sogenannte Zoom-Bombing. Hierbei verschaffen sich Unbekannte Zutritt zu Konferenzen, um diese gezielt zu stören. Auch der Bereich der Online-Lehre war hiervon betroffen. Die Login-Daten wurden dabei oftmals von Teilnehmern des Unterrichts einfach weitergegeben. Ein entscheidendes Sicherheitsrisiko bei der Nutzung von Videokonferenzplattformen ist das mangelnde Wissen über die Bedienung bestimmter Systemfunktionen. Im Berichtzeitraum kam es wiederholt zu Vorfällen, bei denen Personen des öffentlichen Lebens Bilder ihrer Online-Sitzungen in Sozialen Netzwerken publizierten und dabei die Einwahldaten z. B. in Form der sichtbaren URL mit veröffentlichten. Dies hatte zur Folge, dass unter anderem eine vertrauliche Sitzung der europäischen Verteidigungsminister von Unbekannten gestört werden konnte.

Zusammenfassung

Wie bereits in den vergangenen Jahren, beobachtete das BSI auch im aktuellen Berichtszeitraum regelmäßig Meldungen zum Abfluss personenbezogener Daten. Erschwerend kam im aktuellen Berichtszeitraum hinzu, dass *Ransomware*-Vorfälle und Lösegelderpressungen nunmehr in der Regel vom Abfluss solcher Daten und entsprechender Schweigegelderpressung begleitet wurden. In der Praxis verschwimmen beide Phänomene zunehmend. Angesichts des besonders schwerwiegenden Eingriffs in die schützenswerte Intimsphäre von Patientinnen und Patienten, die beispielsweise ein Abfluss sensibler Gesundheitsdaten darstellt, muss der Schutz dieser Daten eine übergeordnete Priorität einnehmen. Der Verlust von sensiblen Gesundheitsdaten kann möglicherweise lebenslange Folgen für Patientinnen und Patienten nach sich ziehen.

Die COVID-19-Pandemie hat einen maßgeblichen Einfluss auf die Bedrohungslage im Bereich Identitätsdaten. Durch die in der Pandemie notwendig gewordene physische Distanz wurde das Vertrauen in die digitale Identität immer wichtiger. Der Verlust vertraulicher Informationen unterminiert nicht nur den Schutz gegen Cyber-Angriffe auf die Infrastrukturen einer digitalen Gesellschaft, sondern beeinflusst auch das Vertrauen in die Digitalisierung selbst. Für einen bedachten und sicheren Umgang mit persönlichen Daten stehen an erster Stelle die Anbieter von Internetdiensten in der Pflicht, aber auch jede oder jeder Einzelne muss sich der Verantwortung bei der Preisgabe von persönlichen Daten bewusst sein. Weitere Informationen finden Sie hier:[g)]

1.4 Schwachstellen

Im Internet zugängliche Produkte, die einem Angreifer aufgrund von Verwundbarkeiten als Brückenkopf beim Eindringen in ein Netzwerk dienen können, stellen ein großes Risiko dar. Beispielhaft hierfür waren im aktuellen Berichtszeitraum insbesondere die das NetLogon-Protokoll betreffende Active-Directory-Schwachstelle Zerologon (CVE-2020-1472) sowie Schwachstellen, die den Groupware- und E-Mail-Server Exchange betreffen. Eine besondere Kritikalität besteht, sobald für anfällige Systeme funktionierender Angriffscode (sog. *(Zero-Day-) Exploit*) veröffentlicht wurde bzw. bereits in bekannte Angriffswerkzeuge integriert wurde (sog. *Exploit-Kits*). Dies macht eine breitere Ausnutzung wahrscheinlich. Diese Charakteristik hatte im Berichtszeitraum insbesondere die Microsoft Exchange betreffende Schwachstelle Proxylogon (CVE-2021-26855). Möglicherweise auch aufgrund der pandemiebedingten Ausweitung des Homeoffice werden von vielen Unternehmen und Organisationen aus betrieblichen Gründen Exchange-Server mit offen aus dem Internet erreichbarem Outlook Web Access (OWA) betrieben. Infolge des Bekanntwerdens dieser Schwachstellen weisen die für Deutschland validierten Zahlen auf ein Grundproblem beim sicheren Betrieb solcher Brückenkopf-Systeme und dem Einspielen wichtiger Sicherheitsupdates hin (vgl. Vorfall

Kritische Schwachstellen in MS Exchange, siehe unten). Veranschaulicht wird das Risiko zudem durch die nach wie vor vielerorts vorzufindende und häufig für Angriffe verwendete Schwachstelle Bluekeep (CVE-2019-0708) in Microsofts Remote Desktop Protocol (RDP) und den häufig immer noch ungepatchten Schwachstellen verschiedener Sicherheits- und *VPN-Applikationen*.

Von zunehmender Bedeutung ist außerdem, dass Softwareprojekte durch die zunehmende Einbindung von

Kritische Schwachstellen in MS Exchange

Sachverhalt

Im März 2021 veröffentlichte Microsoft ein außerplanmäßiges Sicherheitsupdate für den weit verbreiteten Groupware- und E-Mail-Server Exchange. Das Update schloss vier kritische Schwachstellen, die in Kombination bereits für gezielte Angriffe ausgenutzt worden waren. Eine der Schwachstellen ermöglicht Angreifern, sich durch Senden speziell formulierter HTTP-Anfragen auf dem Exchange-Server zu authentisieren. Anschließend kann unter Ausnutzung der weiteren Schwachstellen beliebiger Programmcode mit weitreichenden Zugriffsrechten ausgeführt werden. Angreifer nutzten dies aus, um auf tausenden Servern Hintertüren in Form sogenannter Webshells einzuschleusen. Wurden diese nach der Installation der Sicherheitsupdates nicht entfernt, hatten die Täter weiterhin Zugriff auf betroffene Systeme und konnten darüber zum Beispiel E-Mails ausspähen oder Schadprogramme, wie *Ransomware*, ausrollen. Zum Zeitpunkt des Bekanntwerdens der Schwachstellen waren 98 Prozent der geprüften Systeme in Deutschland verwundbar. Die Ausnutzung für Cyber-Angriffe konnte zunächst vorwiegend in den USA beobachtet werden.

Bewertung

Bereits direkt nach Veröffentlichung der Sicherheitsupdates durch Microsoft hatten Angreifer das Internet großflächig nach verwundbaren Systemen gescannt. Zeitgleich begannen verschiedene Angreifergruppierungen damit, unter Ausnutzung der Schwachstellen Schadsoftware zu installieren. Alle verwundbaren Exchange-Server waren somit unmittelbar einem extrem hohen Risiko ausgesetzt, mit Schadsoftware infiziert zu werden. Daher mussten auch alle zeitnah gepatchten Systeme auf bereits zuvor evtl. erfolgte Kompromittierungen hin untersucht werden. Die Lage wurde weiter dadurch verschärft, dass viele Systeme auf stark veralteten Versionsständen waren, für die keine Updates zur Verfügung standen, dass Exchange-Server zudem in vielen Netzen standardmäßig sehr hohe Rechte besitzen und dass vorgefertigte *Exploit*-Skripte zur Ausnutzung der Schwachstellen schnell im Internet verfügbar waren.

Bereits im Jahr 2020 hatte sich die Nachlässigkeit vieler Systembetreiber am Beispiel der Anfang 2020 veröffentlichten Sicherheitsupdates für eine andere kritische Sicherheitslücke in Microsoft Exchange gezeigt. Da Exchange-Server in vielen Infrastrukturen mit erhöhten Rechten betrieben werden, sind unter Ausnutzung derartiger Schwachstellen häufig weitergehende Angriffe und mitunter die vollständige Kompromittierung der Windows-Domäne möglich. Trotz des großen Risikos waren im Oktober 2020 (acht Monate nach Veröffentlichung der damaligen Sicherheitsupdates durch den Hersteller) immer noch zwei Drittel der Exchange-Server in Deutschland mit offen aus dem Internet erreichbarem Outlook-Web-Access (OWA) anfällig für Angriffe über diese Schwachstelle. Die kontinuierliche Lagebeobachtung offenbarte, dass die zuständigen Systembetreuerinnen und -betreuer entgegen dieser früheren Erfahrungen im diesjährigen Fall schneller und umfangreicher reagierten. Im Laufe der ersten Woche nach Bekanntwerden der Schwachstelle halbierte sich der Anteil der verwundbaren Systeme.

Reaktion

Aufgrund des hohen Risikos stufte das BSI die Bedrohungslage als extrem kritisch ein und stellte regelmäßig aktualisierte Sicherheitsinformationen auf seiner Webseite bereit. Die Zielgruppen des BSI wurden bei der Vorfallsbewältigung unterstützt und zusätzlich in zwei Webinaren über weitere aktuelle lagerelevante Hinweise informiert. Zudem wurden die üblichen *CERT-Bund*-Reports, mit denen das BSI regelmäßig deutsche Netzbetreiber und *Provider* über verwundbare Systeme in ihren Netzen unterrichtet, erweitert und mit Information über das mit den Schwachstellen verbundene Risiko angereichert. Mit der Bereitstellung zusätzlicher Updates für ältere Versionsstände und der Veröffentlichung von Skripten zur Mitigation und Prüfung auf evtl. bereits erfolgte Kompromittierungen durch Microsoft konnte die Situation zunächst etwas entschärft werden.

Im Mai 2021 waren jedoch noch immer knapp neun Prozent der geprüften Exchange-Server in Deutschland für die kritischen Schwachstellen verwundbar.

Software Bill of Materials (SBOM)

Große Coordinated-Vulnerability-Disclosure-Fälle (CVD-Fälle) wie AMNESIA:33 und Ripple20 haben gezeigt, dass viele Hersteller nur mit sehr viel Mühe feststellen können, welche Bibliotheken und andere Drittherstellersoftware in ihren Produkten eingesetzt werden. Diese aufwendigen Analysen kosten wertvolle Zeit und behindern den CVD-Prozess.

Die internationale Community arbeitet mit starker Unterstützung der US-Behörde National Telecommunications and Information Administration (NTIA) an der Spezifikation der SBOM (Software Bill of Materials). In einer SBOM werden alle Abhängigkeiten einer Software aufgelistet. Dies soll eine effiziente Überprüfung, ob eine bekannte Schwachstelle ein Produkt betrifft, ermöglichen. Als Anwender kommen hier zunächst die Hersteller selbst infrage, die in ihren Lieferketten überprüfen müssen, ob sie eine bestimmte verwundbare Version einer Software einsetzen. Erst mit diesem Wissen lassen sich zu ergreifende Maßnahmen bzgl. der Behebung einleiten. In Kombination mit dem Common Security Advisory Framework (CSAF) kann der Prozess innerhalb der Wertschöpfungsnetzwerke umfassend automatisiert werden.

Diesen verbesserten Schutz der Lieferketten unterstützt das BSI auch im Bereich der Spezifikation des VEX-Formates. Mithilfe dieses Formats können die Hersteller den Anwenderinnen und Anwendern mitteilen, dass sie zwar eine verwundbare Version der Software einsetzen, die Schwachstelle aber nicht ausnutzbar ist. Dies kann beispielsweise der Fall sein, wenn aufgrund von Compileroptionen nur ein bestimmter, nicht verwundbarer Codeanteil in das Produkt eingeflossen ist.

Software-Bibliotheken, die sich nicht unter der Kontrolle des für das Softwareprojekt Verantwortlichen befinden, einem schwer zu kalkulierenden Sicherheitsrisiko unterliegen. Eine solche Lieferketten-Problematik wird beispielsweise durch Schwachstellen in weit verbreiteten Software-Komponenten verursacht. Beispielhaft dafür sind die als AMNESIA:33 (33 Schwachstellen in 4 verschiedenen Open Source Netzwerk-Stacks) und Ripple20 (19 Schwachstellen in einem proprietären Netzwerk-Stack) bezeichneten Schwachstellen. Einmal mehr wurde durch diese Beispiele veranschaulicht, welche weitreichenden Implikationen kritische Schwachstellen in häufig genutzten Software-Produkten haben können (vgl. Infokasten *Software Bill of Materials*).

1.5 Advanced Persistent Threats

Advanced Persistent Threats (APT) unterscheiden sich von anderen Bedrohungen der Cyber-Sicherheit durch die Motivation und die Vorgehensweise der Angreifer. Während zum Beispiel Schadprogramme von kriminellen Angreifern in der Regel massenhaft und ungezielt verteilt werden (vgl. Kapitel *Big Game Hunting mit Ransomware*, Seite 12), sind APTs oft langfristig und mit großem Aufwand geplante Angriffe auf einzeln ausgewählte, herausgehobene Ziele. APT-Angriffe dienen nicht der kriminellen Gewinnerzielung, sondern der Beschaffung von Informationen über das Ziel und ggf. der Sabotage.

Technische Vorgehensweisen: Oftmals werden APTs mit der Ausnutzung komplexer Schwachstellen in Verbindung gebracht. Das ist in der Praxis, insbesondere bei Angriffen auf die Endanwenderin bzw. den Endanwender, allerdings oft nicht der Fall. Die meisten E-Mail-basierten Angriffe nutzen inzwischen keine technischen Schwachstellen mehr. Stattdessen steht (genau wie bei kriminellen Angriffen auch) die Anwenderin bzw. der Anwender im Fokus. Sie bzw. er soll dazu verleitet werden, Warndialogfenster zu ignorieren und Makros und andere schädliche Inhalte auszuführen. In anderen Fällen wird die Anwenderin bzw. der Anwender dazu gebracht, EXE- und Verknüpfungsdateien in ZIP-Archiven anzuklicken, was das sogenannte DLL-Sideloading initiiert. Um die Detektion durch Sicherheitsprodukte zu umgehen, übertrugen einige Gruppen den Schadcode nicht mehr direkt im Mail-Anhang, sondern versteckten ihn in sogenannten Remote Templates, die erst beim Öffnen des Dokuments heruntergeladen werden. Dies war insbesondere bei den Gruppen Lazarus, APT28 und Gamaredon zu beobachten.

Ein klarer Trend ist, dass einzelne Gruppen von mail-basierten Angriffen wieder auf Scans gegen Server (wie Remote-Einwahl- oder E-Mail-Server) wechselten oder diese zumindest in ihr Portfolio aufnahmen. Dies gilt z. B. für die Gruppen BerserkBear, APT41, APT28 und auch KarmaPanda. Dieser Trend begann bereits, bevor weltweit viele Firmen wegen der Pandemie das Homeoffice einführten. Mögliche Gründe dafür, dass nicht nur Anwenderinnen bzw. Anwender und ihre Bürosoftware,

sondern auch Server angegriffen werden, sind vielfältig: Server werden in der Regel nicht automatisiert mit Sicherheitsupdates aktualisiert. Für Sicherheitsteams wird das systematische Planen von Update-Prozessen erschwert, weil verschiedene Hersteller in unterschiedlichen Rhythmen *Patches* zur Verfügung stellen. Außerdem ist es für die Angreifer komfortabel, sich über das Internet direkt mit einem kompromittierten Server zu verbinden, statt darauf zu warten, dass ein infizierter Bürorechner gestartet wird und sich für neue Kommandos bei den Angreifern meldet.

Als ein nur schwer zu kontrollierender Angriffsweg hat sich im Berichtszeitraum erneut die Kompromittierung von Software-Supply-Chains herausgestellt. Dabei greifen die Angreifer zunächst Softwarehersteller an und fügen dort Schadcode in legitime Software-Produkte ein. Eine besonders aufwändige Kampagne nutzte dafür die Software Orion von SolarWinds (vgl. Vorfall *SolarWinds*, Seite 30).

Obwohl viele Gruppen inzwischen auf bekannte, öffentlich verfügbare Werkzeuge wie CobaltStrike, Meterpreter und PowershellEmpire setzen, wird trotzdem nach wie vor auch eigene, gruppenspezifische *Malware* entwickelt. Das gilt sowohl für technisch sehr fortschrittliche als auch für eher unterdurchschnittlich befähigte Gruppen. Zudem haben viele Gruppen aus den unterschiedlichsten Regionen der Welt im aktuellen Berichtszeitraum viel Aufwand betrieben, um ihre *Payloads* vor Analysten zu schützen. Dafür wurden in die Infektionsketten immer wieder neue Zwischenschritte eingebaut, die erst nach und nach weitere Schadcode-Stufen nachladen. Dies ist nicht zu verwechseln mit dem bisher beobachteten Ansatz, verschiedene Schadcode-Module optional nachzuladen. Stattdessen ist es bei diesen Angriffsketten zwingend notwendig, dass alle Schritte sequentiell durchlaufen werden. Weil die Täter in jedem Schritt den nächsten Schadcode von den Angriffsservern entfernen können oder nur weitermachen, wenn von einem früheren Schritt Informationen übermittelt werden, konnten Analysten von Sicherheitsfirmen und Behörden oftmals die eigentlichen Schadprogramme nicht analysieren.

Internationale politische Maßnahmen: Neben technischen Sicherheitsmaßnahmen setzen manche Staaten inzwischen auch auf außenpolitische Maßnahmen, um gegen APT-Aktivitäten vorzugehen. Vor dem Hintergrund der kontinuierlichen APT-Angriffe haben im Berichtszeitraum eine Reihe von Staaten ihre Standpunkte zum Völkerrecht im Cyber-Raum veröffentlicht, darunter Positionen zur Souveränität, dem Recht auf Gegenwehr und zur Frage, wann die Schwelle zum bewaffneten Angriff überschritten ist. Auch Deutschland hat seine Standpunkte zum Völkerrecht im Cyber-Raum veröffentlicht (vgl. *Quellenverzeichnis*[22]).

Vor allem die USA sind behördenübergreifend konzertiert gegen Akteure im Cyber-Raum vorgegangen. Die Regierungsmaßnahmen umfassen: Sanktionen gegen als nicht-vertrauenswürdig eingestufte Lieferanten, wirtschaftliche Sanktionen und Anklagen gegen Personen, die mit APT-Angriffen in Verbindung gebracht wurden, die Schaffung von Rechtsgrundlagen für offensive Cyber-Operationen und schließlich auch die Durchführung von offensiven Cyber-Operationen gegen Angriffsinfrastrukturen.

Fälle in Deutschland: Das BSI hat im Berichtszeitraum eine Reihe von Fällen bearbeitet und APT-Gruppen zugeordnet. Der überwiegende Teil der Gruppen versuchte, Regierungsbehörden anzugreifen. Dies deckt sich mit dem weltweit berichteten Trend, dass Regierungsbehörden das häufigste Ziel von gezielten Angriffen sind. Das BSI betreibt Attribution nur auf Gruppenebene, die identifizierten APT-Gruppen werden von den zuständigen Nachrichtendiensten und Strafverfolgungsbehörden sowie internationalen Sicherheitsfirmen meist übereinstimmend mindestens vier unterschiedlichen Ursprungsländern zugeordnet.

Traditionell ist weltweit auch der Rüstungssektor ein beliebtes Ziel. Im Berichtszeitraum sind dem BSI in diesem Bereich in Deutschland APT-Gruppen aufgefallen, die von Behörden und Sicherheitsfirmen zwei unterschiedlichen Staaten zugeordnet werden. Mindestens vier Gruppen führten gezielte Angriffe gegen weitere Unternehmen durch.

Ein zunehmender Trend ist, dass Thinktanks und Nichtregierungsorganisationen (NGOs) auch in Deutschland angegriffen werden. Betroffen sind meist solche Organisationen, die sich mit außenpolitischen Themen oder Menschenrechten beschäftigen.

Auch in Deutschland lebende ausländische Regierungskritiker waren Ziel von APT-Angriffen.

Ziel: Personenbezogene Daten: Die erwähnten Angriffe auf ausländische Regierungskritiker werden durch Berichte über Angriffe im Ausland bestätigt, bei denen personenbezogene Daten von Individuen gestohlen wurden. Fluglinien, Flughäfen, Telekommunikationsunternehmen, Behörden und Gesundheitsorganisationen wurden angegriffen, um teilweise gezielt, teilweise massenhaft Informationen über Personen zu erlangen. Der Schutz dieser Daten in den unterschiedlichen Sektoren und Organisationen muss inhärenter Bestandteil der Digitalisierung sein.

SolarWinds

Eine der Angriffskampagnen, die im Berichtszeitraum die größte politische und öffentliche Aufmerksamkeit erhalten haben, nutzte die Software Orion des amerikanischen Herstellers SolarWinds, um Unternehmen und Behörden zu kompromittieren. Deutsche Ziele standen dabei weniger im Fokus als Ziele in anderen Ländern, der Sachverhalt ist aber dennoch in zweierlei Hinsicht überaus relevant: Zum einen verdeutlicht er das enorme Potenzial, das sich Angreifern durch sogenannte Supply-Chain-Angriffe eröffnet, bei denen legitime Software-Produkte bereits im Netzwerk des Herstellers mit Schadcode versehen werden. Zum anderen wurde durch die Analyseberichte deutlich, dass die Angreifergruppe ein bis dato selten gesehenes hohes technisches Niveau besaß, mit dem sie ihre Angriffe lange unentdeckt durchführen konnte.

Sachverhalt
Der US-Hersteller SolarWinds entwickelt unter anderem die Software Orion, die ein Monitoring von Netzwerken, Systemen und Anwendungen ermöglicht. US-Regierungsstellen gaben Mitte Dezember 2020 bekannt, dass Unbekannte in Orion Update-Dateien eine *Backdoor* eingefügt hatten. Dieses Update wurde von bis zu 18.000 SolarWinds-Kundinnen und -Kunden heruntergeladen und installiert. Nur bei ausgewählten Unternehmen und Behörden nutzten die Angreifer die Sunburst oder Solorigate genannte *Backdoor*, um weitere Schadprogramme nachzuladen und sich im internen Netzwerk auszubreiten (vgl. *Quellenverzeichnis*[23]). Mehrere US-Behörden wie das Handels- und Finanzministerium sind Medienberichten zufolge kompromittiert worden. Dem Software-Unternehmen Microsoft waren mindestens 40 betroffene Organisationen bekannt, bei denen die Angreifer manuelle Folgeaktivitäten durchführten. Davon waren knapp die Hälfte in der IT-Branche angesiedelt (vgl. *Quellenverzeichnis*[24], vgl. *Quellenverzeichnis*[25]). Die Dunkelziffer der Betroffenen kann höher liegen.

Die Angreifer ließen laut der technischen Berichte der IT-Sicherheitsfirmen FireEye und CrowdStrike besondere Vorsicht walten, um nicht entdeckt zu werden (vgl. *Quellenverzeichnis*[26]). So wurde der Schadcode nicht in den eigentlichen Quellcode des Orion-Produkts eingefügt, wo er durch Code-Prüfungen aufgefallen wäre. Stattdessen wurde der Kompilierungsprozess, bei dem der Quellcode in ausführbaren Code übersetzt wird, manipuliert, sodass der Schadcode nur im Arbeitsspeicher und im Endprodukt vorhanden war. Offenbar hatten die Angreifer viel Aufwand und Zeit investiert, um die Orion-Software zu analysieren und ihre *Backdoor* in legitime Module und Netzwerkprotokolle einzufügen.

Bei den späteren Angriffen auf Unternehmen und Behörden passten die Angreifer ihre Werkzeuge und Kontrollserver für jedes Ziel individuell an. Dies bedeutet einen Aufwand, den andere Angreifer meistens vermeiden.

Die Angriffe scheinen auf langfristige Kompromittierungen ausgelegt gewesen zu sein. Beispielsweise wartet die Schadsoftware nach der Installation zwei Wochen, bevor überhaupt der erste Kontakt zu einem Kontrollserver der Angreifer aufgenommen wird. Die initialen Angriffe sollen bereits im Frühjahr 2020 stattgefunden haben.

In Deutschland ist dem BSI eine zweistellige Zahl von Einrichtungen bekannt, die das *maliziöse* Orion-Update installiert haben. Jedoch haben die Angreifer in diesen Fällen keine zusätzlichen *Backdoors* nachgeladen und sich nicht weiter im internen Netzwerk ausgebreitet.

Bewertung
Der Vorfall hat technische, wirtschaftliche bzw. politische sowie strategische Implikationen.

1. Auf der technischen Ebene zeigt der Vorfall, welches Potenzial Supply-Chain-Angriffe haben. Als *Angriffsvektor* sind manipulierte Software-Installationsdateien oder -Updates geeignet, um verbreitete Detektionsmaßnahmen zu unterlaufen. Wenn die Angreifer in den späteren Phasen des Angriffs, wie im vorliegenden Fall, vor allem legitime Administrationswerkzeuge und gestohlene Zugangsdaten verwenden, kann der Angriff lange unentdeckt bleiben. Je nach Verbreitung der manipulierten Software können die Angreifer Zugriff auf eine hohe Zahl an Netzwerken und Systemen erlangen. Für Kundinnen und Kunden von Software-Produkten sind Supply-Chain-Angriffe nur schwierig zu erkennen. Die wichtigsten Akteure, die das Einbringen von Schadcode in Software-Produkte verhindern können, sind die Hersteller selbst. Entwicklungs- und Auslieferungssysteme bedürfen eines entsprechend hohen Sicherheitsniveaus.

Auch der Aufwand und die Kompetenz der Angreifer, lange unentdeckt zu bleiben, muss als technischer Meilenstein gewertet werden, der Anlass zur Sorge gibt.

2. Die wirtschaftlichen bzw. politischen Konsequenzen für die betroffenen Unternehmen und Behörden sind davon abhängig, welche Informationen die Angreifer stehlen konnten. Hierzu sind - wie bei solchen Vorfällen üblich - kaum öffentliche Informationen vorhanden. Zum einen ist der Nachweis, welche Dokumente abgeflossen sind, oftmals nicht mehr möglich, zum anderen äußern sich die Betroffenen in der Regel nicht öffentlich dazu. An welchen Arten von Informationen die Angreifer Interesse haben, hängt auch von der Frage ab, welche Angreifergruppe für die Angriffe verantwortlich ist und welchen Auftrag sie haben. Amerikanische, britische und kanadische Regierungsstellen machten die Gruppe APT29 für die Angriffe verantwortlich, die bisher vor allem für langfristige Spionage gegen Behörden und Thinktanks bekannt war (vgl. *Quellenverzeichnis*[27], vgl. *Quellenverzeichnis*[28], vgl. *Quellenverzeichnis*[29]). Einig sind sich die bei den Untersuchungen beteiligten Stellen darin, dass es bisher keine Anzeichen für Sabotage gegeben hat, obwohl dies in großem Umfang möglich gewesen wäre.

3. Auf der strategischen Ebene führte der Fall vor allem in den USA zu Diskussionen in Politik, Forschung und Medien über die Fragen, wie es zu einem solch massiven Sicherheitsvorfall kommen konnte, wie darauf reagiert werden soll und ob die USA ihre Cyber-Politik anpassen müssen.

IT-Konzerne wie Microsoft forderten beispielsweise, dass Behörden und Unternehmen mehr Informationen miteinander austauschen müssen (vgl. *Quellenverzeichnis*[30], vgl. *Quellenverzeichnis*[31]). Kritik wurde unter anderem an dem staatlichen Einstein-Projekt geäußert, für das mit hohem Budget eine Art Intrusion Detection System für Behörden und Unternehmen aufgebaut wurde, das den SolarWinds-Angriff aber nicht entdeckt hat. Andererseits wurde darauf hingewiesen, dass solche Systeme ihre Stärke bei der Detektion langanhaltender, bekannter Kampagnen haben, während die Angreifer in diesem Fall viel Aufwand trieben, um eben nicht über wiederverwendete Indikatoren detektiert werden zu können.

Auch grundlegende Fragen wurden aufgeworfen, etwa, ob Abschreckung durch offensive Cyber-Fähigkeiten funktionieren kann und ausgebaut werden sollte (vgl. *Quellenverzeichnis*[32]).

Eine weitere Diskussion entspann sich entlang der Frage, ob dieser massive Supply-Chain-Angriff internationale Cyber-Normen verletzt habe, und wenn nicht, ob zusätzliche Normen entwickelt werden müssten. Erst wenn solche Verhaltensregeln international etabliert sind, können Verletzungen dieser Normen politisch oder juristisch geahndet werden.

Politische Kommentatoren in den USA gehen davon aus, dass diese grundlegenden strategischen Fragen wie Kooperation zwischen Staat und Wirtschaft, Abschreckung, *Defending Forward* und Cyber-Normen die Cyber-Politik der Biden-Präsidentschaft prägen werden.

Reaktion
Das BSI warnte nach Bekanntwerden der Orion-Schwachstelle umgehend vor deren Ausnutzung. Zudem informierte das BSI in Deutschland potenziell betroffene Institutionen und Unternehmen und unterstützte sie bei Bedarf bei der Analyse.

1.6 Distributed Denial of Service (*DDoS*)

Als Denial-of-Service-Angriffe (*DoS*-Angriffe) werden Überlastungsangriffe auf Internetdienste bezeichnet. Es ist somit eine gefährliche Angriffsform, die das Schutzziel Verfügbarkeit betrifft. Sie sind seit langem bekannt und können jeden treffen - aber es gibt Schutz. *DoS*-Angriffe richten sich gegen die Verfügbarkeit von Diensten, Webseiten, einzelnen Systemen oder ganzen Netzen. Wird ein solcher Angriff mittels mehrerer Systeme parallel ausgeführt, spricht man von einem verteilten bzw. Distributed *DoS* (*DDoS*). Diese können von zu einem *Botnetz* zusammengeschlossenen, kompromittierten Systemen ausgeführt werden oder auch von wissentlich zusammengeschalteten Rechnern von freiwilligen Teilnehmerinnen und Teilnehmern. Eine weitere Art von *DDoS-Angriffen* sind die sogenannten Reflection-Angriffe. Hierbei werden öffentlich erreichbare Server (zum

Beispiel NTP-Server) missbraucht, um den Angriff zu verstärken. Die Betreiberinnen und Betreiber solcher Server werden somit ungewollt zu Mittätern. Bei dieser Art von Angriff sind für die Erzielung der gleichen Wirkung wesentlich weniger Systeme notwendig als bei einem Angriff über ein klassisches *Botnetz*.

DDoS-Angriffe werden von Cyber-Kriminellen meist genutzt, um gezielt Schaden anzurichten, ihre Opfer zu erpressen oder Aufmerksamkeit für eine eigene Sache zu erregen, beispielsweise eine politische Forderung. Ein weiteres Motiv von *DDoS-Angriffen* liegt darin, andere Angriffe zu verschleiern oder erst zu ermöglichen.

DDoS-Angriffe existieren seit über 20 Jahren. Am 22. Juli 1999 wurde ein Computer der University of Minnesota in den USA mit einem Netzwerk aus 114 Rechnern, auf denen das Programm Trin00 lief, angegriffen. Dieser Vorfall gilt als der erste *DDoS*-Angriff (vgl. *Quellenverzeichnis*[33]).

Seitdem kennt die Entwicklung der *DDoS-Angriffe* im Wesentlichen nur die Richtung nach oben, die anhand stetig steigender *DDoS*-Parameter wie z. B. Angriffszahlen, Bandbreite und Paketratendurchsatz leicht nachvollziehbar ist.

So wurden von der Firma Netscout z. B. in Jahr 2020 erstmals mehr als 10 Millionen *DDoS-Angriffe* pro Jahr registriert (vgl. *Quellenverzeichnis*[34]). Link11 schätzt, dass 2020 weltweit insgesamt ca. 50 Millionen *DDoS-Angriffe* stattgefunden haben (vgl. *Quellenverzeichnis*[35]).

Ein begünstigender Faktor dafür ist der Bandbreitenausbau, denn dadurch können immer bandbreitenstärkere *DDoS-Angriffe* realisiert werden.

Daneben schafft aber auch die zunehmende Digitalisierung Raum für neue Angriffswege, auch mittels *DDoS-Angriffen*, wie die folgenden Beispiele zeigen:

Als eine Maßnahme zur Eindämmung der Covid-19-Pandemie wurden viele Unternehmensprozesse digitalisiert, z. B. indem Unternehmen ihren Betrieb durch Bildschirmarbeit aus dem Homeoffice fortführten. In der Umsetzung brachte dies häufig mit sich, dass zur Verarbeitung sensibler Geschäftsprozesse Informationstechnologie im privaten Umfeld genutzt wurde, ohne die zuvor noch hohen Sicherheitsstandards mit Firmenfirewalls im Hintergrund. Die verstärke Nutzung des öffentlichen Internets vergrößerte die quantitative und qualitative Angriffsfläche für *DDoS-Angriffe* signifikant. So mussten beispielsweise Remote-Zugänge ad hoc eingerichtet oder Mailserver kurzfristig aus dem öffentlichen Internet zugänglich gemacht werden. Trotz der vergrößerten Angriffsfläche liegen dem BSI jedoch keine Hinweise vor, dass es im Rahmen der COVID-19-Pandemie zu verstärkten *DDoS*-Aktivitäten in Deutschland gekommen ist.

Weiterhin ist zu beobachten, dass, wie auch in anderen Cybercrime-Bereichen, *DDoS-Angriffe* verstärkt für Erpressungen genutzt werden. Bekannt ist dieses Vorgehen bereits seit 2015, als ein privater E-Mail-*Provider* infolge eines *DDoS*-Erpressungsangriff zeitweise nicht erreichbar war (vgl. *Quellenverzeichnis*[36]). Die Ausweitung solcher Erpressungen zu langanhaltenden globalen *DDoS*-Erpressungskampagnen stellt eine Spezialisierung dar, die erstmalig im aktuellen Berichtszeitraum beobachtet wurde. Neben der bekannten Lösegelderpressung durch *Ransomware* (vgl. Kapitel *Big Game Hunting mit Ransomware*, Seite 12) stellt diese Cyber-Form der Schutzgelderpressung eine neue, ernstzunehmende Erscheinungsform von Cyber-Erpressung dar.

Bei einer seit Mitte August 2020 beobachteten Erpressungskampagne erhielten nationale und internationale Unternehmen vermehrt Erpresser-E-Mails (vgl. Vorfall *DDoS-Schutzgelderpressung*, Seite 34). Die Angriffe richteten sich gegen Unternehmen aus verschiedenen Branchen und schlossen auch Betreiber Kritischer Infrastrukturen ein (vgl. *Quellenverzeichnis*[37]). Im internationalen Umfeld wurde ein Erpressungsversuch auf die neuseeländische Börse NZX Ende August 2020 bekannt, in dessen Verlauf *DDoS-Angriffe* dazu führten, dass der Handel innerhalb von vier Tagen mehrfach gestoppt werden musste. Auch ein Angriff auf ein großes Fortune Global 500-Unternehmen Ende 2020 erlangte hohen Bekanntheitsgrad (vgl. *Quellenverzeichnis*[38]; Fortune Global 500 ist eine jährlich erscheinende Liste der 500 umsatzstärksten Unternehmen der Welt. Sie wird vom US-amerikanischen Wirtschaftsmagazin Fortune veröffentlicht). In Deutschland fanden mehrere derartige Angriffe statt, u. a. auf ein Unternehmen im Finanzsektor Ende August 2020 (vgl. *Quellenverzeichnis*[39]). Ebenso betroffen war auch die Branche der Bezahldienstleister. Hier fanden eine Reihe von Angriffen u. a. gegen die Bezahlsysteme MoneyGram, YesBank India, Worldpay, PayPal, Braintree und Venmo statt (vgl. *Quellenverzeichnis*[40]).

Auch der Einsatz veralteter Technologien (z. B. veraltete Servertechnologien), vergrößert die *DDoS*-Angriffsfläche. Dieser Effekt verstärkt sich zusätzlich, wenn diese Angriffsflächen zudem noch erklärte Ziele von politisch motivierten *DDoS*-Angreifern oder *DDoS*-Hacktivisten sind. Ein Beispiel aus dem Berichtszeitraum sind *DDoS*-Attacken auf Lernplattformen, die zur Aufrechterhaltung des schulischen Bildungssystems während der COVID-19-Pandemie eingeführt wurden.

Die Infrastrukturen, in denen Lernplattformen in Deutschland betrieben werden, sind heterogen. Sowohl zwischen den Ländern als auch innerhalb der Länder werden Lernplattformen in unterschiedlichen Infrastrukturen betrieben. Diese reichen von teilweise veralteten Servern, die von den Schulen oder den Schulträgern betrieben werden und auf denen die bereitgestellte Lernplattformsoftware betrieben wird, bis hin zu *Cloud*-Lösungen für Lernplattformen. *Cloud*-Lösungen verzeichneten dabei in den letzten Monaten einen verstärkten Zuwachs.

Die Wahl der zugrundeliegenden Infrastruktur wird dabei von mehreren Parametern (z. B. finanzielle Mittel im Bildungssystem, technologische Ausstattung und Digitalisierungsgrad der Schulen, fachliche Kompetenz im Umgang mit den Infrastrukturen in den Schulen, usw.) bestimmt.

Je nach Art der zugrundeliegenden Infrastruktur, in welcher die Lernplattformen betrieben werden, ergeben sich unterschiedliche Risikoprofile für *DDoS-Angriffe*.

Cloud-Lösungen bieten technologiebedingt (zum Beispiel durch hochbandbreitige Anbindung, Administration durch fachkundiges Personal, usw.) in der Regel bereits wirksame Schutzmaßnahmen gegen *DDoS-Angriffe*, die je nach Geschäftsmodell durch Mitigationsmaßnahmen erweitert werden können. Demgegenüber stehen beispielsweise dezentral verwaltete und veraltete Schulserver *DDoS-Angriffen* nahezu schutzlos gegenüber. Für diese ergibt sich hierdurch ein hohes bis sehr hohes Risikoprofil für den Betrieb von Lernplattformen. So wurde im September 2020 bekannt, dass es einem 16-jährigen Schüler aus Miami, USA, gelungen war, den Online-Unterricht seiner Schule South Miami Senior High über drei Tage zu stören, indem er die Server des viertgrößten US-amerikanischen Schulbezirks Miami Dade angegriffen hat. Für den Angriff nutzte er das bereits seit Jahren nicht mehr weiterentwickelte Tool Low Orbit Ion Cannon (LOIC). Der Erfolg des Angriffs war überraschend, da LOIC-Angriffen nur ein geringes Bedrohungspotenzial bei aktuellen Konfigurationseinstellungen im Zielsystem zugesprochen wird.

In Deutschland standen Lernplattformen aufgrund ihrer Bedeutung für die Bildungssysteme der Länder unter Pandemiebedingungen sehr stark in der öffentlichen Wahrnehmung. Zudem verzeichnen Lernplattformen ein starkes Wachstum der Nutzerzahlen. Das Hasso-Plattner-Institut (HPI) meldete, dass mitten im zweiten harten Lockdown die HPI Schul-*Cloud* die Grenze von 1.000.000 Nutzern überstiegen hätte. Seit März 2020 habe sich die Nutzerzahl der Lernplattform des HPI damit nahezu verdreißigfacht (vgl. *Quellenverzeichnis*[41]).

Der Zusammenhang zwischen Lernplattformen und den Maßnahmen zur Eindämmung der COVID-19-Pandemie ist ein Grund für politisch motivierte *DDoS*-Angriffe, sogenannter Hacktivismus (digitaler Vandalismus), auf Lernplattformen. Erfahrungsgemäß ist eine stark treibende Motivation zur Durchführung solcher *DDoS-Angriffe*, ob und inwieweit das Angriffsziel in der öffentlichen Wahrnehmung steht und wie stark die vom Angreifer erwarteten Schutzmaßnahmen sind. Das BKA hat am 20.01.2021 eine Warnmeldung hierzu veröffentlicht (vgl. *Quellenverzeichnis*[42]).

Insgesamt zeigte sich im Berichtszeitraum, dass *DDoS*-Angriffe unter den Cyber-Angriffen etabliert sind, deren Bedrohungspotenzial sich im Lauf der Zeit durch Entwicklungen hinsichtlich Vielfältigkeit und Einfallsreichtum in seinen Erscheinungsformen stetig gesteigert hat. Eine permanente Implementierung und Anpassung von geeigneten Schutzmaßnahmen ist erforderlich.

Als Cyber-Sicherheitsbehörde des Bundes stellt das BSI aktuelles und umfangreiches Informationsmaterial für die Prävention und Abwehr von *DDoS-Angriffen* bereit und veröffentlicht eine Liste qualifizierter *DDoS*-Mitigation-Dienstleister mit Auswahlkriterien:[h)]

DDoS-Schutzgelderpressung

Sachverhalt

Im Zuge einer globalen *DDoS*-Erpressungskampagne im dritten und vierten Quartal 2020 wurden bei vielen Erpressungen häufig ähnliche Vorgehensweisen und technische Übereinstimmungen beobachtet.

So erfolgte der initiale Kontakt oft mit einer Erpressungs-E-Mail, in der ein bevorstehender *DDoS*-Angriff auf das Unternehmen angekündigt wurde, falls eine Schutzgeldforderung in Bitcoins (BTC) innerhalb einer genannten Frist nicht gezahlt würde. Um die Ernsthaftigkeit ihrer Forderungen zu unterstreichen, kündigten die Angreifer sog. Warn-Angriffe an und führten diese auch durch. Angriffe dieser Art zeichneten sich durch sehr hohe Bandbreiten bis zu 200 Gbit/s aus und erstreckten sich über mehrere Stunden. Für den Fall, dass den Lösegeldforderungen nicht nachgekommen wird, wurden zusätzliche Angriffe von angeblich über 2 Tbit/s zu einem späteren Zeitpunkt angedroht. Während diese letztgenannten Angriffe in den meisten Fällen ausblieben, wurden sie bei der Erpressung der neuseeländischen Börse NZX tatsächlich umgesetzt. Die Angriffe basierten auf UPD-Floods, TCP-Floods und SYN-Floods. Zur Steigerung der Angriffsvolumina setzten die Täter auf die Reflection-Amplification-Vektoren WS-Discovery und Apple Remote Control sowie DNS (vgl. *Quellenverzeichnis*[43]). Ebenso beobachtet wurden Angriffe mit den *Angriffsvektoren* GRE-Protocol-Flood und SNMP-Flood (vgl. *Quellenverzeichnis*[44]).

In der Folge breitete sich die Kampagne auf weitere Branchen aus. Ab September / Oktober 2020 meldeten mehrere deutsche Internet-Service-*Provider* (ISPs) *DDoS*-Erpressungen. Die Vorgehensweisen ähnelten sich auch hier häufig. Oft starteten die Angreifer zunächst mit SYN-Flood-Angriffen gegen Reverse-Proxys. Die Angriffswirkung wurde durch übermäßig hohe Paketraten bei gleichzeitig geringen Bandbreiten (ca. 1 - 2 Gbit/s) erzielt. Danach wurden die Angriffe mit veränderter Vorgehensweise fortgesetzt, z. B. mit ACK-Flood-Angriffen, bei denen die Angriffswirkung durch eine übermäßig hohe Anzahl von Anfragen erzeugt wurde.

Teil der Bedrohungsstrategie einiger *DDoS*-Erpresser war, sich als bekannte APT-Gruppierungen auszugeben, z. B. als Fancy Bear (aka. Sofacy oder Sednit), Armada Collective (vgl. *Quellenverzeichnis*[45]) oder Lazarus. Die *DDoS*-Erpresser, die sich als Fancy Bear oder Lazarus ausgaben, waren bereits im Oktober 2019 mit *DDoS-Angriffen* in Erscheinung getreten. Diese Strategie zielt nach BSI-Einschätzung darauf, Handlungsdruck beim Opfer zu erzielen, da es sich vermeintlich Angreifergruppen ausgesetzt sieht, über die in der Vergangenheit im Zusammenhang mit nachrichtendienstlichen Aktivitäten berichtet wurde. Die Erpresserschreiben aus 2019 und 2020 sind im Text weitgehend identisch. Lediglich die Bitcoin-Adressen für die Schutzgeldzahlung unterschieden sich (vgl. *Quellenverzeichnis*[46]).

In den Bezahlmodellen der genannten Gruppen gab es Unterschiede: Erpressungsforderungen, die im Namen von Armada Collective gestellt wurden, begannen häufig bei fünf bis zehn BTC (1 BTC ~ 48.000 Euro mit Stand März 2021) und steigerten sich um fünf BTC, wenn innerhalb der genannten Frist kein Schutzgeld gezahlt wurde. Danach erhöhte sich die Forderung um fünf BTC pro Tag. Forderungen, die im Namen von Fancy Bear gestellt wurden, begannen dagegen häufig bei 15 - 20 BTC und steigerten sich beim Erreichen der Frist ohne Zahlung auf 30 BTC, um danach weiter um zehn BTC pro Tag anzuwachsen (vgl. *Quellenverzeichnis*[47], vgl. *Quellenverzeichnis*[48]).

Ende Januar 2021 informierte eine europäische Partnerbehörde des BSI mit Bezug auf eine Veröffentlichung von Radware (vgl. *Quellenverzeichnis*[49]), dass die *DDoS*-Erpresser sich wieder an die Opfer wendeten, die in der Vergangenheit noch nicht gezahlt hatten. Radware veröffentlichte hierzu die Inhalte der Schreiben, die wie folgt begannen: “Maybe you forgot us, but we didn’t forget you. We were busy working on more profitable projects, but now we are back.” Fortgesetzt wurden die Schreiben wie folgt: “We asked for 10 bitcoin to be paid at <bitcoin address> to avoid getting your whole network DDoSed. It’s a long time overdue and we did not receive payment. Why? What is wrong? Do you think you can mitigate our attacks? Do you think that it was a prank or that we will just give up? In any case, you are wrong.”[II)]

[II)] „Sie haben uns vielleicht vergessen, wir haben Sie aber nicht vergessen. Wir haben uns mit profitableren Projekten beschäftigt, aber jetzt sind wir zurück. ... Wir haben Sie darum gebeten, 10 Bitcoin an <Adresse> zu zahlen, um zu verhindert, dass das gesamte Netzwerk ge-*DDoS*-t wird. Es ist lange überfällig und wir haben bisher noch keine Zahlung erhalten. Warum? Wo ist das Problem? Glauben Sie, Sie können unsere Angriffe entschärfen? Denken Sie, das war alles nur ein Scherz und wir geben einfach so auf? Da liegen Sie auf jeden Fall falsch.“

Bewertung
Dem BSI sind noch keine Fälle von derartigen Zahlungserinnerungen bekannt geworden. Es ist jedoch nicht auszuschließen, dass *DDoS*-Erpressungen auch im nationalen Umfeld eine vergleichbare Renaissance erleben.

Reaktion
Das BSI hat seine Zielgruppen in Staat, Wirtschaft und Gesellschaft über die Erpressungskampagne informiert und Gegenmaßnahmen empfohlen. Insbesondere sollten Erpressungsopfer prüfen, welche Folgen der Ausfall der verschiedenen, angreifbaren Komponenten haben kann. Zudem sollte im Falle eines ersten Test-Angriffs der IT-Sicherheitsdienstleister vorgewarnt und Anzeige erstattet werden.

Das BSI empfiehlt grundsätzlich, kein Lösegeld und auch kein Schutzgeld zu zahlen, um das Geschäftsmodell der Cyber-Erpressung nicht zu unterstützen und nicht noch weitere Angriffe auf eigene oder andere Ziele zu motivieren.

DDoS-Angriff auf einen belgischen Internet-*Provider*

Sachverhalt
Am 4. Mai 2021 fand ein *DDoS*-Angriff auf einen großen belgischen Internet-*Provider* statt (vgl. *Quellenverzeichnis*[50]).
Der Angriff begann um 11 Uhr und war in seinen Auswirkungen massiv. Der Berichterstattung zufolge waren ca. 200 Organisationen zumindest temporär beeinträchtigt. Typische Kunden des *Providers* sind Universitäten, Forschungseinrichtungen, aber auch Regierungseinrichtungen. So konnten mehrere Parlamentssitzungen nicht stattfinden, da sich mobile Teilnehmerinnen und Teilnehmer nicht verbinden konnten.

Betroffen waren auch Online-Angebote, wie etwa das belgische Webportal für die Reservierung von COVID-19-Impfterminen.

Laut Medienberichten wiesen einige belgische Politiker über Twitter darauf hin, dass der Angriff etwa zur gleichen Zeit begann, als der Ausschuss für auswärtige Angelegenheiten des Parlaments eine Sitzung abhalten wollte.

Gegenmaßnahmen wurden durch den *Provider* eingeleitet, sodass die Überlastung der Leitungen gegen 17 Uhr desselben Tages gemildert werden konnte. Nach Einschätzung der belgischen Partner des BSI schien der Angriff durch seine technische Natur nicht einfach abzuwehren zu sein. Die Strafverfolgung wurde eingeleitet.

Bewertung
Dem BSI liegen keine Erkenntnisse über die Angreifer und deren Motivation vor. Ein politischer Hintergrund kann aufgrund des zeitlichen Zusammenhangs mit der Ausschusssitzung des belgischen Parlamentes nicht ausgeschlossen werden.

DDoS-Angriffe bleiben nach wie vor ein Angriffsmittel, das – entsprechende Ressourcen auf Angreiferseite vorausgesetzt – zumindest temporär einzelne Organisationen oder in extremen Fällen einzelne *Provider* durch Überlastung vom Internet trennen und Organisationen in ihrer Arbeitsfähigkeit einschränken können. In der Regel hängt die Dauer bis zur Behebung der Störungen von den Vorbereitungen der angegriffenen Organisation (z. B. durch Einkauf von *DDoS*-Mitigation-Diensten) und von der Vernetzung mit Upstream-*Providern* ab. Bei Bedarf können Upstream-*Provider* Angriffsverkehre drosseln bzw. umlenken, brauchen dafür aber eine möglichst exakte Charakterisierung des Angriffsverkehrs. Aus diesem Grund variieren Täter (wie im vorliegenden Fall) ihre Angriffstaktik ggf. sogar mehrfach. Da dies eine komplexe Abwehrstrategie erfordert, besteht mitunter ein hohes Bedrohungspotential.

Maßnahmen
Das BSI stand mit internationalen Partnern im Austausch zu dem Angriff. Auch dieser Angriff, der Dritte getroffen hat, ist ein guter Anlass, die eigenen *DDoS*-Mitigation-Planungen, -Vorbereitungen und -Prozesse nochmals abzugleichen, zu prüfen und ggf. anzupassen.
Das BSI hat zur *DDoS*-Mitigation Dienstleister qualifiziert:[i)]

1.7 Angriffe im Kontext Kryptografie

Kryptografische Mechanismen sind wichtige Bausteine für die Umsetzung von Sicherheitsfunktionen in IT-Produkten. Dem Stand der Technik entsprechende Kryptoalgorithmen liefern hierfür grundsätzlich ausgezeichnete Sicherheitsgarantien. Das BSI empfiehlt in der Technischen Richtlinie TR-02102 eine Reihe kryptografischer Verfahren und Protokolle, die aufgrund eingehender mathematischer Kryptoanalyse allgemein als sicher angesehen werden.

Folgende Aspekte können dazu führen, dass ein Kryptosystem in der Praxis nicht den vorgesehenen Zweck erfüllt:

- Schwächen in kryptografischen Mechanismen oder Protokollen
- Implementierungsfehler
- Unzureichend abgesicherte Seitenkanäle
- Schwächen in der Schlüsselerzeugung

Eine klassische Anwendung der Kryptografie ist die Absicherung der Kommunikation über offene Netzwerke wie das Internet. Für vertrauliche und integritätsgeschützte Verbindungen stehen verschiedene kryptografische Protokolle zur Verfügung, für die gemeinhin angenommen wird, dass ein Angreifer mit Netzwerkzugriff weder die geheimen Schlüssel in Erfahrung bringen noch Nachrichten entschlüsseln oder unbemerkt manipulieren kann. Für die Wirksamkeit der kryptografischen Protokolle muss zum einen die korrekte Implementierung sichergestellt sein. Zum anderen muss verhindert werden, dass das an der Netzwerkschnittstelle beobachtbare Verhalten der Geräte (z. B. Fehlermeldungen oder Antwortzeit) Informationen über verarbeitete Geheimnisse preisgibt. Im Berichtszeitraum wurde beispielsweise ein neuer Angriff veröffentlicht, der Laufzeitunterschiede in einem kryptografischen Protokoll ausnutzt (siehe Infokasten *Raccoon-Angriff*, Seite 37).

Bei der Absicherung von Kryptosystemen, die selbst Angreifern in räumlicher Nähe standhalten sollen, müssen neben der Laufzeit noch weitere Seitenkanäle (z. B. Stromverbrauch oder elektromagnetische Abstrahlung der Geräte) berücksichtigt werden, über die ebenfalls Geheimnisse abfließen können. Die Seitenkanalanalyse, also die Analyse auf Anfälligkeit für *Seitenkanalangriffe*, ist heute ein eigener Forschungszweig, der neben Gegenmaßnahmen auch neue *Angriffsvektoren* hervorgebracht hat. Ein aktueller Trend in der Seitenkanalanalyse und der mathematischen Kryptoanalyse ist der Einsatz von Methoden der Künstlichen Intelligenz (siehe Kapitel *Künstliche Intelligenz*, Seite 82).

Eine wesentliche Voraussetzung für den sicheren Einsatz von Kryptografie ist die Erzeugung von Zufallszahlen, die gewisse Gütekriterien erfüllen. Zufallszahlen werden unter anderem für die Schlüsselerzeugung benötigt. Für kryptografische Anwendungen dürfen Zufallszahlen nicht vorhersagbar sein und dürfen keine ausnutzbaren statistischen Defekte aufweisen. Um Angriffen durch schwache Zufallszahlen vorzubeugen, definiert das BSI in den AIS 20 und AIS 31 (Anwendungshinweise und Interpretationen zum Schema) Funktionalitätsklassen von Zufallszahlengeneratoren für verschiedene Einsatzzwecke. Positiv hervorzuheben ist, dass mittlerweile viele Produkte über einen im deutschen Common-Criteria-Schema (siehe Kapitel *Zertifizierung*, Seite 64) zertifizierten physikalischen Zufallszahlengenerator verfügen.

Die Sicherheitsgarantien vieler heute eingesetzter Kryptoalgorithmen gelten allerdings nicht mehr, sobald ein hinreichend leistungsstarker Quantencomputer zur Verfügung steht. Das Kapitel *Kryptografie* (Seite 84) zeigt Möglichkeiten auf, dieser Bedrohung zu begegnen, und stellt die Aktivitäten des BSI in diesem Bereich dar.

Raccoon-Angriff

Ein Team von Sicherheitsforschern und Kryptologen der Ruhr-Universität Bochum, der Universität Tel Aviv, der Universität Paderborn und des BSI hat im September 2020 einen neuen Timing-Angriff gegen das TLS-Protokoll (Transport Layer Security) unter der Bezeichnung Raccoon veröffentlicht. Das TLS-Protokoll ermöglicht die verschlüsselte Kommunikation zwischen einem Client und einem Server, etwa zwischen einem Webbrowser und einem Webserver im Internet.

Timing-Angriffe nutzen Laufzeitdifferenzen in kryptografischen Implementierungen aus, um Rückschlüsse auf verarbeitete Geheimnisse zu ziehen. Der Raccoon-Angriff zielt auf das gemeinsame Geheimnis ab, auf das sich Client und Server bei Verwendung des Diffie-Hellman-Schlüsselaustauschs (DH) einigen. Der TLS-Standard schreibt für TLS 1.2 und frühere TLS-Versionen vor, dass führende Null-Bytes des gemeinsamen DH-Geheimnisses entfernt werden müssen. Diese Designschwäche in der TLS-Spezifikation kann unter geeigneten Bedingungen dazu führen, dass Geheimnisse mit führenden Null-Bytes schneller weiterverarbeitet werden als Geheimnisse ohne führende Null-Bytes. Ein Netzwerkangreifer, der die Schlüsselaushandlung zwischen einem Client und Server beobachtet, kann daher durch hinreichend präzise Zeitmessungen herausfinden, ob das ausgehandelte DH-Geheimnis mit einem Null-Byte beginnt oder nicht.

Ein Byte des gemeinsamen DH-Geheimnisses zu kennen reicht noch nicht aus, um die Verschlüsselung der TLS-Verbindung zu brechen. Der Angreifer kann jedoch die TLS-Verbindung aufzeichnen und anschließend Abwandlungen des öffentlichen DH-Schlüssels des Clients nutzen, um selbst Verbindungen mit dem TLS-Server aufzubauen. Wenn der TLS-Server seinen DH-Schlüssel mehrfach verwendet, können dadurch viele unterschiedliche Einzelinformationen aus den Antwortzeiten des Servers ermittelt werden, die in Zusammenhang mit der ursprünglichen TLS-Verbindung stehen. Mit einem mathematischen Verfahren ist es dann möglich, aus den Einzelinformationen das gemeinsame DH-Geheimnis von Client und Server zu berechnen, mit dem die aufgezeichnete TLS-Verbindung schließlich entschlüsselt werden kann.

Insgesamt handelt es sich beim Raccoon-Angriff um einen komplexen Angriff, der nur unter speziellen Rahmenbedingungen und mit hohem Aufwand durchführbar ist. Die praktische Gefährdung durch diesen Angriff ist also eher gering. Dennoch identifiziert der Raccoon-Angriff eine Schwachstelle, die bei der Entwicklung neuer Protokolle vermieden werden sollte.

Die neueste TLS-Version 1.3 und der Diffie-Hellman-Schlüsselaustausch über elliptischen Kurven (TLS-ECDH und TLS-ECDHE) sind nicht vom Raccoon-Angriff betroffen.

Weitere Informationen zum Raccoon-Angriff sind auf der Webseite https://raccoon-attack.com abrufbar.

1.8 Hybride Bedrohungen

Hybride Bedrohungen bezeichnen verschiedene Formen illegitimer Einflussnahme durch fremde Staaten und deren Proxies, beispielsweise neben verschiedenen Formen von Cyber-Angriffen auch durch die Beeinflussung der öffentlichen Meinungs- und Willensbildung durch online verbreitete Desinformation und Propaganda oder wirtschaftliche Druckmittel zur Durchsetzung politischer Ziele. Typischerweise können diese Aktivitäten mehrere Wirkungsbereiche oder Stufen sowie eine große Bandbreite an verdeckten und offenen Mitteln umfassen. Die im Rahmen von hybriden Bedrohungen eingesetzten Mittel ermöglichen es den jeweiligen Akteuren oft, verhältnismäßig einfach die Täterschaft und die dahinterliegenden Motivationen zu verschleiern bzw. abzustreiten. Ein Beispiel für Angriffe im Sinne hybrider Bedrohungen sind Cyber-Spionageangriffe, die sensible Informationen rechtswidrig aus IT-Systemen abgreifen, um diese in einem zweiten Schritt manipulativ zu verbreiten und so im Informationsraum mittels Diskreditierung oder Desinformation schädliche Wirkung zu entfalten. Auch Cyber-Sabotageangriffe können das Ziel verfolgen in weiteren Bereichen, z. B. in der Wirtschaft, insbesondere aber auch in Kritischen Infrastrukturen schädlich einzuwirken und die daraus folgenden Auswirkungen im Informationsraum manipulativ auszunutzen.

Die Digitalisierung blieb auch im Berichtszeitraum ein maßgeblicher Treiber der Dynamik hybrider Bedrohungen, da sich aus ihr neue potenzielle Verwundbarkeiten von Staat, Wirtschaft und Gesellschaft eröffnet

haben. Der Domäne Cyber-Raum kommt deshalb in hybriden Kampagnen eine herausgehobene Stellung zu. Zusätzlich hat sie eine Querschnittsfunktion, da auch Maßnahmen in anderen Domänen oft erst durch sie ermöglicht werden. In einer hybriden Kampagne können die physische Schicht (z. B. Hardware und *Firmware*), die logische Schicht (z. B. Virtualisierungen und Betriebssysteme) und die informationelle Schicht (z. B. Anwendungen und Daten) des Cyber-Raums ausgenutzt werden. Im Berichtszeitraum zeigte z. B. die andauernde COVID-19-Pandemie, wie Akteure versuchten, mittels Cyber-Angriffen und Desinformationen europäische Impfkampagnen zu beeinflussen. So wurde die Europäische Arzneimittelagentur EMA im Dezember 2020 Ziel eines Cyber-Angriffs. Infolgedessen kam es zu einem Datenabfluss im Zusammenhang mit einem laufenden Zulassungsverfahren für einen COVID-19-Impfstoff (vgl. Vorfall *Cyber-Angriff gegen die Europäische Arzneimittelagentur EMA,* Seite 41). Abgeflossene Dokumente tauchten später im Darknet auf. Durch die selektive Verbreitung solcher gestohlenen Informationen können hybride Akteure versuchen, die öffentliche Meinung in illegitimer Weise zu beeinflussen und Falschbehauptungen Vorschub zu leisten.

Desinformation, d. h. die gezielte Verbreitung falscher und irreführender Informationen in täuschender Absicht ist ein häufiges Mittel hybrider Bedrohungen. Dieses stützt sich in einer digitalisierten Welt zunehmend auf technische, digitale Hilfsmittel und Kanäle. Wenn Daten digital gespeichert oder verarbeitet werden, dient IT-Sicherheit auch dem Schutz vor deren unautorisierter Verbreitung (Hack and Leak). Bei Hack and Leak-Angriffen ist auch die Manipulation authentischer Informationen möglich, etwa das Verfälschen von Foto-, Video- und Tonaufnahmen, ebenso das Vortäuschen einer bestimmten Urheberschaft einer Datenübermittlung (z. B. einer E-Mail oder eines Beitrags in Sozialen Netzwerken). Bei der Identifizierung solcher Manipulationen bringt das BSI seine technische Fachexpertise ein.

Als Cyber-Sicherheitsbehörde des Bundes unterstützt das BSI außerdem die Betreiber Kritischer Infrastrukturen, wirkt auf die Verbesserung der IT-Sicherheit im Rahmen von Wahlen hin, steht im Austausch mit den Betreibern Sozialer Netzwerke, z. B. im Rahmen einer Initiative zur Entwicklung von Sicherheitsempfehlungen, und sensibilisiert die Bevölkerung für IT-Sicherheitsthemen. Das BSI beteiligt sich zudem auch international, unter anderem im Austausch mit der Fachcommunity. Dadurch trägt das BSI auf unterschiedliche Weise dazu bei, die technische und gesellschaftliche *Resilienz* gegenüber hybriden Bedrohungen zu stärken.

1.9 Gefährdungen der Cyber-Sicherheit durch die COVID-19-Pandemie

Die COVID-19-Pandemie wirkte als Katalysator für die Digitalisierung des wirtschaftlichen und gesellschaftlichen Lebens in Deutschland. So sahen sich viele Unternehmen und öffentliche Einrichtungen mit der Herausforderung konfrontiert, ihre Geschäftstätigkeiten und Dienstleistungen verstärkt digital anbieten zu müssen. In gleichem Maße, wie sich für Betriebe und Behörden durch die schlagartige Einführung digitaler Arbeitsmittel und des Arbeitens von Zuhause neue Möglichkeiten eröffneten, boten sich auch für Cyber-Kriminelle in der Pandemie neue Gelegenheiten, diese auszunutzen. Das BSI registrierte bereits während des ersten Lockdowns im Frühjahr 2020 cyber-kriminelle Angriffe, bei denen versucht wurde, die Pandemielage als thematischen Aufhänger für *Phishing*- und andere Social-Engineering-Angriffe auszunutzen (vgl. *Quellenverzeichnis*[51]).

Dieser Trend hat sich im vergangenen Jahr fortgesetzt. Trotz der deutlich vergrößerten Angriffsfläche, die durch die Verlagerung vieler Tätigkeiten ins mobile Arbeiten entstand, konnte das BSI keine signifikante Steigerung der Anzahl an Angriffen feststellen. Viele Cyber-Kriminelle haben ihren thematischen Aufhänger für Social-Engineering-Angriffe lediglich auf die Pandemie zugeschnitten, nicht jedoch gänzlich neue Angriffsarten entwickelt.

Anhand seiner Lagebeobachtung geht das BSI davon aus, dass viele der zu Beginn der Pandemie festgestellten technischen und organisatorischen Probleme bei der Einführung dezentraler Arbeitsweisen, wie beispielsweise die Verfügbarkeit eines zentralen IT-Supports, fortbestehen. Daher nimmt das BSI an, dass viele Organisationen durch die Verlagerung ihrer Tätigkeiten in den digitalen Raum weiterhin eine potenziell größere Angriffsfläche aufweisen, als es vor der Pandemie der Fall war. Aus diesem Grund appelliert das BSI bei der Einrichtung und dem Betrieb digitaler Lösungen, auch wenn diese kurzfristig eingerichtet werden müssen, die IT-Sicherheit nicht hintanzustellen.

Ausnutzung der Pandemie für Social-Engineering-Angriffe

Das BSI beobachtete im Berichtszeitraum eine große Bandbreite an Social-Engineering-Angriffen, die das Thema der COVID-19-Pandemie ausnutzten (vgl. Kapitel *Phishing und weitere Betrugsformen*, Seite 24). Beispielsweise registrierte das BSI offiziellen Internetseiten nachgeahmte Internetauftritte, die dem vermeintlichen Verkauf einer Vielzahl von gefälschten Produkten dienten. Zum Kauf

angeboten wurde vor allem in der Pandemie nachgefragte Schutzausrüstung oder auch COVID-19-Vakzine. In zumindest einem Fall wurde eine Internetseite zur Beantragung von COVID-19-Wirtschaftshilfen gefälscht, um die bei der Beantragung notwendigen umfangreichen persönlichen Daten abzugreifen (vgl. *Quellenverzeichnis*[52]). Diese Daten ermöglichten es Kriminellen, sich der Identität der Opfer zu ihren eigenen Gunsten zu bedienen. Sie wurden zum Beispiel genutzt, um im Namen des Opfers Unterstützungsleistungen zu beantragen und deren Auszahlung umzuleiten. Solche umfangreichen persönlichen Daten werden von Kriminellen auch auf illegalen Marktplätzen meistbietend verkauft (vgl. *Kapitel Schadprogramme und Daten-Leaks*, Seite 25). Um diesen Gefahren zu begegnen, unterstützte das BSI in Zusammenarbeit mit der Verbraucherzentrale NRW die Polizei bei der Suche nach auf diese Art gefälschten Internetseiten, sodass diese, wo möglich, aus dem Internet entfernt werden konnten.

Eine neue Gefährdungslage trat im vergangenen Jahr durch Vorfälle ein, bei denen Cyber-Kriminelle oder staatliche Akteure gezielt Firmen und Behörden aus dem Gesundheitsbereich angriffen. Anders als noch zu Beginn der Pandemie beobachtete das BSI im aktuellen Berichtszeitraum gezielte IT-Angriffe mit Bezug zu COVID-19 auf Schlüsselbereiche des Gesundheitssektors. Hierzu zählen beispielsweise der Angriff auf die Europäische Arzneimittelagentur (EMA), Angriffe auf ausländische Impfstoffhersteller, ein *DDoS*-Angriff auf das COVID-19-Impfportal des Bundeslandes Thüringen und ein *Ransomware*-Angriff auf einen deutschen Hersteller von COVID-19-Antigentests (vgl. Vorfall *Cyber-Angriff gegen die Europäische Arzneimittelagentur EMA,* Seite 41).

Vergrößerung der Angriffsfläche

Angriffe auf Videokonferenzen: Zur Realisierung von Homeoffice und Homeschooling stellen Konferenzmöglichkeiten ein essentielles Hilfsmittel dar. So gewannen im zurückliegenden Berichtszeitraum verschiedene Produkte für Telefon- und Videokonferenzen besondere Bedeutung für die Aufrechterhaltung beruflicher, aber auch privater Kommunikation. Durch die teilweise zwingende Erreichbarkeit derartiger Systeme über das freie Internet sind sie ein attraktives und leicht zu erreichendes Ziel für Cyber-Angriffe. Dem BSI wurden gezielte Cyber-Angriffe gegen bestimmte Meetings bekannt, bei denen sich Unbefugte mittels zuvor abgeflossener Daten Zugang zu internen Besprechungen verschafften und diese ausspionierten oder sabotierten. (vgl. *Kapitel Cyber-Angriffe auf Videokonferenzen*, Seite 25).
Das BSI hat Empfehlungen zum sicheren Umgang mit Telefon- und Videokonferenzen ausgesprochen:[j)]

***VPN*-Sicherheit:** In der Regel sind Organisationsnetzwerke vom offenen Internet abgetrennt und weisen nur für vereinzelte Dienste sogenannte Netzübergänge auf. Solche Dienste können beispielsweise E-Mail-Server oder Proxy-Server für den Internetverkehr aus dem Organisationsnetzwerk heraus oder auch *VPN*-Server sein. Beim Zugriff auf ein Organisationsnetzwerk nehmen diese *VPN*-Server eine außergewöhnliche Rolle ein. Sie sollen sicherstellen, dass sich nur dazu Befugte aus dem Internet in das Organisationsnetzwerk einwählen und dort agieren können, ganz so, als würde der Befugte beispielsweise in den Büroräumen ebenjener Organisation selbst sitzen. Hierfür erfolgt zum einen eine Authentifikation gegenüber dem *VPN*-Server zur Verifizierung der Identität und Befugnis des Einwählenden und zum anderen wird die Verbindung zwischen dem Einwählenden und dem *VPN*-Server verschlüsselt. So wird effektiv verhindert, dass der Netzverkehr in unverschlüsselter Form mitgelesen oder manipuliert werden kann. Um die beschriebene Schutzwirkung auch erzielen zu können, müssen *VPN*-Lösungen und die Architektur des Organisationsnetzwerks aufeinander abgestimmt sein. Durch die teilweise kurzfristigen Anpassungen beim Wechsel ins Homeoffice dürfte diese notwendige Abstimmung sowie die sichere Konfiguration von *VPN*-Lösungen und den ähnlichen Zwecken dienenden Remote-Lösungen (wie das Remote Desktop Protokoll (RDP)) nicht flächendeckend erfolgt sein. Hinzu kommt, dass derartige Remote-Lösungen bereits vor der Pandemie beispielsweise von Angreifern, die in Zusammenhang mit bekannter *Ransomware* stehen, häufig ausgenutzt wurden. Schlecht abgesicherte Lösungen können also von Seiten der Angreifer ohne den Aufbau von zusätzlichem Wissen kurzfristig ausgenutzt werden. Da die Absicherung von Remote-Lösungen auch unabhängig von der Pandemie aus Sicht des BSI eine besondere Rolle einnimmt, hat das BSI in der Allianz für Cyber-Sicherheit Empfehlungen zusammengetragen:[k)]

BYOD: Bring Your Own Device (BYOD) bezeichnet den Einsatz privater IT im beruflichen Kontext. So können etwa berufliche Telefonate über private Mobiltelefone geführt, privater und beruflicher Kalender zwischen Heim-PC und Bürocomputer synchronisiert und der vom Arbeitgeber zur Verfügung gestellte USB-Stick auch für private Zwecke verwendet werden. Insbesondere zur Bewältigung von Homeoffice-Anforderungen stellten und stellen BYOD-Lösungen eine für Arbeitgeber wie auch für Arbeitnehmer komfortable Lösung dar. Zugleich geht von privaten Geräten, die im beruflichen Kontext genutzt werden oder gar mit Firmennetzwerken verbunden werden, ein hohes Risiko aus. So ist eine mit einem Schadprogramm behaftete E-Mail schon auf einem gut abgesicherten Firmengerät in einem widerstandsfähigen Firmennetzwerk eine erhebliche Bedrohung.

Wird eine solche *maliziöse* E-Mail aber – etwa über eine Webanwendung – von einem privaten, weniger gut abgesicherten Gerät aus geöffnet, findet das Schadprogramm auf diesem Privatgerät oftmals leichter ausnutzbare Schwachstellen vor. Das Öffnen und Bearbeiten von E-Mail-Verkehr und damit auch potenziell *maliziöser Spam*-Mails, die an Organisations-E-Mail-Adressen gerichtet sind, wird daher aller Wahrscheinlichkeit nach zu einer leichteren und schnelleren Infektion auf einem privaten PC führen, als es sonst der Fall wäre. Damit hat ein Angreifer den wichtigsten Schritt bereits geschafft und einen Fuß in der Tür zum Firmennetzwerk. Bei der Absicherung eines Organisationsnetzwerks stellen BYOD-Lösungen auch aus Administratorensicht eine ernsthafte Herausforderung dar, da zum Beispiel die Sicherstellung von aktuellen *Patches* auf privaten Geräten nur schwer garantiert werden kann. Aus diesen und weiteren Gründen hat das BSI bereits im ersten Lockdown aktuelle Empfehlungen zum sicheren Umgang mit dem Thema Homeoffice ausgesprochen:[1)]

Schatten-IT: Ähnlich risikobehaftet ist sogenannte Schatten-IT in Unternehmen, also Geräte, die fachseitig beschafft wurden und daher nicht von der zentralen IT-Administration verwaltet werden. Dabei kann es sich beispielsweise um Testgeräte, Präsentationslaptops, Laborserver oder Ähnliches handeln. Für die Einrichtung und Verwaltung solcher Geräte, insbesondere für die Versorgung mit Sicherheitsupdates, gibt es häufig keine klare Zuständigkeit. Das Sicherheitsniveau solcher Geräte weicht daher unter Umständen deutlich von den übrigen Unternehmensstandards ab. Häufig ist das Ausmaß der in einer Organisation vorhandenen Schatten-IT sogar gänzlich unbekannt. Schatten-IT stellt daher, insbesondere unter Bedingungen des verstärkten Homeoffice, ein schwer zu kalkulierendes Risiko dar.

Internetstabilität in der Pandemie: Durch die umfangreiche Nutzung des mobilen Arbeitens und die Tatsache, dass durch die Ausgangsbeschränkungen mehr Zeit zu Hause verbracht wird, steigt der Bedarf an Internetkapazität – sei es für *VPN*-Zugänge und Video-Meetings oder für Video-Streaming und Online-Gaming. Diese steigende Nutzung ist auch bei Internet-Betreibern spürbar. Insbesondere im März und April 2020 wurde medienöffentlich regelmäßig über das steigende Verkehrsaufkommen bei Internetzugangsanbietern (Internet Service *Providern*, ISP) und Internetknotenpunkten (Internet Exchange Points, IXP) berichtet. Es wurde befürchtet, dass es durch die gegen die Pandemie ergriffenen Maßnahmen zu einer Überlastung der Internetinfrastruktur kommen könnte. Das BSI hat die geänderten Anforderungen an die Internetinfrastruktur beobachtet und bewertet. Geändert hat sich nach Einschätzung des BSI neben Nutzungsarten und Nutzungszeiten auch das Verkehrsvolumen insgesamt. Die Steigerung im Verkehrsaufkommen ist an zahlreichen Internetknotenpunkten sichtbar. Dennoch liegt der Zuwachs im Rahmen der eingeplanten Kapazitäten. Ausfälle durch die gestiegene Last sind daher nicht zu befürchten. In Deutschland sind auch die Auswirkungen auf die größten Internetzugangsanbieter marginal. Die Latenzen sind nahezu unverändert, die Downloadraten teilweise sogar geringer. Insgesamt kommt das Internet – insbesondere in Deutschland – gut mit den gestiegenen Anforderungen zurecht. In ländlichen Regionen, in denen keine Breitbandanschlüsse verfügbar sind, gab es bereits vor COVID-19 Engpässe. Diese haben sich vermutlich durch den gestiegenen Bandbreitenbedarf verstärkt.

Gefahr von Cyber-Angriffen für die Bewältigung der Pandemie

Wie zuvor dargestellt, wirkt sich die COVID-19-Pandemie auf jeden Lebensbereich und jede Organisation aus. In dem komplexen Zusammenspiel aus Staat, Wirtschaft und Gesellschaft nimmt insbesondere die Digitalisierung eine zentrale Rolle ein, um sich an ebenjene veränderten Anforderungen in derartiger Kurzfristigkeit anpassen zu können. So nehmen digitale Prozesse und Lösungen auch einen entscheidenden Stellenwert in der Bewältigung der Pandemie ein.

Dies führt dazu, dass von Cyber-Angriffen eine besondere Gefahr für die Bewältigung der Pandemie ausgeht. In einer eng verzahnten Produktionswelt mit komplexen Lieferketten, in der durch die Pandemie jede noch so kleine Ressource ausschlaggebend geworden ist, kann schon ein einzelner Cyber-Angriff zu bedrohlichen Dominoeffekten führen, die es in jedem Fall zu vermeiden gilt. Das BSI appelliert daher, bei der Umsetzung von kurzfristigen Anpassungen digitaler Prozesse und Vorgehensweisen die IT-Sicherheit nicht hintanzustellen.

Ausblick

Das BSI beobachtet die IT-Sicherheitslage insbesondere unter Berücksichtigung der angeführten Umstände und Gefahren mit besonderer Aufmerksamkeit und steht im engen Austausch mit nationalen wie internationalen Partnern, um ein umfassendes Bild der Lage zu behalten und möglichst frühzeitig präventive Maßnahmen ergreifen zu können. Auf absehbare Zeit erwartet das BSI, dass sich die Ausnutzung des Themas der Pandemie in Cyber-Angriffen zum Beispiel für *Social Engineering* in *Phishing*- und *Spam*-Mails fortsetzen wird.

Cyber-Angriff gegen die Europäische Arzneimittelagentur EMA

Sachverhalt
Die Europäische Arzneimittelagentur (EMA), die für die Zulassung von Arzneimitteln in Europa zuständig ist, meldete am Mittwoch, dem 9. Dezember 2020, Ziel eines Cyber-Angriffs geworden zu sein. Dabei sind unter anderem Daten des Zulassungsantrags des COVID-19-Impfstoffs der Pharmaunternehmen BioNTech und Pfizer abgeflossen.

Ein Angreifer hatte sich zunächst Zugriff auf den Rechner des Mitarbeiters eines Dienstleisters der EMA verschafft. Darüber erlangte der Angreifer die Zugangsdaten für das Nutzerkonto dieses Mitarbeiters bei der EMA. Mit Hilfe dieses Nutzerkontos konnte er sich remote ins Netz der EMA und dort zum Dokumentenmanagementsystem verbinden. Der Angreifer suchte aktiv nach Dokumenten mit Bezug zur Impfstoffentwicklung und -verteilung.

Auswirkungen auf das Zulassungsverfahren für den COVID-19-Impfstoff der Unternehmen BioNTech und Pfizer hatte der Vorfall nicht.

Am 8. Januar 2021 wurde bekannt, dass Daten, die augenscheinlich aus dem Angriff auf die EMA stammten, in Internetforen veröffentlicht worden waren. Die veröffentlichten Informationen wurden derart arrangiert, dass davon ausgegangen werden muss, dass die Veröffentlichung Zweifel am Impfstoff hervorrufen sollte. Die geleakten Informationen wurden jedoch nicht breit im Internet geteilt.

Bewertung
Der Angriff zeigt, dass Informationen zu COVID-19-Impfstoffen für Angreifer interessant sind. Dabei schien die Motivation der Angreifer nicht nur im Bereich der Wirtschaftsspionage zu liegen. So wurden offenbar Teile der entwendeten Informationen auch genutzt, um das Vertrauen in den Impfstoff zu untergraben. Ob dies in wirtschaftlichen Interessen des Angreifers begründet war oder ein anderes Ziel verfolgt wurde, ist nicht bekannt. Welche Auswirkungen ein geringes Vertrauen in einen Impfstoff auf die Impfkampagne in Deutschland haben kann, zeigt sich an den Diskussionen zum Impfstoff von AstraZeneca.

Einmal mehr zeigt der Angriff die wachsende Bedeutung der Schwachstelle „Mensch“ als Einfallstor für Cyber-Angriffe. In diesem Fall wurde zwar schon eine Zwei-Faktor-*Authentisierung* für den Zugriff von Dienstleistern auf das System der EMA genutzt, jedoch hatte der Nutzer des angegriffenen Clients auf diesem beide Faktoren gespeichert, wodurch der Sicherheitseffekt unterlaufen wurde. Durch die Befolgung von grundlegenden IT-Sicherheitsmaßnahmen hätte der Angriff verhindert werden können bzw. wäre deutlich erschwert worden.

Reaktion
Das BSI hat umgehend Kontakt zu BioNTech bezüglich der geleakten Daten hergestellt, um die Bedrohungslage zu bewerten. Weiter wurden laufend alle dem BSI diesbezüglich zur Verfügung stehenden Informationen an Unternehmen und Organisationen in Deutschland weitergeleitet, die für die Entwicklung, Produktion und Distribution von COVID-19-Impfstoffen wichtig sind.

Seit Beginn der Pandemie arbeitet das BSI zusammen mit den Behörden des Nationalen Cyber-Abwehrzentrums an der Identifikation und dem Schutz von für die Bekämpfung der Pandemie relevanten Unternehmen und Organisationen vor Cyber-Angriffen und hat dazu auch eine Task Force eingerichtet.

Die Lage der IT-Sicherheit in Deutschland 2021 im Überblick

RANSOMWARE/DDOS

Deutliche Ausweitung cyber-krimineller Erpressungsmethoden

Neuer Trend

+ 360 % Daten-Leak-Seiten

Schweigegeld-Erpressung

Lösegeld-Erpressung

Schutzgeld-Erpressung

13 Tage lang konnte ein Universitätsklinikum nach einem *Ransomware*-Angriff keine Notfall-Patienten aufnehmen.

144 MIO. neue Schadprogramm-Varianten

+22 % gegenüber 2020: **117,4 MIO.**

DURCHSCHNITTLICH **394.000** neue **Schadprogramm-Varianten** pro Tag

2020: 322.000

IM HÖCHSTWERT **553.000**

2020: 470.000

DOPPELT SO VIELE

***BOT*-INFEKTIONEN DEUTSCHER SYSTEME**

pro Tag im Tagesspitzenwert

20.000 > 40.000

98 %

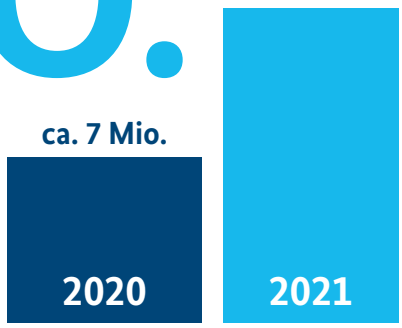
aller geprüften Systeme waren durch Schwachstellen in **MS Exchange** verwundbar.

14,8 MIO.

Meldungen zu Schadprogramm-Infektionen übermittelte das BSI an deutsche Netzbetreiber, mehr als

DOPPELT SO VIEL

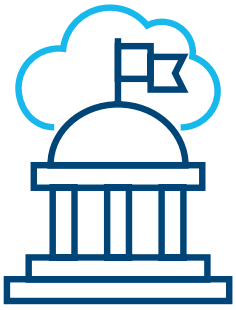
wie im Jahr zuvor.



44.000

Mails mit Schadprogrammen wurden im Durchschnitt pro Monat in deutschen Regierungsnetzen abgefangen.

2020 35.000



74.000

Webseiten wurden wegen enthaltener Schadprogramme durch die Webfilter der Regierungsnetze gesperrt.

2020 52.000

BSI unter **TOP 3 NATIONEN** weltweit bei Common-Criteria-Zertifikaten.

5.100

MITGLIEDER DER ALLIANZ FÜR CYBER-SICHERHEIT

- 2020: 4.400
- 2019: 3.700
- 2018: 2.700

< 10 %

waren nach Warnungen von BSI und Microsoft immer noch durch Schwachstellen in **MS Exchange** verwundbar.

Deutschland
Digital•Sicher•BSI•

Im Überblick

12 Monate Cyber-Sicherheit

Juni

- Vereinbarung zwischen BSI und Verbraucherschutzzentrale
- BSI bringt das Thema Cyber-Sicherheit in deutsche EU-Ratspräsidentschaft ein
- Vorstellung der Corona-Warn-*App*
- BSI und VDA: Gemeinsam für mehr Cyber-Sicherheit im Auto

August

- Argentinien: Ransomware-Angriff bei Einwanderungsbehörde mit Abfluss von Passdaten
- Neuseeland: Erpressungsversuch via *DDoS-Angriffen* auf die Börse NZX
- Erpressungsversuche via *DDoS*-Angriffen im Finanzsektor und auf Bezahldienstleister
- Sicherheitsanforderungen für Telekommunikationsnetze veröffentlicht
- Handlungsempfehlungen zur Migration zu Post-Quanten-Kryptografie aktualisiert

Oktober

- Cyber-Erpressung mit Sextortion-Kampagne
- BSI und Kraftfahrt-Bundesamt: Verwaltungsvereinbarung für Cyber-Sicherheit im Automotive-Bereich
- Veröffentlichung der Cyberfibel durch BSI und Deutschland sicher im Netz e. V.
- ECSM: Livestream-Reihe mit der Bundezentrale für politische Bildung zu Cyber-Sicherheit, Desinformation und *Deepfakes*
- BSI veröffentlicht „Leitfaden für Ihr virtuelles Event“
- BSI veröffentlicht Sicherheitsanforderungen für Online-Sozialwahlen

2020

Globale *DDoS*-Erpressungskampagne

Juli

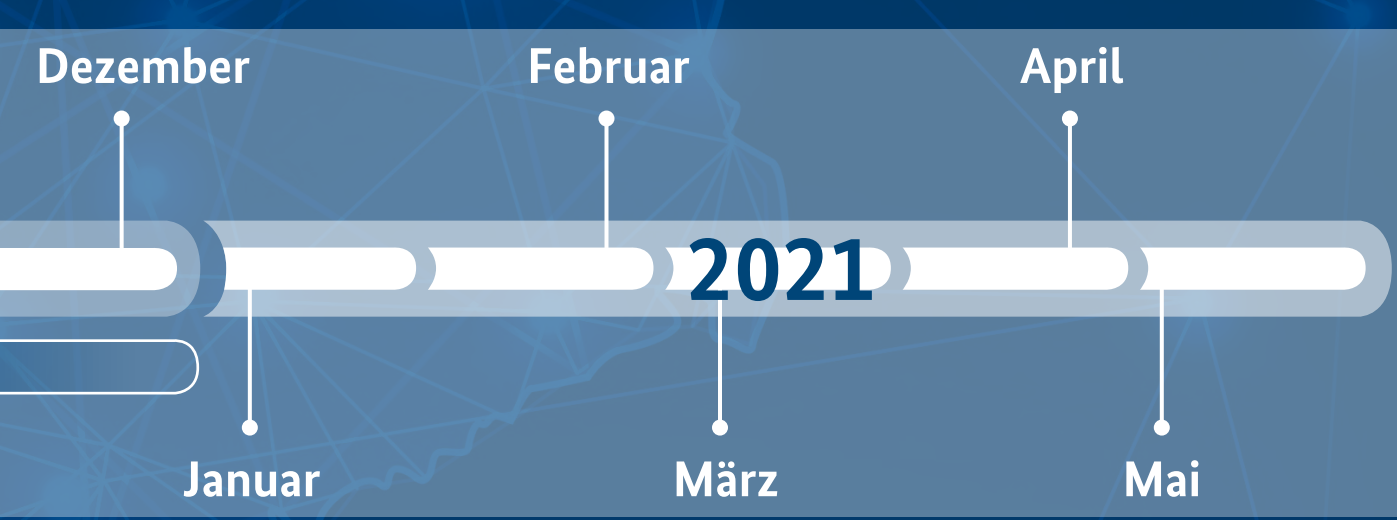
- BSI veröffentlicht Prüfspezifikationen für Breitband-Router
- BSI wirkt an europäischem Standard für vernetzte Geräte im Smart Home mit
- Nachweis von Sicherheitsmängeln in der Telematik-Infrastruktur durch Fehlkonfigurationen

September

- *Ransomware*-Angriff auf Universitätsklinikum in NRW
- EvilQuest: Schadsoftware, die sich gegen Apples Betriebssystem MacOS richtet
- *DDoS*-Erpressungen bei Internet-Service-*Providern* (auch Oktober)
- Erfolgreiches BSI-Team bei der Krypto-Konferenz CHES-Challenge
- BSI und EASA für mehr Cyber-Sicherheit in der Luftfahrt
- BSI und ProPK veröffentlichen Digitalbarometer 2020
- Start des BSI-Podcasts „Update verfügbar“

November

- *Ransomware*-Angriff auf Flughafen Saarbrücken
- Offizielle Cyber-Sicherheitskonferenz der deutschen EU-Ratspräsidentschaft durch BMI und BSI
- Symposium „Digitalisierung, Cyber-Sicherheit & Ich-Perspektiven im Gesundheitswesen“ am Universitätsklinikum Bonn
- Kooperationsvereinbarung zwischen BSI und Fraunhofer IAIS zur gemeinsamen Entwicklung von Prüfverfahren



- Cyber-Angriff auf Europäische Arzneimittelagentur EMA
- *Ransomware*-Angriff auf große deutsche Mediengruppe
- USA: APT-Angriff auf Monitoring-Anbieter SolarWinds
- Beschluss der Informations-sicherheitsrichtlinie IT-Konsolidierung Bund
- Informationssicherheits-beauftragter für die IT-Konsolidierung Bund ernannt
- Erste Version der Normungs-roadmap Künstliche Intelligenz auf Digital Gipfel vorgestellt

- Höchster jemals gemessener durchschnittl. Tageszuwachs an neuen Schadprogramm-Varianten: 553.000
- „Smishing“ SMS-*Phishing*-Nachrichten mittels Android-Schadprogramm MoqHao
- BSI veranstaltet 17. Deutschen IT-Sicherheitskongress erstmalig digital
- Veröffentlichung des Kriterienkatalogs für KI-basierte *Cloud*-Dienste (AIC4)

- Verabschiedung des IT-Sicherheitsgesetzes 2.0
- *Deepfake*-Manipulation: Erfolgreiche Täuschung mehrerer europ. Politiker
- EU-Kommission und 18 weitere Staaten: Erfolgreiche Einbindung der Online-Ausweisfunktion in eID-Schema
- Start des Projekts eMergent zur Digitalisierung im Rettungsdienst
- Allianz für Cyber-Sicherheit knackt die 5.000-Teilnehmer-Marke
- Vorstellung der Ergebnisse der BSI-Wirtschaftsumfrage zum Homeoffice

- Infrastruktur der Schadsoftware Emotet zerschlagen
- Cyber-Erpressung mit Sextortion-Kampagne
- Bundeskartellamt und BSI: Gemeinsam für digitalen Verbraucherschutz
- Draft des neuen BSI-Standards 200-4 zum Business Continuity Management veröffentlicht

- Sicherheitsupdate für Schwachstellen auf Exchange-Servern von Microsoft
- Cyber-Erpressung mit Sextortion-Kampagne
- BSI veröffentlicht „Mindeststandard für Videokonferenzdienste“
- Start der BMI-BSI-Kampagne #einfachaBSIchern

- USA: Cyber-Angriff (Darkside) auf IT-Infrastruktur des Pipeline-Betreibers Colonial Pipeline Company
- Belgien: *DDoS*-Angriff auf einen großen Internet-*Provider*
- Cyber-Erpressung mit Sextortion-Kampagne
- *UP KRITIS*: 750 Organisationen sind Teilnehmer der Plattform
- IT-SiG 2.0 tritt in Kraft

2 Zielgruppenspezifische Erkenntnisse und Maßnahmen

2 Zielgruppenspezifische Erkenntnisse und Maßnahmen

Das BSI ist die Cyber-Sicherheitsbehörde des Bundes und gestaltet die sichere Digitalisierung in Deutschland – gemeinsam mit den Bürgerinnen und Bürgern unseres Landes, der Wirtschaft sowie mit Staat und Verwaltung und internationalen Institutionen. Seit seiner Gründung 1991 hat sich das BSI zu einem nationalen Kompetenzzentrum für alle Fragen der Informationssicherheit entwickelt. Mit dem IT-Sicherheitsgesetz 2.0 wurde der Auftrag des BSI 2021 erweitert, um den Herausforderungen der fortschreitenden Digitalisierung zu begegnen, unter anderem mit der Verankerung des digitalen Verbraucherschutzes im BSI. Damit unterstützt das BSI Verbraucherinnen und Verbraucher in der Risikobewertung von Technologien, Produkten, Dienstleistungen und Medienangeboten.

2.1 Gesellschaft

Für die Zukunft des Standorts Deutschland ist die Digitalisierung ein wesentlicher Erfolgsfaktor. Unverzichtbare Voraussetzung dafür ist die Informationssicherheit. Das BSI arbeitet intensiv daran, die Informationssicherheit in allen Bereichen des Lebens zu verbessern, damit die Bürgerinnen und Bürger ihre persönlichen Daten gut aufgehoben wissen, IT sicher anwenden und sich vertrauensvoll in unserer vernetzten Welt bewegen können. Dafür bündelt das BSI umfangreiches Know-how in den Bereichen Prävention, Detektion und Reaktion und leitet daraus konkrete Informationsangebote für gesellschaftliche Gruppen, aber auch für die einzelne Bürgerin und den einzelnen Bürger ab.

2.1.1 Erkenntnisse zur Gefährdungslage in der Gesellschaft

Das BSI und das Programm Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) kooperieren, um Verbraucherinnen und Verbraucher umfassend über Schutzmöglichkeiten und die Risiken im Internet aufzuklären. Grundlage dieser Arbeit ist das Digitalbarometer, eine gemeinsame, repräsentative Online-Befragung, die seit 2019 in jedem Frühjahr durchgeführt wird. In dieser wird erhoben, welche Bedeutung Sicherheit im Internet für Verbraucherinnen und Verbraucher hat, inwiefern sie sich vor den Gefahren der digitalen Welt schützen und wie sie sich über Schwachstellen, Risiken und Schutzmaßnahmen informieren.

Jeder Vierte war bereits Opfer

Für den Berichtszeitraum bleibt die generelle Betroffenheit bei Bürgerinnen und Bürgern wie auch in den vergangenen beiden Jahren konstant: Jeder Vierte gab an, bereits Opfer von Kriminalität im Internet gewesen zu sein (24 %). Dabei sind den Befragten vor allem ein Fremdzugriff auf mindestens einen ihrer Online-Accounts (31 %) oder eine Infektion mit Schadsoftware (29 %) widerfahren. *Phishing*, also das Ausspionieren von Zugangs- oder Kontoinformationen, betraf ein Viertel (25 %) der Opfer. Gaben 2020 noch 40 Prozent der Opfer von Kriminalität im Internet an, von Betrug bei Onlineshopping betroffen gewesen zu sein, waren es 2021 nur noch 19 Prozent. Zudem berichtete ein Zehntel der Befragten (10 %), *Phishing*-Mails mit Bezug zur COVID-19-Pandemie erhalten zu haben.

Die bewusste Anwendung von Schutzmaßnahmen durch Verbraucherinnen und Verbraucher bleibt weiterhin ausbaufähig. Zwar ist beispielsweise die Nutzung von Antivirenprogrammen (62 %), sicheren Passwörtern (60 %) und einer aktuellen Firewall (53 %) verbreitet, diese werden aber längst nicht umfassend eingesetzt. Gab 2020 nur ein Viertel der Befragten an, automatische Updates zu nutzen, sind es 2021 rund ein Drittel (32 %). Ähnlich verhält es sich bei der Aktivierung einer Zwei-Faktor-*Authentisierung*: Diese nahm 2020 ein Drittel der Befragten (33 %) vor, 2021 ist der Anteil auf 40 % leicht gestiegen.

Umgang mit Sicherheitsempfehlungen

Rund zwei Drittel der Befragten (67 %) kennen Sicherheitsempfehlungen zum Schutz vor Kriminalität im Internet (65 %). 37 Prozent der Befragten setzen solche Sicherheitsempfehlungen zum Teil um, gut jeder Zehnte vollständig (12 %). Wer Sicherheitsempfehlungen kennt, aber nicht umsetzt (12 %), begründet dies entweder durch den zu hohen Aufwand oder dadurch, dass die Empfehlungen zu kompliziert seien und nicht verstanden würden.

Der größte Teil der Befragten informiert sich hin und wieder über Internetsicherheit (40 %), gut ein Fünftel nie (22 %). Besonders wichtig ist den Befragten die Sicherheit beim Onlinebanking (88 %) und Onlineshopping (67 %), aber auch bei der Anwendung von *Cloud*-Diensten (66 %). Knapp ein Drittel der Befragten kennt die Informationen des BSI zum Schutz vor Kriminalität im Internet, der größte Teil hiervon (43 %) ist eher zufällig auf diese Informationen gestoßen.

Wunsch nach Orientierung für den Notfall

Die Opfer von Kriminalität im Internet gaben meist an, sich selbst geholfen zu haben. Das entspricht auch ihrem Bedarf nach Informationen: Die meisten Betroffenen wünschen sich eine Checkliste als Hilfestellung für den Notfall, gefolgt von einer Webseite mit Erklärvideos und einer Beraterin oder einem Berater bei der Polizei. Auch insgesamt betrachtet äußerte über die Hälfte der Befragten den Wunsch nach mehr Informationen zu Themen rund um die Sicherheit im Internet, insbesondere Hinweise, wie sie Kriminalität im Internet erkennen können (57 % von diesen) und wie sich sensible Daten schützen lassen (48 % von diesen). Empfehlungen, welche Software zum Schutz geeignet ist, und was Opfer von Onlinekriminalität tun können, sind ebenfalls gefragt (jeweils 48 % von diesen).

2.1.2 Digitaler Verbraucherschutz

Der Trend, sich mit Hilfe von Gesundheits-*Apps* zu informieren, Körperwerte zu analysieren oder sich persönlich zu motivieren, ist, nicht nur bedingt durch die COVID-19-Pandemie, ungebrochen. Die Schutzbedürftigkeit sensibler Daten gerade im Gesundheitsbereich sorgt jedoch für hohe Anforderungen an die IT-Sicherheit solcher Anwendungen. Das BSI hat im Dezember 2020 und Januar 2021 ausgewählte Android- und iOS-*Apps* im Gesundheitsbereich untersucht, die kein Medizinprodukt sind bzw. nicht im Verzeichnis der Digitalen Gesundheitsanwendungen (DiGA) gelistet werden. Analysiert wurden Anwendungen aus den Bereichen Krankheitsmanagement, Fitness, Ernährung sowie Entspannung und Achtsamkeit.

Das betrachtete Marktsegment ist von einer hohen Wachstumsdynamik sowie schnellen technologischen Weiterentwicklungen und Erweiterungen geprägt. Aber noch wichtiger: Die Ergebnisse der Studie zeigen, dass bei der IT-Sicherheit der *Apps* großer Nachholbedarf besteht.

Bei den 84 betrachteten Anbietern wurde festgestellt, dass der Grundsatz *Security by Design* nur in Teilen des Entwicklungsprozesses berücksichtigt wurde. Fehlende Prozesse für Updates und den Umgang mit bekannt gewordenen Schwachstellen gingen einher mit der unzureichenden Umsetzung technischer und organisatorischer Maßnahmen. Spezifische Testfelder in der IT-sicherheitstechnischen Untersuchung (siehe *Abildung 6*) von sieben ausgewählten *Apps* zeigten weitere Risiken, darunter die Übertragung von Passwörtern im Klartext (siehe Kapitel *Diebstahl und Missbrauch von Identitätsdaten*, Seite 24) oder der unzureichende Schutz vor dem Abfangen, Auslesen und Manipulieren von Kommunikationsinhalten zwischen *App* und dem *Cloud*-Backend des Anbieters.

Um Verbraucherinnen und Verbraucher im Markt für Gesundheits-*Apps* besser zu schützen, besteht neben der Sensibilisierung für mögliche Risiken vor allem auf Anbieterseite erheblicher Handlungsbedarf, mit geeigneten Maßnahmen die IT-Sicherheit der *Apps* zu erhöhen. Die vollständige Analyse sowie detaillierte Ergebnisse der Studie „IT-Sicherheit auf dem digitalen Verbrauchermarkt: Fokus Gesundheits-*Apps*“ unter:[m]

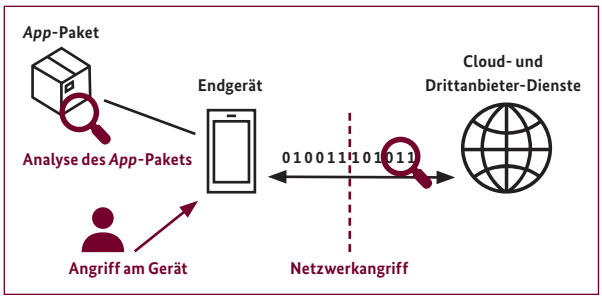


Abbildung 6: Testfelder der IT-sicherheitstechnischen Untersuchung

2.1.3 Das IT-Sicherheitskennzeichen

Mit dem 2021 in Kraft getretenen IT-Sicherheitsgesetz 2.0 haben Bundestag und Bundesrat den Weg für das IT-Sicherheitskennzeichen in Deutschland geebnet. Das Kennzeichen soll dazu dienen, IT-Sicherheitseigenschaften von Verbraucherprodukten transparent zu machen. So soll die IT-Sicherheit als verbraucherrelevantes Merkmal auf Produkten etabliert werden.

Fachleute des BSI haben die international anerkannte Technische Richtlinie (TR) für Breitbandrouter entwickelt und die auf europäischer Ebene Standards setzende Norm für vernetzte Consumer *IoT*-Geräte ETSI EN 303 645 auf den Weg gebracht (vgl. Kapitel *Sicherheit im Internet der Dinge, Smart Home und Smart Cities*, Seite 50).

Im Herbst 2021 wird das BSI diese TR durch das Marktprodukt IT-Sicherheitskennzeichen ergänzen. Zunächst wird es für Router vergeben, später soll das IT-Sicherheitskennzeichen auf weitere Produkte aus dem Feld der Consumer-*IoT* ausgeweitet werden.

Mit seinem Antrag, das IT-Sicherheitskennzeichen führen zu dürfen, bestätigt der Hersteller dem BSI offiziell und formal, dass er die vom BSI festgelegten technischen Standards für das Produkt einhält. Das BSI prüft dann diese Herstellererklärung anhand der eingereichten Unterlagen auf Vollständigkeit und Plausibilität. Eine produktspezifische (technische) Prüfung, wie z. B. bei der Zertifizierung nach Technischen Richtlinien, erfolgt für das IT-Sicherheitskennzeichen im Rahmen der Antragsstellung nicht.

Hat der Hersteller das Antragsverfahren erfolgreich durchlaufen, kann er das IT-Sicherheitskennzeichen auf seine Produktverpackung aufbringen. Über einen QR-Code oder Kurzlink findet die Verbraucherin bzw. der Verbraucher dann schnell und einfach alle aktuellen produktspezifischen Sicherheitsinformationen, z. B. wie lange dieses Produkt vom Hersteller mit Updates versorgt wird oder ob Sicherheitslücken bekannt geworden sind.

Nach Vergabe des IT-Sicherheitskennzeichens unterliegt das gekennzeichnete Produkt dann einer Marktaufsicht durch das BSI, d. h. werden Sicherheitslücken zu dem Produkt bekannt, informiert das BSI u. a. auf der jeweiligen Produktseite darüber.

Mit der Unterstützung von Unternehmen, die Verbraucherschutz und Informationssicherheit als wichtiges Kriterium ihres eigenen Handelns begreifen, wird das IT-Sicherheitskennzeichen die Produktlandschaft auf dem IT-Konsumentenmarkt insgesamt sicherer und übersichtlicher machen. Perspektivisch strebt das BSI an, das IT-Sicherheitskennzeichen in einer verbindlichen, europäischen Kennzeichnung aufgehen zu lassen.

2.1.4 Information und Sensibilisierung von Verbraucherinnen und Verbrauchern

Regelmäßig informiert das BSI Verbraucherinnen und Verbraucher zu aktuellen Neuigkeiten sowie zu Themen des Basisschutzes, weist auf Gefahren hin und gibt alltagstaugliche Empfehlungen rund um die IT-Sicherheit, damit sich jeder und jede Einzelne sicher und selbstbestimmt im Netz bewegen kann.

Zu Beginn des Berichtszeitraums, im Sommer 2020, lag ein besonderes Augenmerk auf der Fragestellung, wie in Zeiten der COVID-19-Pandemie und dem dadurch bedingten Wegfall persönlicher Treffen eine digitale Teilhabe sicher ermöglicht werden kann. Dazu bot das BSI auf seiner Webseite Artikel für die Gestaltung eines sicheren digitalen Alltags an, beispielsweise durch Videokonferenzen oder andere digitale Kommunikationsformate. Der im Oktober 2020 entwickelte Leitfaden für virtuelle Events bietet zudem gezielt Vereinen und Menschen im Ehrenamt eine Orientierung zu Fragen der Cyber-Sicherheit.

Ab Herbst 2020 entstand in Kooperation mit der Bundeszentrale für politische Bildung anlässlich des European Cybersecurity Month eine dreiteilige Livestream-Reihe. Expertinnen und Experten sprachen über Cyber-Sicherheit, Desinformation und *Deepfakes*. Interessierte konnten so – auch vor dem Hintergrund der Präsidentschaftswahl in den USA – mehr zum Thema „Wahrheit und Relevanz im digitalen Raum“ erfahren.

Cyber-Sicherheit

Das BSI konzentriert sich mit seinen Angeboten für Verbraucherinnen und Verbraucher immer auf die aktuellen Bedürfnisse und Fragen der Menschen. So informieren zahlreiche kontinuierliche Angebote regelmäßig über den Basisschutz von Hard- und Software. Denn laut dem Digitalbarometer (siehe Kapitel *Erkenntnisse zur Gefährdungslage in der Gesellschaft*, Seite 47) werden wichtige Maßnahmen des Basisschutzes immer noch nicht flächendeckend von allen Internetnutzerinnen und -nutzern umgesetzt. Das führt dazu, dass jede oder jeder Vierte bereits eine Straftat im Internet erlebt hat.

- Die Webseite bsi-fuer-buerger.de ist seit Februar 2021 in den neuen Verbraucherbereich der BSI-Webseite bsi.bund.de/VerbraucherInnen integriert:[n)]
  Dort finden Interessierte einen umfangreichen Überblick zu allen wichtigen Themen der Cyber-Sicherheit und erhalten Empfehlungen für den digitalen Alltag.

- Der kostenlose Warn- und Informationsdienst *Bürger-CERT* umfasst die Technischen Warnungen und den vierzehntägigen Newsletter „Sicher ° Informiert“. Mit seiner Hilfe macht das BSI Schwachstellen und aktuelle Vorfälle bekannt und gibt Tipps zur Abhilfe. Derzeit nutzen rund 112.000 Abonnentinnen und Abonnenten dieses Angebot.

- Über die bürgernahen Social Media-Plattformen auf Facebook (rund 43.700 Abonnierende) und YouTube (aktuell etwa 3.000 Abonnierende) gibt das BSI regelmäßig aktuelle Hinweise und Empfehlungen. Die Erklär- und Animationsvideos auf YouTube wurden im Berichtszeitraum etwa 700 Stunden lang angeschaut. Besonders erfolgreich waren Themen wie Sicherheitsupdates, Informationen zu kritischen Schwachstellen oder der Video-Podcast „Update verfügbar“.

- Ein Service-Center steht telefonisch unter 0800-2741000 für Anwenderfragen zu Themen der IT- und Internetsicherheit zur Verfügung.

- Fünf Broschüren, die erklären, wie Verbraucherinnen und Verbraucher das Internet, Smartphone, Tablet und Co, soziale Netzwerke, *Cloud*-Dienste und das *Internet der Dinge* sicher nutzen können, wurden im April 2021 inhaltlich und grafisch neu gestaltet. Sie stehen auf der Webseite zum Download zur Verfügung oder können dort kostenfrei als gedrucktes Exemplar bestellt werden.

- Im Oktober 2020 ist die Cyberfibel erschienen. Es handelt sich um ein Nachschlagewerk für Menschen in der Verbraucherberatung oder -aufklärung. Die Fibel fasst Informationen zu digitalen Lebenswelten und Empfehlungen zu grundlegenden Kompetenzen im Bereich der IT-Sicherheit zusammen und dient als Grundlage für Seminare oder Beratungsgespräche. Das Produkt ist im Rahmen einer Kooperation mit Deutschland sicher im Netz (DsiN) entstanden.
- Seit September 2020 erscheint der BSI-Podcast „Update verfügbar“ am Ende jedes Monats auf den wichtigsten Plattformen, um aktuelle Vorfälle bürgernah und aus Sicht der Verbraucherinnen und Verbraucher zu besprechen. Hier ging es unter anderem um *Deepfakes*, Sicherheit im Gesundheitswesen, Sicherheit beim Homeschooling und Account-Schutz.

KIS-IT-Kampagne

Am 22. März 2021 starteten BMI und BSI ihre gemeinsame Sensibilisierungs- und Informationskampagne zur IT-Sicherheit für Verbraucherinnen und Verbraucher #einfachaBSIchern. Ziel ist es, das Bewusstsein von Verbraucherinnen und Verbrauchern für Gefahren im Netz zu erhöhen und ihre Handlungskompetenz zu stärken. Auf einfachaBSIchern.de erfahren Interessierte mehr zu Themen wie sichere E-Mail-Kommunikation, Schutz des Smart Homes oder sicheres Onlineshopping:[o)]

2.1.5 Sicherheit im Internet der Dinge, Smart Home und Smart Cities

Vernetzte Geräte aus dem *Internet der Dinge (Internet of Things; IoT)* nehmen bei der Gestaltung der digitalen Zukunft sowohl für Industrie und Unternehmen als auch für Verbraucherinnen und Verbraucher eine immer bedeutendere Rolle ein. So steigt die Anzahl der Haushalte deutlich, die mit smarten *IoT*-Produkten ausgestattet sind. Nach dem aktuellen Digital Market Outlook von Statista (vgl. *Quellenverzeichnis*[53]) wird voraussichtlich die Zahl der smarten Haushalte in Europa bereits im kommenden Jahr die Grenze von 60 Millionen übersteigen. Da *IoT*-Komponenten auch Risiken für die Privatsphäre sowie die Informations- und Cyber-Sicherheit mit sich bringen, steigt auch die entsprechende Gefährdungslage. Begleitet wird dieser Trend unter anderem durch einen Anstieg der Schadprogramm-Varianten (siehe Kapitel *Neue Schadprogramm-Varianten*, Seite 11).

Um dem Anteil von Produkten entgegenzuwirken, die durch Schwachstellen belastet und dadurch angreifbar sind (siehe Kapitel *Botnetze*, Seite 19), sieht das BSI dringenden Handlungsbedarf. Dieser besteht insbesondere in der Prävention etwa durch neue Standards.

In diesem Kontext rückt die Cyber-Sicherheit vernetzter Geräte im Berichtszeitraum stärker in den Fokus europäischer Initiativen. So ist das Thema Gegenstand mehrerer Schlussfolgerungen des Rates der Europäischen Union, insbesondere unter der deutschen EU-Ratspräsidentschaft im zweiten Halbjahr 2020.

> *„Der Rat der Europäischen Union [...] stellt fest, dass die zunehmende Nutzung von Konsumgütern und industriellen Geräten, die mit dem Internet verbunden sind, auch neue Risiken für die Privatsphäre und die Informations- und Cyber-Sicherheit birgt [...]. Cyber-Sicherheit und Privatsphäre sollten als wesentliche Anforderungen im Rahmen der Produktinnovation, der Produktions- und Entwicklungsprozesse, einschließlich der Entwurfsphase (eingebaute Sicherheit - Security by Design), anerkannt und während des gesamten Lebenszyklus eines Produkts und über seine gesamte Lieferkette hinweg sichergestellt werden. [...] [Der Rat] erkennt an, dass die Zertifizierung vernetzter Geräte einschlägige Normen, Standards oder technische Spezifikationen für Cyber-Sicherheitsbewertungen im Rahmen des Rechtsakts zur Cyber-Sicherheit erfordern würde [...] und empfiehlt, die Bemühungen der europäischen Normungsorganisationen in diesem Bereich zu verstärken; [dabei] nimmt [dieser] gleichzeitig die Cyber-Sicherheitsnorm ETSI EN 303 645 für IoT-Geräte für Verbraucher als wichtigen Schritt in diese Richtung zur Kenntnis.“*

Ein europäischer Ansatz zur Stärkung der Cyber-Sicherheit hat den Vorteil, dass das Sicherheitsniveau von *IoT*-Produkten im gesamten europäischen Binnenmarkt im Einklang mit europäischen Werten erhöht werden kann, um so einen wertvollen Beitrag für eine globale Herausforderung zu leisten.

In diesem Sinne schafft das Engagement des BSI bei der Erstellung von ETSI EN 303 645 und der dazugehörigen Prüfspezifikation ETSI TS 103 701 (Fertigstellung im zweiten Halbjahr 2021 erwartet*) wichtige Voraussetzungen zur Etablierung europäischer Zertifizierungsschemata und zur Erhöhung der Cyber-Sicherheit in Europa.

Das *Internet der Dinge* ist nicht nur auf den Bereich des Consumer *IoT* beschränkt, sondern umfasst ebenso den Bereich des Public *IoT*. Dieser spielt bei der Digitalisierung, insbesondere der kommunalen Daseinsvorsorge (Smart City), eine entscheidende Rolle. Der dramatische Anstieg von Schadprogramm-Varianten und infizierten Geräten wirkt sich auch auf diesen Bereich aus.

Bei diesen digitalen Transformationsprozessen existieren im Hinblick auf den Verbraucher-Bereich vergleichbare technologische Grundherausforderungen. Allerdings haben Kommunen im Rahmen der Daseinsvorsorge eine Verantwortung gegenüber ihren Bürgerinnen und Bürgern und sind daher bestrebt, eine Gefährdung des Gemeinwohls zu vermeiden. Dies drückt sich im Fall der Cyber-Sicherheit in der Etablierung eines angemessenen Sicherheitsniveaus digitaler Infrastrukturen aus. Hierzu benötigen sowohl Kommunen als auch beteiligte Unternehmen Handlungsempfehlungen und Standards, um sichere *IoT*-Infrastrukturen unter Berücksichtigung der vorliegenden Risiken betreiben zu können. Das BSI unterstützt durch einen engen Austausch mit aktiven Kommunen die Gestaltung und Umsetzung der IT-Sicherheit.

2.1.6 Sicherheit von Medizinprodukten

Angriffe auf Institutionen des Gesundheitswesens (vgl. Vorfall *Ransomware-Angriff auf ein Universitätsklinikum in Nordrhein-Westfalen*, S. 15) und Schwachstellen in Gesundheitsanwendungen, können weitreichende Folgen mit sich bringen bis hin zur Gefahr für die Gesundheit von Patientinnen und Patienten. Das Projekt „ManiMed – Manipulation von Medizinprodukten“ startete Anfang 2019 und wurde im Dezember 2020 beendet. Es hat den Anspruch, die Cyber-Sicherheitslage von aktuell auf dem deutschen Markt verfügbaren vernetzten Medizinprodukten durch tiefgehende IT-sicherheitstechnische Untersuchungen möglichst realistisch abzubilden. Insgesamt wurden dabei mehr als 150 Schwachstellen in zehn Produkten aus fünf Kategorien (implantierbare Herzschrittmacher, Defibrillatoren und deren Zubehör, Insulinpumpen, Beatmungsgeräte, Patientenmonitore und Infusionspumpen) sowie der jeweils zugehörigen Infrastruktur gefunden.

Die meisten Schwachstellen betrafen das Zubehör, beziehungsweise die Infrastrukturkomponenten, nicht das Medizinprodukt selbst. Das zeigt, dass statt einer Betrachtung der Einzelkomponenten eine Gesamtsicht auf das Medizinprodukte-Ökosystem notwendig ist. Zudem sind Schwachstellen generell abhängig von der spezifischen Betriebsumgebung eines Produkts. Ein Hersteller muss bei Schwachstellen abwägen und priorisieren, ob und in welcher Form eine Behebung der Sicherheitslücken möglich, notwendig und wirtschaftlich ist. Die gefundenen Schwachstellen wurden den jeweiligen Herstellern im Rahmen des Projekts kommuniziert.

Konfigurationsfehler umfassen beispielsweise die Preisgabe von Informationen, wie Software-Versionsnummern oder die Nutzung von Standardkonten zur *Authentisierung*. Oft waren die identifizierten Schwachstellen mit veralteter Software verbunden. In den meisten Fällen lassen sich diese Arten von Schwachstellen leicht beheben. Problematisch ist allerdings, dass die Behebung zwar angemessen und schnell erfolgen kann, oft jedoch grundsätzliche Sicherheitsmechanismen oder Konfigurationskonzepte fehlen.

Die große Anzahl der identifizierten Schwachstellen bestätigt bisherige Forschungen und zeigt deutlich, dass Verbesserungsbedarf hinsichtlich der IT-Sicherheit in Medizinprodukten besteht. Zukünftig sollte die IT-Sicherheit von Anfang an in der Entwicklung beachtet werden. Darüber hinaus sollte die IT-Sicherheit von komplexen Ökosystemen als Gesamtsystem durch tiefgehende Untersuchungen auch regelmäßig überprüft werden.

Das Projekt ManiMed hat einen Gesamtüberblick über die Sicherheit in vernetzten Medizinprodukten verschafft. In Anschlussprojekten soll ein detaillierter Einblick in weitere Teilbereiche erfolgen, die im Projekt ManiMed nur oberflächlich evaluiert werden konnten.

Als Spezialisierung auf eine gesonderte Anwendungsumgebung wurde zum 12. April 2021 das Projekt eMergent gestartet, um die Digitalisierung im Rettungsdienst zu analysieren. Hier liegt der Fokus auf bodengebundenen, mobilen Medizinprodukten und Dokumentationssystemen, die nicht auf eine geschützte Infrastruktur zugreifen können. Sie unterliegen daher Anforderungen wie ein robustes Design, die Bedienbarkeit durch Personal mit geringen IT-Kenntnissen und hohe Verfügbarkeit. Das Projekt eMergent soll ein Lagebild über ein noch wenig untersuchtes Gebiet der Digitalisierung im Gesundheitswesen schaffen und Chancen sowie Herausforderungen erkennen, bei denen das BSI zur Stärkung der IT-Sicherheit beitragen kann.

* Bis zur Veröffentlichung von ETSI TS 103 701 sind unter *http://docbox.etsi.org/CYBER/CYBER/Open/Latest_Drafts* Entwürfe öffentlich verfügbar.

2.1.7 Corona-Warn-App

Die Corona-Warn-*App* (CWA) ist ein wichtiger Baustein in der digitalen Pandemiebekämpfung. Seit Beginn der Arbeiten an der *App* führt das BSI Sicherheitsanalysen durch. Das BSI unterstützt die Weiterentwicklung der *App* laufend durch Penetrationstests und Code Reviews, die sieben Tage dauern und in zweiwöchigem Rhythmus stattfinden. Die Entwicklung der Anwendung findet transparent in einem öffentlich zugänglichen Quellcode-Verwaltungssystem auf Github statt. Dort meldet das BSI, ebenfalls transparent, die identifizierten Schwachstellen an die Entwickler. Seit der Veröffentlichung der CWA gab es in enger Abstimmung zwischen BSI, RKI, Deutscher Telekom und SAP zahlreiche Erweiterungen, inklusive eines Kontakttagebuchs und einer Eventregistrierung. Außerdem wurde die *App* an das europäische Gesamtsystem sowie das System der Schweiz angepasst.

Die Erweiterungen erhöhen den Funktionsumfang der CWA und beheben identifizierte Schwachstellen, durch die Aktivitäten des BSI konnten innerhalb eines Jahres über 70 Schwachstellen identifiziert werden.

2.1.8 eHealth und Telematik-Infrastruktur

Die Digitalisierung des Gesundheitswesens hat von 2020 bis heute stark zugenommen, insbesondere bei Anwendungen der Telematik-Infrastruktur (TI). So waren die vergangenen Monate vor allem durch den Start der elektronischen Patientenakte (ePA), des Frontends des Versicherten (FdV) sowie vom Notfalldatenmanagement (NFDM) und der Arzneimitteltherapiesicherheit (AMTS) geprägt. Zugleich gab es Fortschritte beim sogenannten E-Rezept, dem Zusammenspiel von Telematik-Infrastruktur mit digitalen Gesundheits- und Pflege-*Apps* sowie bei Implantaten und dem europaweiten Zusammenspiel in der Notfallversorgung. Die Aufnahme zusätzlicher Leistungserbringer wie Pflegepersonal oder Hebammen steht bevor.

Diese Fülle neuer Anwendungsfälle erfordert eine Neugestaltung der Telematik-Infrastruktur, die sich vor allem im aktuellen Entwurf zum Gesetz zur digitalen Modernisierung von Versorgung und Pflege (DVPMG) sowie in den Planungen der gematik zur Telematik Infrastruktur 2.0 wiederfinden. Bei all diesen Entwicklungen steht das BSI Gesellschaft, Staat und Wirtschaft in sicherheitstechnischen Fragen mit Beratung, Prüfung und Nachweis der Sicherheit sowie mit der Vertretung der Interessen zur Verfügung. So umfasst das aktuelle Release 4.0.2 im Fachportal der gematik 93 Spezifikationen, 15 Konzepte und 95 Steckbriefe, die in Begleitung des BSI entstanden sind.

Im Nachweis der Sicherheit von Anwendungen der Telematik-Infrastruktur ist ein Umdenken erforderlich: Die auf den Konnektor auch heute noch angewendeten Zertifizierungsverfahren (wie die aktuellen Produkttypversion-4-Zertifizierungen) lassen sich auf Smartphone-Anwendungen, wie das Frontend der Versicherten, nur eingeschränkt anwenden. Durch eine Vielzahl an Betriebssystemversionen und eng getaktete Updates sowohl der *Apps* als auch der Betriebssysteme stehen die etablierten Prüfmechanismen vor großen Hürden. Darauf hat das BSI durch die „Prüfvorschrift Frontend des Versicherten - elektronische Patientenakte“ (vgl. *Quellenverzeichnis*[54]) reagiert, indem ein maßgeschneidertes alternatives Prüfverfahren definiert wurde.

Der ursprüngliche Sicherheitsansatz der Telematik-Infrastruktur basiert im Wesentlichen auf einem sicheren Netz, in dem Leistungserbringer ohne zusätzlichen Internetzugang durch mit einem *VPN* vergleichbaren Konnektor an die Telematik-Infrastruktur angeschlossen und so innerhalb dieser sicheren Umgebung vor äußerer, unberechtigter Einflussnahme geschützt werden. Trotz dieses hohen Sicherheitsniveaus gab es potentielle oder tatsächliche Schwachstellen:

- Die Telematik-Infrastruktur bietet mehrere Wege der Anbindungen an (vgl. *Quellenverzeichnis*[55]). Viele Leistungserbringer nutzen nicht den von der gematik empfohlenen Reihenbetrieb, in dem das Netz des Leistungserbringers direkt an den zertifizierten Konnektor angeschlossen ist und der einen hohen Schutz durch integrierte Sicherheitsfunktionen, etwa durch eine Firewall, bietet. Stattdessen wird häufig der Parallelbetrieb verwendet, in dem der Konnektor wie andere Geräte der Praxis-IT an einen Router angeschlossen ist, der direkt mit dem Internet verbunden ist. Dieser Betrieb ist für große IT-Dienstleister mit eigenen Schutzmechanismen vorgesehen und bietet keinen integrierten Schutz vor Angriffen aus dem Internet.

- Eng verwandt damit waren Sicherheitsmängel durch Fehlkonfigurationen, die Sicherheitsforscher im Juli 2020 sowie auf dem Chaos Communication Congress im Dezember 2020 vorstellten. Dabei konnte über das Internet auf eine Admin-Schnittstelle einiger Konnektoren zugegriffen werden.

- Mitte 2020 kam es durch einen Konfigurationsfehler zu Störungen im Versichertenstammdatenmanagement (VSDM) einiger Konnektoren diverser Hersteller (vgl. *Quellenverzeichnis*[56]). VSDM wird benötigt, damit sich Patientinnen und Patienten gegenüber der Praxis mit der elektronischen Gesundheitskarte (eGK) als Versicherte ausweisen können. Die betroffenen Konnektoren konnten sich nicht mit der Telematik-Infrastruktur verbinden, wodurch insbesondere der Online-Datenabgleich nicht möglich war. Die Infrastruktur selbst war dadurch zwar nicht gefährdet, aber die Verfügbarkeit in den Arztpraxen eingeschränkt.

- Im Dezember 2019 wurden auf dem Chaos Communication Congress Mängel in der Auslieferung von Sicherheitskarten HBA und SMC-B vorgestellt (vgl. u. a. *Quellenverzeichnis*[57]). Auch wenn es sich hierbei um Schwachstellen in organisatorischen Prozessen außerhalb der informationstechnischen Systeme handelte, wäre die Informationssicherheit bei einer tatsächlichen Ausnutzung der Schwachstellen gefährdet gewesen.

Die Neugestaltung der TI zur Telematik Infrastruktur 2.0 ist mit erheblichen Eingriffen in die Sicherheitsarchitektur verbunden, die ein Umdenken und eine Neubewertung vieler Fragen erforderlich machen. Auch hier wird das BSI an der Gestaltung einer bestmöglichen Lösung mitwirken, zu der bereits folgende Säulen der IT-Sicherheit identifiziert wurden:

- Das bisherige Sicherheitsniveau wird mindestens erhalten bleiben.
- Schutzmechanismen werden unter einer ganzheitlichen Betrachtung der Prozesse und Systeme durch entsprechende Sicherheits- und Risikoanalysen definiert.
- Die zur Verarbeitung medizinischer Daten genutzten Endgeräte müssen über ein geeignetes Sicherheitsniveau verfügen (z. B. Secure Element).
- Kryptografische Sicherheit muss auf einem Hardware-Sicherheitsanker unter alleiniger Kontrolle des Datenbesitzers basieren.
- Jegliche Kommunikationsverbindung muss verschlüsselt und beidseitig authentifiziert sein.
- Anwenderinnen und Anwender müssen durch eine Zwei-Faktor-*Authentifizierung* mit Vertrauensniveau hoch authentifiziert werden.
- Für Anwenderinnen und Anwender, die das erforderliche Sicherheitsniveau auf ihrem eigenen Endgerät nicht sicherstellen können, muss es eine geeignete Alternative geben.
- Der Übergang von TI 1.0 auf TI 2.0 folgt einem Migrationskonzept, in dem alle Zwischenzustände das Sicherheitsniveau aufrecht halten.

eHealth und die Einführung der Telematik-Infrastruktur bleiben ein zentraler Treiber für das Zusammenspiel von Leistungserbringern, Krankenkassen, Patientinnen und Patienten und anderen Stakeholdern. Nur durch einen steten Wandel kann die Digitalisierung des Gesundheitswesens mit der IT-Sicherheitslage Schritt halten.

2.1.9 Sichere Gestaltung virtueller Versammlungen und Abstimmungen

Die COVID-19-Pandemie hat dazu geführt, dass viele Versammlungen, Abstimmungen und Wahlen nicht vor Ort als Präsenzveranstaltung stattfinden konnten. Infolgedessen ist der Bedarf an virtuellen Alternativen stark gestiegen. Neben praktischen Fragen nach dem technischen Umgang mit Videokonferenzprogrammen und datenschutzrechtlichen Problemen rückte der Fokus vor allem in Richtung Informationssicherheit: Wie lassen sich virtuelle Versammlungen gestalten? Worauf ist zu achten, damit Informationen sicher übertragen und ausgetauscht werden können? Welche Risiken ergeben sich und welche Anforderungen stellen sich bei geheimen Abstimmungen? Im Dialog mit der Fachöffentlichkeit hat das BSI dazu frühzeitig Hilfestellungen für alle Zielgruppen in Staat, Gesellschaft und Wirtschaft erarbeitet. Darauf basierend hat das BSI den Deutschen Bundestag und Parteien beraten, wie sich virtuelle Parteitage und Abstimmungen sicher umsetzen lassen.[p)]

Online-Wahlen

Noch komplexer wird es beim Thema Online-Wahlen. Im Rahmen eines Modellprojektes wird den Krankenkassen bei den Sozialversicherungswahlen im Jahr 2023 neben der herkömmlichen Stimmabgabe per Briefwahl fakultativ die Möglichkeit eröffnet, Online-Wahlen durchzuführen. Die Wahlberechtigten können somit ihr Votum nicht nur per Briefwahl, sondern auch elektronisch über das Internet abgeben. Mit der Technischen Richtlinie TR-03162 „IT-sicherheitstechnische Anforderungen zur Durchführung einer Online-Wahl im Rahmen des Modellprojekts nach § 194a Fünftes Buch Sozialgesetzbuch (Online-Wahl)“ macht das BSI Vorgaben für die Informationssicherheit und schafft damit eine wesentliche Grundlage für die sichere Digitalisierung der Sozialversicherungswahlen 2023. Diese Richtlinie beinhaltet auch kryptografische Anforderungen, mit deren Hilfe die Einhaltung der Wahlgrundsätze gewährleistet werden soll. Dieses Projekt wurde unabhängig von der COVID-19-Pandemie initiiert, bekam durch die aktuelle Situation jedoch einen höheren Stellenwert. Das BSI widmet sich daher zusätzlich der Prüfung, inwieweit andere nichtpolitische Wahlen sicher digitalisiert werden können. Weiterführende Informationen finden Sie hier:[q)]

Informationen zur Cyber-Sicherheit von Bundestags- und Landtagswahlen finden Sie im entsprechenden Kapitel ab Seite 74.

2.1.10 Sicherheit von Bezahlverfahren

Die Starke Kundenauthentifizierung (SCA) bei Zahlungen mit digitalen oder physischen Karten am Point of Sale (POS), bei Transaktionen am Geldautomaten oder bei Zahlungen im E-Commerce ist bereits seit einiger Zeit in Gebrauch. Chipkarten in Kombination mit einer PIN oder die Kombination von digitaler Karte und einem biometrischen Faktor, wie dem Fingerabdruck, werden mittlerweile fast schon selbstverständlich genutzt.

Die Einführung der SCA speziell bei Kreditkartenzahlungen im Rahmen von Online-Einkäufen dagegen wurde immer wieder verschoben oder war noch nicht vollständig verpflichtend, weil die Integration in die Shopsysteme und die Kommunikation zu den Banken Probleme bereitete. Bei vielen Online-Einkäufen wurden aufgrund mangelhafter Implementierung der Sicherheitsfeatures Kreditkartenzahlungen zurückgewiesen, und der Kaufvorgang wurde abgebrochen. Kundinnen und Kunden suchten sich Shops ohne die erweiterte Eingabe zusätzlicher Faktoren oder sogar gänzlich andere Bezahlverfahren.

Inzwischen ist 3D-Secure der Sicherheitsstandard, der bei der Zahlung mit Kreditkarten im Internet verpflichtend zum Einsatz kommt.

Das 3D-Secure-Verfahren ist sowohl für den Einsatz im Web als auch in *Apps* geeignet. Damit können biometrische Schnittstellen wie Fingerabdruck-Scanner oder Gesichtserkennung zur *Authentifizierung* verwendet werden.

Die auf der Kreditkarte gespeicherten Daten werden nur zwischen der Bank und der 3D-Secure-Webseite getauscht, der Händler hat keinen Zugriff auf die Daten.

Zur Nutzung von 3D-Secure ist zwar eine Registrierung bei der Bank erforderlich ist, aber dadurch entstehen keine zusätzlichen Kosten für die Nutzerin bzw. den Nutzer. Das BSI bewertet das Verfahren als sicherer als die bloße Eingabe der auf der Kreditkarte angezeigten Daten. Ein Betrug wird erschwert, da eine wirkliche *Authentifizierung* der Kundin bzw. des Kunden stattfindet.

Mehr dazu in der BSI-Broschüre zu Online-Bezahlverfahren:[r)]

2.1.11 Zwei-Faktor-Authentisierung

Der übliche Weg, sich bei einem Online-Dienst zu authentisieren, ist nach wie vor die Eingabe eines Passworts. Hier wird also ein einzelner Faktor abgefragt, um eine Nutzerin bzw. einen Nutzer zu authentifizieren. Passwörter sind einfach einzusetzen, haben aber Nachteile: Zum einen reicht die Kenntnis dieses einen Faktors, um den Authentisierungsmechanismus zu hacken, zum anderen ist es aufwändig, für jeden Dienst ein sicheres und individuelles Passwort zu wählen.

Immer mehr Dienste fragen daher neben dem Passwort einen zweiten Faktor ab, etwa einen Authentisierungscode, der auf das Smartphone gesendet wird. Eine höhere Sicherheit ist hier aber nur dann gegeben, wenn eine echte Trennung der Geräte stattfindet und sich die Faktoren nicht gleichzeitig angreifen lassen. Wenn zum Beispiel für eine Smartphone-Anwendung als erster Faktor ein Passwort und als zweiter Faktor ein an das Smartphone geschickter Code verwendet wird, kann beides durch Schadsoftware auf dem Smartphone ausgelesen werden und ist daher ungeeignet. Darüber hinaus ergeben sich oft weitere Usability-Probleme, etwa beim Wechsel des Smartphones oder der Mobilfunknummer.

Vorteilhafter ist, wenn bei einer Zwei-Faktor-Authentisierung zwei Faktoren aus unterschiedlichen Kategorien (Besitz, Wissen, Biometrie) abgefragt werden. Durch die Kombination der Stärken der einzelnen Faktoren wird ein Angriff um ein Vielfaches erschwert. Dabei sollten biometrische Merkmale nicht beim Onlinedienst gespeichert, sondern lokal verwendet werden.

Als Mitglied der Fast Identity Online Allianz (FIDO) ist das BSI an der Definition nachweisbar sicherer Authentifikatoren beteiligt. Der Nachweis eines hohen Sicherheitsniveaus kann durch eine Zertifizierung nach Common Criteria erbracht werden. Das BSI hat hierzu ein Schutzprofil mit hoher Prüftiefe für sichere FIDO-U2F-Token veröffentlicht, nachdem ein vom BSI entwickelter FIDO-U2F-Token erfolgreich zertifiziert wurde. Dieser Token passt sich nahtlos in existierende Webinfrastrukturen ein, da der Besitz des Authentikators im zweiten Schritt nach einer erfolgreichen Passwort-*Authentisierung* nachgewiesen wird. Ohne eine Prüfung mit entsprechender Sicherheitszertifizierung ist die Gefahr für Implementierungsfehler hoch. Auch eine Zertifizierung nach den FIDO-Sicherheitsstandards steht kurz vor dem Abschluss.

Zum Schutzprofil gelangen Sie hier:[s)]

2.1.12 Bewertung von elektronischen Identifizierungsverfahren

COVID-19-bedingte Kontaktbeschränkungen haben vielfach den Bedarf einer digitalisierten Verwaltung von Bund und Ländern verdeutlicht. Für die digitale Schnittstelle zwischen Bürgerinnen und Bürgern auf der einen und dem Staat auf der anderen Seite gibt es mit dem 2017 erlassenen Onlinezugangsgesetz (OZG) zudem die rechtliche Vorgabe, Verwaltungsleistungen bis Ende 2022 grundsätzlich auch online anzubieten (vgl. Kapitel *Umsetzung des Online-Zugangsgesetzes*, Seite 78).

Eine neue, digitale Normalität bei Verwaltungsleistungen kann nur gelingen, wenn sich Bürgerinnen und Bürger sowie Unternehmen an den Schnittstellen zur Verwaltung nutzerfreundlich und sicher identifizieren und authentisieren können. Bürgerinnen bzw. Bürger und Unternehmen müssen auch im digitalen Raum auf geeignete, sichere Zugangslösungen zu Verwaltungsdienstleistungen vertrauen können.

Mit Portalverbund und Nutzerkonten (vgl. *Quellenverzeichnis*[58]) von Bund und Ländern zur Umsetzung des OZG wird in Deutschland gleichzeitig die digitale föderale Kooperation vorangebracht. Das BSI bewertet sowohl grundlegende Technologien als auch konkrete Verfahren, um für Staat, Wirtschaft und Gesellschaft die damit verbundenen Risiken, etwa durch Identitätsbetrug, zu minimieren.

Das BSI hat zwei Technische Richtlinien veröffentlicht, die es ermöglichen, Verfahren für elektronische Identitäten und Vertrauensdienste für Onlineprozesse systematisch zu bewerten. Die TR-03107-1 behandelt Vertrauensniveaus und Mechanismen für elektronische Identitäten sowie Vertrauensdienste im E-Government, die TR-03147, komplementär dazu, Verfahren zur Identitätsprüfung natürlicher Personen. Bewertungen erfolgen differenziert für die Vertrauensniveaus „normal“, „substantiell“ und „hoch“.

Das BSI hat bislang zwei privatwirtschaftliche Verfahren bewertet, im Berichtszeitraum wurde zudem die Bewertung von zwei weiteren elektronischen Identifizierungsverfahren gestartet. Die technische Bewertung bildet für das BMI die Grundlage zur Entscheidung über die Zustimmung zur Nutzung des jeweiligen Verfahrens im E-Government.

Von besonderem Interesse sind hierbei Verfahren, die mindestens das Vertrauensniveau „substantiell“ nach TR-03107-1 erreichen. Für die dafür benötigten kryptografischen Algorithmen und Protokolle existieren sowohl geeignete Verfahren als auch etablierte Bewertungskriterien. Wesentlich komplexer ist die Vertrauensniveaubewertung an den Schnittstellen zur analogen Welt und bei Medienbrüchen. Häufig ist das bei der initialen Identifizierung oder Registrierung von Personen für elektronische Identifizierungsverfahren der Fall. Neben Verfahren, in denen Ausweisdokumente ganz klassisch vor Ort vorgelegt werden, kommen hier häufig noch videobasierte Verfahren zum Einsatz, bei denen Personen mit ihren Ausweisdokumenten abgefilmt und dann geprüft werden. Zur Bewertung, inwiefern auch bei einer videobasierten Prüfung von Ausweisdokumenten das Vertrauensniveau „substantiell“ erreicht werden kann, kooperiert das BSI auch mit dem Bundeskriminalamt.

2.1.13 Sichere elektronische Identitäten auf dem Smartphone

Immer größere Teile des heutigen Lebens finden digital statt. Viele Dienstleistungen werden heute über Smartphones bezogen. Für jeden Service, egal ob Onlinebanking, Einkaufen, digitale Behördengänge oder soziale Netzwerke, benötigen die Nutzer eine digitale Identität. Um diese sicher auf dem Smartphone zu verwenden, entwickelt die Bundesregierung zurzeit den Online-Ausweis weiter. Die neue Smart eID basiert auf der Technologie des Personalausweises und ermöglicht es, Identitätsdaten sicher abzuspeichern und datensensible Dienste auch auf dem Smartphone nutzbar zu machen.

Um eine Vielzahl von Onlineservices nutzen zu können, benötigen die Bürgerinnen und Bürger eine elektronische Identität (eID), ein Begriff, der für ganz unterschiedliche Onlinezugänge stehen kann:

- für ein Pseudonym in Onlineforen,
- für Accounts in sozialen Netzwerken,
- um als Käuferin oder Käufer in einem Onlineshop oder
- als Bankkundin oder Bankkunde beim Onlinebanking aufzutreten.

Jede dieser eIDs muss gegen Missbrauch geschützt werden – je nach Art der elektronischen Identität unterschiedlich stark. Manchmal genügt die Eingabe einfacher Zugangsdaten (wie Nutzername und Passwort). Bei sensiblen Daten reicht dieser Schutz aber nicht. Wer beispielweise mit dem Smartphone Bankgeschäfte erledigen oder den Zutritt auf das Firmengelände steuern möchte, sollte eine besser geschützte eID nutzen.

Einführung der Smart-eID

Smartphones sind, wie jedes vernetzte Gerät, ständig der Gefahr eines Cyber-Angriffes ausgesetzt. Darum müssen besondere Voraussetzungen erfüllt sein, um die sichere Speicherung einer eID auf dem Smartphone zu gewährleisten.

Grundlage für die Smart-eID ist ein so genanntes eID-Applet, das ausschließlich innerhalb eines Sicherheitselements des Mobilgerätes ausgeführt werden darf. Das Sicherheitselement wird durch einen dedizierten Chip realisiert, welcher für die sichere Speicherung von kryptografischen Schlüsseln sowie die sichere Ausführung kryptografischer Operationen oder *Applikationen* optimiert ist. Dieser kann in Mobilgeräten entweder als ein sogenanntes Secure Element (SE) realisiert werden oder durch eine fest-

verbaute SIM-Karte, welche auch eUICC oder eSIM genannt wird. Das Applet selber basiert auf etablierten kryptografischen Protokollen, die bereits beim elektronischen Personalausweis zum Einsatz kommen. Das bietet den Vorteil, dass die Smart-eID kompatibel zu bereits bestehenden Diensten ist, die bereits die Online-Ausweisfunktion anbieten.

Im nächsten Schritt muss gewährleistet werden, dass das eID-Applet nur auf Sicherheitselementen mit einem geeigneten Sicherheitsniveau verwendet und auf diese aufgespielt werden kann. Dafür wird mit dem Trusted Service Manager (TSM) eine Infrastruktur geschaffen, die für alle Anbieter von sicheren Applets diskriminierungsfrei zugänglich ist und höchste Sicherheits- und Datenschutzstandards erfüllt. Der TSM übernimmt als Schnittstelle zwischen dem Ausweishersteller, dem Mobilgerätehersteller und der Endkundin bzw. dem Endkunden die Aufgabe, die Eignung der Sicherheitselemente von mobilen Endgeräten zu validieren und das eID-Applet sicher auf diese aufzubringen. Um das zu ermöglichen, engagiert sich das BSI in der Standardisierung der notwendigen Komponenten, Interfaces und Abläufe, damit die entwickelte Technologie für möglichst viele Mobilgeräte und Endnutzer zur Verfügung steht.

Für die eigentliche Verwendung der Smart eID muss das eID-Applet schließlich noch mit validen Identitätsdaten des Nutzers bespielt werden. Das wird durch einen Dienst ermöglicht, bei dem die Nutzerin bzw. der Nutzer ihren bzw. seinen bestehenden Personalausweis via Online-Ausweisfunktion ausliest und die Daten im Anschluss verifizierbar und manipulationssicher im Applet hinterlegt.

Das BSI agiert als technischer Projektleiter für die Auftragnehmer, die an der Umsetzung der Smart-eID beteiligt sind, und steuert Sicherheitsvorgaben in Form von Technischen Richtlinien und Schutzprofilen bei. Gleichzeitig hat das BSI viele Gespräche mit Herstellern von mobilen Endgeräten geführt und seine Expertise in verschiedenen Standardisierungsgremien eingebracht. Diese Tätigkeiten erfolgten mit dem Ziel, Hersteller für die Anforderungen an Sicherheit in Smartphones, Tablets und Wearables zu sensibilisieren und die Ansprüche des BSI in internationalen Standards zu verankern. Nur über entsprechend einzuhaltende Standards lässt sich erreichen, dass jede Käuferin bzw. jeder Käufer von mobilen Geräten die notwendigen Sicherheitsfunktionen erhält, um ihre bzw. seine eID zu schützen. Die Smart-eID soll zum Herbst 2021 auf ersten Smartphone-Modellen eingeführt werden.

2.1.14 Biometrie im Zeitalter der Künstlichen Intelligenz

Unter einer medialen Identität versteht man Individuen in einem digitalen Medium, die anhand von biometrischen Merkmalen, beispielsweise des Gesichts oder der Stimme, identifiziert werden können. Verfahren zur Manipulation solcher medialen Identitäten existieren schon seit vielen Jahren. Durch Methoden aus dem Bereich der Künstlichen Intelligenz (KI) ist es aber deutlich einfacher geworden, Fälschungen mit vergleichsweise wenig Aufwand und Expertise in einer hohen Qualität zu erstellen. Aufgrund der Nutzung von tiefen neuronalen Netzen werden solche Verfahren umgangssprachlich als Deepfakes bezeichnet. Mit Hilfe dieser Verfahren ist es beispielsweise möglich, das Gesicht einer Person in einem Video mit dem Gesicht einer anderen Person zu tauschen (Face Swapping), oder die Stimme des Audiokanals durch eine andere zu ersetzen (Voice Conversion). Der Prozess eines Face-Swapping-Verfahrens ist in Abbildung 7 skizziert. Um solche Fälschungen herstellen zu können, ist es notwendig, Material (z. B. Video- bzw. Audioaufnahmen) von der zu fälschenden Identität zu besitzen.

Mittels dieser Verfahren ist es auch für den technisch versierten Laien möglich, mediale Identitäten zu manipulieren, um beispielsweise Fernidentifikationssysteme zu überwinden, Personen zu verleumden, zu betrügen (z. B. *CEO-Fraud*) oder Falschnachrichten zu erstellen. Im April 2021 wurde ein Fall bekannt, in dem mehrere europäische Politiker von einem *Deepfake* getäuscht wurden: Sie hatten in einer Videokonferenz vermeintlich mit Leonid Wolkow gesprochen, einem Vertrauten des Kremlkritikers Alexei Nawalny, und erst im Nachhinein gemerkt, dass es sich bei dem Gesprächspartner in Wirklichkeit um eine andere Person gehandelt hat (vgl. *Quellenverzeichnis*[59]). Damit war eine neue Qualität von *Deepfakes* erreicht, der durch adäquate Detektionstechnologien und Verteidigungsmaßnahmen begegnet werden muss.

Quellen: J. Naruniec et al. High-Resolution Neural Face Swapping for Visual Effects, EGSR 2020, 39, 4 (2020)

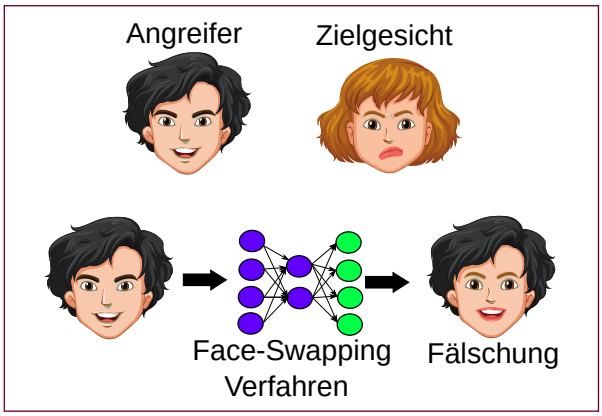


Abbildung 7: Beim Face Swapping wird das Gesicht einer Zielperson in das eines Angreifers eingefügt, wobei der Gesichtsausdruck des Angreifers beibehalten werden soll.
Quelle: brgfx / Freepik

Aktuelle Entwicklungen im Bereich der Manipulation medialer Identitäten beschäftigen sich damit, die Qualität der Ergebnisse zu optimieren und die Anzahl der von der Zielperson benötigten Daten zu minimieren. Diese werden meist von wissenschaftlichen Instituten, vereinzelt auch von Konzernen unterstützt, jedoch wird die Software in den meisten Fällen nicht veröffentlicht. Für die Zukunft ist aber davon auszugehen, dass auch für die Öffentlichkeit Methoden zur Verfügung stehen werden, mit denen sich qualitativ hochwertige Fälschungen ohne offensichtliche Artefakte in Echtzeit erstellen lassen.

Andererseits ist KI auch wesentliche Grundlage für Verteidigungsmaßnahmen gegen die Fälschung medialer Identitäten. Ein Problem vieler dieser Maßnahmen besteht aber darin, dass sie für ein bestimmtes Einsatzszenario gute Ergebnisse liefern, oft aber nur schlecht auf veränderte Rahmenbedingungen, wie zum Beispiel eine Veränderung der Manipulationsmethode, reagieren.

Die Verfahren zur Manipulation medialer Identitäten werden stetig weiterentwickelt. Das macht auch die fortlaufende Verbesserung der Verteidigungsmaßnahmen notwendig. Das BSI beobachtet die Entwicklung dieser Angriffstechniken, um die tatsächlich möglichen Angriffe besser abschätzen zu können. Dies erlaubt im Anschluss die Entwicklung und Empfehlung von Verteidigungsmaßnahmen, die dem Stand der Forschung entsprechen.

2.2 Wirtschaft

Vernetzung und Austausch sind wichtige Faktoren für die Wirtschaft in Deutschland. Dabei hängt sie in hohem Maße von einer funktionierenden und sicheren IT ab. Dies gilt besonders für Betreiber Kritischer Infrastrukturen (KRITIS). Daher prüft das BSI, ob und inwieweit ein ausreichender Schutz gewährleistet ist, und schafft gleichzeitig die Voraussetzungen für eine Weiterentwicklung der entsprechenden Infrastrukturen. Mit der Allianz für Cyber-Sicherheit und ihren derzeit rund 5.000 Institutionen stärkt das BSI außerdem die Widerstandsfähigkeit des Standorts Deutschland gegen Cyber-Angriffe. Insbesondere kleine und mittlere Unternehmen profitieren vom fachlichen Austausch sowie von praxisorientierten IT-Sicherheitsempfehlungen. Für mehr Informationssicherheit neuer Technologien gestaltet das BSI u. a. praxisgerechte Sicherheitsanforderungen, Standards und Handlungsempfehlungen. Auch als zentrale Zertifizierungs- und Standardisierungsstelle in Deutschland übernimmt das BSI Verantwortung für den Digitalstandort Deutschland. Zudem leistet das BSI einen wesentlichen Beitrag zum Gelingen großer Digitalisierungsprojekte.

2.2.1 Gefährdungslage Kritischer Infrastrukturen

Kritische Infrastrukturen sind Organisationen mit wichtiger Bedeutung für das Gemeinwesen. Sie erbringen kritische Dienstleistungen wie die medizinische Versorgung oder die Versorgung mit Lebensmitteln, Wasser oder Strom. Kritische Dienstleistungen sind aber auch die Verarbeitung und Speicherung von Daten in Rechenzentren oder die Versorgung der Bevölkerung mit Bargeld. Durch die COVID-19-Pandemie ist der öffentliche Fokus bei Vorfällen derzeit auf das Gesundheitssystem gerichtet, Cyber-Angriffe sind jedoch für KRITIS-Betreiber aller Branchen beinahe an der Tagesordnung.

Alle kritischen Dienstleistungen sind ganz besonders von einer störungsfrei arbeitenden IT abhängig. Eine Störung, Beeinträchtigung oder auch ein Ausfall dieser zentralen Dienstleistungen kann zu nachhaltig wirkenden Versorgungsengpässen, erheblichen Störungen der öffentlichen Sicherheit oder anderen dramatischen Folgen führen. Daher sieht das BSI-Gesetz (BSIG) für KRITIS-Betreiber Maßnahmen zur Prävention (§ 8a BSIG) und zur Bewältigung (§ 8b BSIG) von IT-Sicherheitsvorfällen oder IT-Störungen vor.

IT-Sicherheitsgesetz stärkt durch Nachweispflicht die IT-Sicherheit bei Kritischen Infrastrukturen

Mit dem IT-Sicherheitsgesetz wurde 2015 für KRITIS-Betreiber in § 8a Absatz 3 BSIG eine Nachweispflicht zum Umsetzungsstatus der Sicherheitsanforderungen eingeführt. Die Betreiber müssen gegenüber dem BSI alle zwei Jahre den Nachweis erbringen, dass ihre IT-Sicherheit auf dem Stand der Technik ist. Die Nachweise enthalten Informationen zu umgesetzten Sicherheitsmaßnahmen, aber auch zu im Rahmen der Nachweisprüfung aufgedeckten Sicherheitsmängeln.

Im letzten Nachweiszyklus, der jeweils zwei Jahre umfasst, wurden in den Sektoren Informationstechnik und Telekommunikation, Finanz- und Versicherungswesen sowie Wasser und Energie im Rahmen der Prüfung der turnusmäßigen Nachweise insgesamt 1.805 Sicherheitsmängel gefunden. Die Sicherheitsmängel sind im Folgenden für jeden dieser Sektoren nach den Kategorien dargestellt, wie sie in der Orientierungshilfe zu Nachweisen festgelegt wurden.

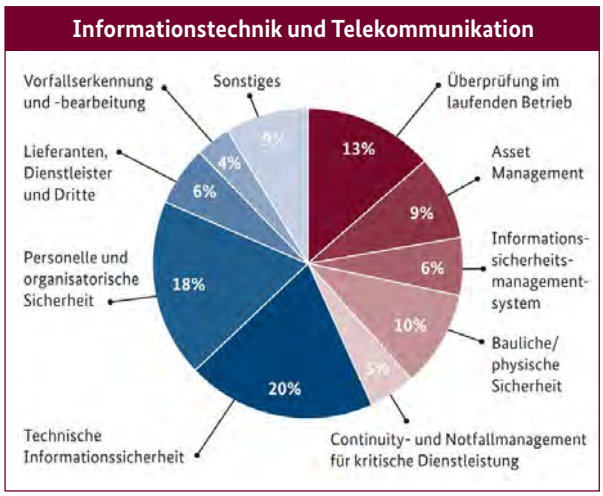


Abbildung 8: Mängel nach Kategorien im Sektor Informationstechnik und Telekommunikation.

Im **KRITIS-Sektor Informationstechnik und Telekommunikation** wurden vergleichsweise häufig Mängel in den Bereichen der technischen Informationssicherheit, der personellen und organisatorischen Sicherheit sowie der Überprüfung im laufenden Betrieb identifiziert. Deutlich seltener als in den Sektoren Energie und Wasser wurden Sicherheitsmängel im Bereich des Informationssicherheitsmanagementsystems (ISMS) identifiziert.

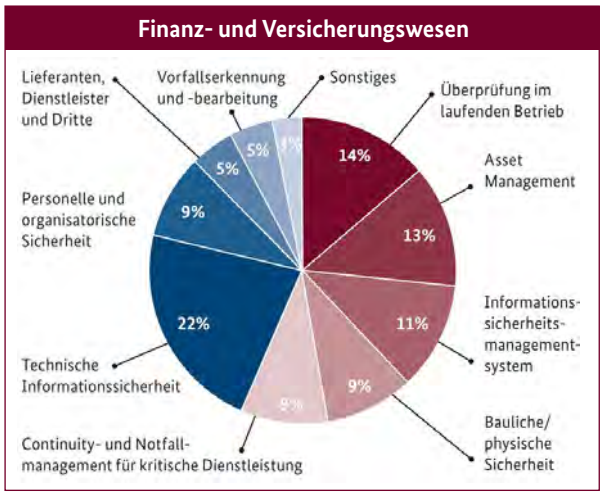


Abbildung 9: Mängel nach Kategorien im Sektor Finanz- und Versicherungswesen.

Im **KRITIS-Sektor Finanz- und Versicherungswesen** traten am häufigsten Mängel in den Kategorien technische Informationssicherheit, Überprüfung im laufenden Betrieb, Asset Management und ISMS auf. Mängel im Bereich der technischen Informationssicherheit waren im Sektor Finanz- und Versicherungswesen im Vergleich zu den anderen Sektoren am häufigsten. Das galt auch für die absolute Häufigkeit an Mängeln im Bereich der technischen Informationssicherheit. Grund dafür könnte sein, dass in diesem stark von IT geprägten und bereits vor dem IT-Sicherheitsgesetz durch gesetzliche Anforderungen regulierten Sektor ein höherer Reifegrad der IT-Sicherheit erreicht ist, mit entsprechend weniger Mängeln in den anderen Kategorien.
Zu berücksichtigen ist allerdings, dass die Kategorie der technischen Informationssicherheit sehr umfassend ist, also viele verschiedene Mängel subsumiert. Mängel im Bereich Asset Management hängen häufig damit zusammen, dass die Betreiber ihre KRITIS-Anlagen zunächst entsprechend eindeutig identifizieren und klassifizieren müssen.

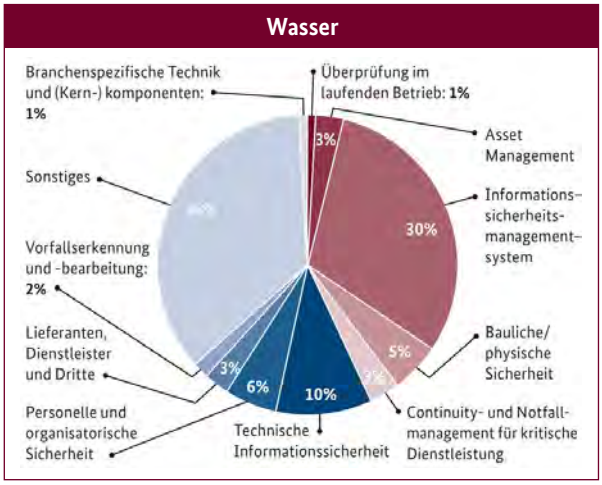


Abbildung 10: Mängel nach Kategorien im Sektor Wasser.

Rund ein Drittel aller Mängel im **KRITIS-Sektor Wasser** sind dem Bereich ISMS zuzuordnen. Es wird deutlich, dass viele Optimierungspotenziale im Bereich ISMS im Sektor Wasser noch nicht ausgeschöpft sind. Anders als in den Sektoren Informationstechnik und Kommunikationstechnik sowie Finanz- und Versicherungswesen wird in diesem Sektor nur jeder zehnte im Rahmen einer Nachweisprüfung gefundene Mangel der Kategorie technische Informationssicherheit zugeordnet, allerdings ist der Sektor auch vergleichsweise gering digitalisiert und damit weniger von IT abhängig.

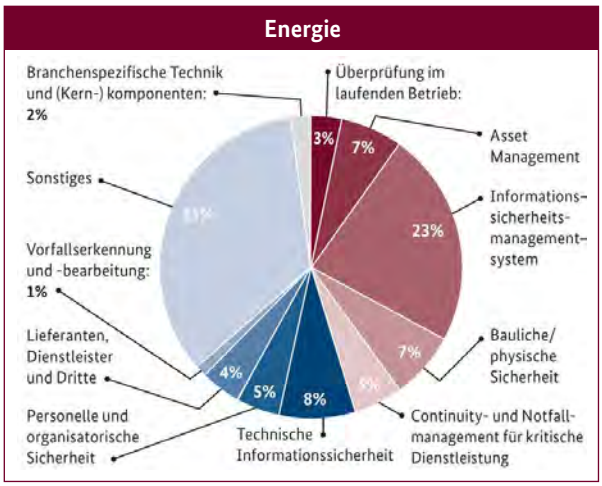


Abbildung 11: Mängel nach Kategorien im Sektor Energie.

Im **KRITIS-Sektor Energie** ergibt sich ein ähnliches Bild wie im Sektor Wasser. Rund ein Viertel der im Sektor festgestellten Mängel sind der Kategorie ISMS zugeordnet. Ähnlich wie im Sektor Wasser ist auch im Sektor Energie der Anteil der Mängel im Bereich der technischen Informationssicherheit im Verhältnis zur Gesamtmenge an Mängeln gering. Dieser weitestgehend digitalisierte Sektor ist allerdings im Gegensatz zum Sektor Wasser sehr stark von IT abhängig.

Von den Erkenntnissen des BSI aus den Nachweisen profitieren Staat und Wirtschaft

Die aus den Nachweisen gewonnenen Erkenntnisse helfen den Sektorbetreuerinnen und -betreuern im KRITIS-Fachbereich des BSI, die Unternehmen aus den betreuten Branchen bei der Verbesserung ihrer IT-Sicherheit spezifisch zu beraten. Auch in die Erarbeitung neuer branchenspezifischer Sicherheitsstandards (B3S) fließen die von Betreibern und BSI erlangten Erkenntnisse aus den Nachweisen ein.

Um künftig ein noch detaillierteres Bild über die Häufigkeit und die zugrundeliegenden Ursachen von Mängeln zu erlangen, soll der Pool an Mangelkategorien ergänzt werden. Auf diese Weise erhalten nachweispflichtige KRITIS-Betreiber konkrete Anhaltspunkte zu Prüffeldern und Verbesserungspotenzial bei ihrer IT-Sicherheit.

2.2.2 *UP KRITIS*

Der *UP KRITIS* ist eine Plattform für die operative und konzeptionelle Zusammenarbeit von KRITIS-Betreibern, deren Fachverbänden und den zuständigen Behörden in Deutschland. Ziel ist der Schutz der Kritischen Infrastrukturen, wobei ein Schwerpunkt der Arbeiten auf Cyber-Sicherheit liegt. Seit über 10 Jahren arbeiten die Beteiligten im *UP KRITIS* zusammen, bis Mai 2021 sind 750 Organisationen Teilnehmer des *UP KRITIS* geworden. Das BSI ist seit der Gründung des *UP KRITIS* an der Partnerschaft beteiligt und betreibt dessen Geschäftsstelle.

Erfolgreiche Zusammenarbeit von Betreibern und Staat zum Schutz Kritischer Infrastrukturen

Im *UP KRITIS* wird sowohl auf operativer wie auch auf konzeptioneller Ebene kooperiert. Auf operativer Ebene tauschen sich die Beteiligten zur aktuellen Cyber-Sicherheitslage aus. Hierzu versendet das BSI Warnungen, Lageberichte und Hintergrundinformationen. In den Arbeitskreisen des *UP KRITIS* werden Vorfälle thematisiert und im vertraulichen Rahmen besprochen. Zudem steht das BSI über eine dedizierte KRITIS-Ansprechpartnerin oder einen dedizierten KRITIS-Ansprechpartner im Nationalen IT-Lagezentrum mit den KRITIS-Betreibern im Kontakt, um bei Unregelmäßigkeiten oder Vorfällen schnell reagieren zu können. Insbesondere zu größeren Vorfällen (wie z. B. der Exchange-Schwachstelle im Frühjahr 2021, vgl. Vorfall *Kritische Schwachstellen in Microsoft Exchange*, Seite 27) findet ein intensiver Informationsaustausch im *UP KRITIS* statt.

Weiterentwicklung der Cyber-Sicherheit der KRITIS-Betreiber in den Arbeitskreisen des *UP KRITIS*

An konzeptionellen und inhaltlichen Fragen wird vor allem in den Themenarbeitskreisen (TAK) des *UP KRITIS* gearbeitet. Neu gegründet wurde der TAK Detektion, da die Detektion von Cyber-Angriffen zunehmend an Bedeutung gewinnt. Der Arbeitskreis entwickelt aktuell unter Beteiligung des BSI Orientierungshilfen zu Fragestellungen der Detektion. Der TAK Operativer Informationsaustausch hat die Risikomatrix des *UP KRITIS* weiterentwickelt. Die Matrix ermöglicht es den Branchen, anhand eines Bedrohungskatalogs branchenspezifische Verwundbarkeiten und Eintrittswahrscheinlichkeiten abzuschätzen. Durch eine regelmäßig wiederholte Risikoanalyse (z. B. im Rahmen der Sitzungen der Branchenarbeitskreise) können Risikotrends ermittelt werden. Die Auswertung der Ergebnisse der KRITIS-Branchen führt zu einem branchenübergreifenden KRITIS-Lagebild, das auch Trends darstellt.

Reformierte Gremienstruktur im *UP KRITIS*

Nach über 10 Jahren der erfolgreichen Zusammenarbeit hat sich 2021 der *UP KRITIS* neu aufgestellt. Neben den Themen- und Branchenarbeitskreisen (AK) sind das Plenum und der Rat übergreifende Gremien (siehe *Abbildung 12*).

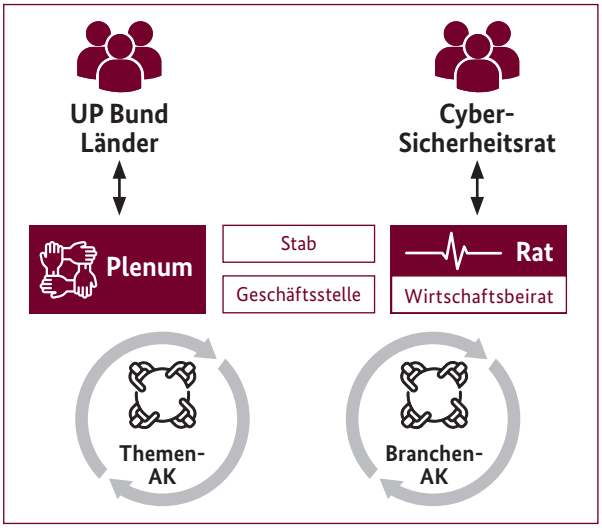


Abbildung 12: Gremienstruktur des *UP KRITIS*

Das Plenum des *UP KRITIS* ist die beschlussfassende Versammlung der Arbeitskreissprecher im *UP KRITIS*. Nach einer Umstrukturierung des Plenums kann seit 2021 jede KRITIS-Branche eine Person als Branchensprecher in das Plenum entsenden. Dadurch sind alle KRITIS-Branchen im Plenum vertreten.

Der Rat ist das politische Beratungsgremium des *UP KRITIS*. Er gibt Impulse und Anregungen für strategische Ziele und Projekte im *UP KRITIS* und stärkt dadurch die partnerschaftliche Zusammenarbeit von Staat und Wirtschaft. Die Ratsvertreter aus der Wirtschaft werden für jeweils zwei Jahre von den KRITIS-Branchen bestimmt und vom Plenum bestätigt, zuletzt Anfang 2021.
Hier gelangen Sie zur Webseite von *UP KRITIS*:[t)]

2.2.3 Digitalisierung der Energiewirtschaft: Rollout intelligenter Messsysteme

Durch die Verwendung von intelligenten Messsystemen und der damit verbundenen Nutzung zertifizierter Smart Meter Gateways werden künftig wichtige Systeme des Energienetzes über eine sichere Kommunikationsinfrastruktur vernetzt. Zugleich wird Cyber-Angriffen auf solche Systeme wirksam begegnet, die im Berichtszeitraum weiter zugenommen haben.

Vier Hersteller von Smart Meter Gateways haben derzeit das Produktzertifizierungsverfahren des BSI erfolgreich abgeschlossen, zwei Hersteller (Power Plus Communications und EMH metering) konnten bereits innerhalb weniger Monate das Rezertifizierungsverfahren mit einem erweiterten Funktionsumfang erfolgreich abschließen.

Mit den zwei Smart Meter Gateways, die derzeit Netzzustandsdaten und Einspeisewerte bereitstellen können, erhalten Stromnetzbetreiber mit Hilfe intelligenter Messsysteme wichtige Informationen über die aktuelle Belastung ihres Netzes und können so mögliche Engpässe rechtzeitig erkennen und vorbeugen. Zudem helfen die Informationen, den Ausbau des Stromnetzes effizient und kostengünstig zu gestalten. Dabei gewährleisten die Geräte weiterhin Informationssicherheit auf höchstem Niveau.

Flexible Verbrauchseinrichtungen (Wärmepumpen, Elektromobile usw.) und dezentrale Erzeugungsanlagen können zukünftig über das Smart-Meter-Gateway gesteuert und somit netz- und marktdienlich eingesetzt werden.

Gemeinsam mit dem Bundeswirtschaftsministerium werden derzeit mit den Verbänden und den Unternehmen der Energiewirtschaft die wesentlichen technischen Eckpunkte und die daraus resultierenden BSI-Standards für ein sicheres Energienetz der Zukunft festgelegt. Dadurch können aktuelle Trends und Innovationen zielgerichtet erfasst und die Gateway-Technologie kontinuierlich für den Einsatz in weiteren Bereichen weiterentwickelt werden.

2.2.4 Moderne Telekommunikationsinfrastrukturen (5G)

Eine technologische Basis der zunehmenden Digitalisierung sind moderne Mobilfunkstandards im Bereich 5G/6G, die schnellere Verbindungen, weniger Latenzzeit und höhere Datenraten ermöglichen. Aufgabe des BSI ist, die Voraussetzungen dafür zu schaffen, dass diese Netze das höchstmögliche Niveau an Vertraulichkeit, Integrität und Authentizität erreichen. Basis für den Aufbau sicherer 5G/6G-Netze ist aktuell der Katalog von Sicherheitsanforderungen, den die Bundesnetzagentur gemeinsam mit dem BSI und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) auf Grundlage der Bestimmungen von § 109 TKG aktualisiert hat, und der für die neu aufzubauenden 5G/6G-Netze zur Anwendung kommen wird.

Sicherheitskatalog

Das Telekommunikationsgesetz (TKG) definiert die gesetzlichen Rahmenbedingungen für Betreiber von Telekommunikationsnetzen. Für die IT-Sicherheit ist dabei vor allem § 109 Abs. 6 des TKG relevant, der die nationalen Sicherheitsanforderungen an die Telekommunikationsinfrastrukturen in Form des sogenannten Sicherheitskatalogs regelt. Der Katalog wird im Einvernehmen mit dem BSI und dem BfDI durch die Bundesnetzagentur erstellt und laufend an die technischen und regulatorischen Rahmenbedingungen angepasst.

Die neu erstellte Anlage des Sicherheitskatalogs thematisiert unter anderem die Vertrauenswürdigkeit von Herstellern und Lieferanten, die Absicherung der Integrität von Komponenten über den gesamten Lebenszyklus sowie Anforderungen für die Aufrechterhaltung des sicheren Betriebs von Netzen mittels Sicherheitsmonitoring und Schlüsselmanagement. Darüber hinaus sind die Betreiber verpflichtet, kritische Netzkomponenten einer Sicherheitszertifizierung zu unterziehen.

Zertifizierungsstrategie

Um zu ermöglichen, dass sowohl für Produkte als auch für Systeme in den unterschiedlichen Netzbereichen unterschiedliche und aufeinander aufbauende Zertifizierungsschemata eingesetzt werden können, erarbeitet das BSI derzeit eine Zertifizierungsstrategie für 5G. Hierbei greift das BSI auf international anerkannte und etablierte Standards zurück, um den Aufwand für Hersteller und Betreiber zu minimieren.

Für die Produktzertifizierung dient das von der GSMA (Global System for Mobile Communications Association) entwickelte Prüf- und Auditierungsschema Network

Equipment Security Assurance Scheme (NESAS) als Grundlage. Zusammen mit der GSMA entwickelt das BSI derzeit das NESAS-Schema mit dem Ziel weiter, dieses als europäisches Zertifizierungsschema unter dem Cybersecurity Act zu verankern und weitere Prüfanforderungen, wie etwa einen sicheren Produktlebenszyklus inklusive Supply Chain-Betrachtung, in den Standard zu integrieren. Entsprechend der Technologie- und Marktentwicklung soll zu einem späteren Zeitpunkt die Produktzertifizierung um die Schemata Beschleunigte Sicherheitszertifizierung (BSZ) und Common Criteria (CC) ergänzt werden. Ziel ist, dass für ausgewählte, kritische Netzfunktionen Schutzprofile nach CC erarbeitet und europäisch (3GPP/GSMA) harmonisiert bzw. standardisiert werden.

Im Bereich der Systemzertifizierung erarbeitet das BSI für die Netzbetreiber Vorgaben im Rahmen von IT-Grundschutz bzw. ISO/IEC 27001. Diese umfassen u. a. Vorgaben für die Aufrechterhaltung des sicheren Netzbetriebs sowie zum Umgang mit kritischen Komponenten über den gesamten Produktlebenszyklus.

Die Technische Richtlinie des BSI, welche die im Rahmen der 5G-Zertifizierungsstrategie ausgewählten Schemata zur Produkt- und Systemzertifizierung zusammenfasst, wurde weiterentwickelt.

Europäische Harmonisierung

Die EU-Kommission empfiehlt ein abgestimmtes Vorgehen bei der Sicherheit von 5G-Netzen und veröffentlicht in ihrer Empfehlung Cyber-Sicherheit der 5G-Netze ((EU) 2019/534 vom 26. März 2019) einen Fahrplan zur Erarbeitung einer europaweiten Toolbox von Maßnahmen zur Erhöhung der Sicherheit in 5G-Telekommunikationsnetzen. Zu diesen Maßnahmen gehören insbesondere die Einrichtung einer Kooperationsgruppe, die Erstellung einer koordinierten europäischen Risikobewertung sowie die Entwicklung eines harmonisierten Maßnahmenkatalogs zur Bewältigung der identifizierten Risiken.

Das BSI setzt sich in dieser Gruppe dafür ein, geeignete Zertifizierungsschemata (z. B. das oben genannte NESAS-Schema) als europäische Zertifizierungsschemata einzuführen. Der entsprechende Auftrag zur Entwicklung eines 5G-Zertifizierungsschemas unter dem Cybersecurity Act ist im Januar 2021 durch die EU-Kommission an die ENISA übermittelt worden. Das BSI wird sich an dem weiteren Gestaltungsprozess in den Ad-hoc-Gruppen der ENISA beteiligen.

Technische Kompetenz und Förderung

Das BSI bündelt im neuen Standort Freital bei Dresden die verschiedenen 5G-Aktivitäten. Dazu wurde mit dem Ausbau von technischen Kompetenzen begonnen. Der Aufbau eines 5G-Security-Labors im BSI befindet sich in Planung. Dabei wird von Beginn an der breite Kontakt und Austausch mit Forschungseinrichtungen, Prüfstellen, Herstellern und Betreibern gesucht. Mit der absehbaren Verfügbarkeit von Produkten und Lösungen für das 5G-Release 16 im Jahr 2021 werden sich die Anwendungsfälle der 5G-Technologie deutlich verbreitern und auch in Campusnetzen stärker etablieren. Das BSI betrachtet deshalb auch verstärkt diesen Bereich aus der Sicherheitsperspektive.

Hervorzuheben ist das Thema Open RAN. Die O-RAN Alliance treibt international Spezifikationen voran, die einen deutlichen Umbruch bei den Radio Access Networks (Funkzugangsnetze, RAN) im Mobilfunk mit sich bringen werden. Auch die führenden Mobilfunknetzbetreiber in Europa setzen für den zukünftigen 5G-Netzausbau auf Open RAN. Die Betrachtungen zur IT-Sicherheit bei Open RAN müssen aus Sicht des BSI noch intensiviert und die aktuellen Open-RAN-Spezifikationen in puncto IT-Sicherheit noch weiterentwickelt werden. Gleichzeitig bietet die Aufschlüsselung von RAN-Funktionen neue Chancen für Sicherheitsbetrachtungen im RAN-Bereich.

Im Rahmen des Konjunkturprogramms der Bundesregierung (Corona-Folgen bekämpfen, Wohlstand sichern, Zukunftsfähigkeit stärken, Ziffer 45) hat auch Open RAN einen hohen Stellenwert eingenommen. Das BSI beteiligt sich an der Ausgestaltung konkreter Fördermaßnahmen zur IT-Sicherheit in 5G- und später auch in 6G-Funknetzen. Dabei wird ebenfalls die Sicherheit von Open RAN im Fokus stehen.

2.2.5 Cyber-Sicherheit im Automobilbereich

Im Straßenverkehr ergeben sich durch die zunehmende Vernetzung und Automatisierung sowie aus den Anforderungen der E-Mobilität gänzlich neue Bedrohungen durch mögliche Angriffe auf die Fahrzeug-IT, die bisher in der Fahrzeugtypgenehmigung nicht berücksichtigt wurden. Zahlreiche in den vergangenen Jahren publizierte Angriffe auf Fahrzeugsysteme, insbesondere über drahtlose Schnittstellen, zeigen das Bedrohungspotential auf.

Im Juni 2020 wurden daher auf internationaler Ebene Regelungen für die Cyber-Sicherheit von Kraftfahrzeugen verabschiedet, die Anfang des Jahres in Kraft getreten sind (*Quellenhinweis*[60]). Die neuen Vorschriften werden in EU-Recht überführt und sind ab Juli 2022 verbindlich. Durch die Regulierung werden Automobilhersteller verpflichtet, möglichen IT-bezogenen Gefährdungen u. a. durch geeignete Entwicklungs- und Reaktionsprozesse Rechnung zu tragen.

Vor diesem Hintergrund hat das BSI mit dem Kraftfahrt-Bundesamt (KBA) im Oktober des vergangenen Jahres eine Verwaltungsvereinbarung geschlossen, um die Kompetenzen im Bereich Cyber-Sicherheit im vernetzten und automatisierten Fahren zu bündeln. Das BSI unterstützt das KBA bei den Prozessen zur Typgenehmigung nach den oben genannten neuen UNECE-Regelungen ebenso, wie bei IT-Sicherheitsfragen in der Marktüberwachung. Zu diesem Zweck werden derzeit in beiden Behörden Prozesse zur gemeinsamen Bewertung von IT-Sicherheitsvorfällen und Schwachstellen in Kraftfahrzeugen etabliert, Analysekompetenzen aufgebaut sowie Anforderungen an Prüfungen formuliert und Testleitfäden entwickelt.

Im Juni 2020 unterzeichneten das BSI und der Verband der Automobilindustrie (VDA) eine Absichtserklärung, in der ein regelmäßiger Austausch zu Themen der IT-Sicherheit vereinbart wurde. Ziel ist, ein gemeinsames Verständnis für die verschiedenen Teilbereiche der Cyber-Sicherheit im Automobilbereich zu entwickeln und Handlungsbedarfe, z. B. in der Standardisierung, zu benennen. In den ersten Gesprächen wurde u. a. vereinbart, das Thema IT-Sicherheit in der Lieferkette aufzuarbeiten.

Die Fahrzeug-zu-Fahrzeug- bzw. Fahrzeug-zu-Infrastruktur-Kommunikation für kooperative intelligente Transportsysteme (C-ITS) findet ebenfalls weitere Verbreitung. Im Rahmen der Absicherung von C-ITS hat das BSI Entwürfe für Technische Richtlinien zur interoperablen Umsetzung der europäischen Vorgaben erstellt. Hierbei handelt es sich um Leitfäden für Kommunikationskomponenten in Road Side Units und in Fahrzeugen sowie für die zugehörigen Public Key-Infrastrukturen. Die Entwürfe werden zurzeit mit Vertreterinnen und Vertretern der beteiligten Industrie und Behörden abgestimmt.

Daneben befasst sich das BSI auch mit den Sicherheitsaspekten von KI-Verfahren, die im Kontext des (teil-)autonomen Fahrens zunehmend eingesetzt werden (siehe Kapitel *Künstliche Intelligenz*, Seite 82).

2.2.6 Cyber-Sicherheit im Luftverkehr

Mit der Verabschiedung der Durchführungsverordnung (EU) 2019/1583 Grundstandards für die Luftsicherheit in Bezug auf Cyber-Sicherheit auf europäischer Ebene müssen die nach den §§ 5, 8, 9 und 9a Luftsicherheitsgesetz (LuftSiG) regulierten Unternehmen ab dem 1. Januar 2022 zusätzlich zu ihren bereits bestehenden gesetzlichen Aufgaben auch Anforderungen an die IT-Sicherheit umsetzen. Hierzu zählen u. a. Präventivmaßnahmen im Bereich der Cyber-Sicherheit, wie beispielsweise der Schutz vor und die Erkennung von Cyber-Angriffen sowie der angemessene, praktikable und rechtzeitige Austausch von Informationen zu Schwachstellen und Schadsoftware. Ziel ist der Schutz des zivilen Luftverkehrs vor Cyber-Angriffen sowie vor Flugzeugentführungen, Sabotageakten und terroristischen Anschlägen.

Durch die zunehmende Digitalisierung und Vernetzung von Systemen ist es umso wichtiger geworden, neben dem klassischen Verständnis von Security und Safety auch IT-Sicherheit mit zu berücksichtigen. Beeinträchtigungen der Integrität, Authentizität oder gar der Ausfall von IT-Systemen können massive Auswirkungen auf den Flugbetrieb haben. Dass auch Flughäfen in Deutschland Opfer von Cyber-Angriffen werden können, wurde im November 2020 in Saarbrücken deutlich. Die IT-Systeme am Flughafen wurden durch eine *Ransomware* verschlüsselt und waren danach für einige Zeit nicht mehr verfügbar. Dieser Vorfall zeigt, dass die Bedrohungslage bzgl. der IT-Sicherheit für die Luftfahrt durchaus als kritisch zu bewerten ist.

In Deutschland wird das BSI für die Organisation und Steuerung der Maßnahmen zur Informationssicherheit für die nach §§ 5 und 8 Luftsicherheitsgesetz (LuftSiG) regulierten Unternehmen zuständig sein. Darunter fallen die ca. 200 deutschen Flughafenbetreiber sowie die Bereiche der Personen- und Gepäckkontrollen. Für die §§ 9 und 9a LuftSiG, worunter die Luftfahrtunternehmen und die Beteiligten der sicheren Lieferkette fallen, liegt die Zuständigkeit beim Bundesministerium für Verkehr und Infrastruktur. Zu den Beteiligten einer sicheren Lieferkette zählen nach LuftSiG reglementierte Beauftragte, bekannte Versender, Transporteure, Unterauftragnehmer von reglementierten Beauftragten, reglementierte Lieferanten und bekannte Lieferanten im Bereich der Luftfracht.

Das BSI wird für die Informationssicherheit in der Luftsicherheit Vorgaben und Anforderungen für die nach den §§ 5 und 8 LuftSiG regulierten Unternehmen erarbeiten und im Nationalen Luftsicherheitsprogramm (NLSP) festschreiben, welche von diesen im Rahmen der regelmäßig neu durchzuführenden Zulassung überprüft werden müssen.

Auch die Anforderungen an die Prüfung zur Einhaltung der Konformität mit den gesetzlichen Vorgaben wird das BSI ausarbeiten und im NLSP festschreiben.

2.2.7 Cyber-Sicherheit in der industriellen Versorgungskette

Im Zuge der Industrie 4.0 werden immer mehr Prozesse entlang der Lieferkette digitalisiert. Dies kann einerseits helfen, die Güter der Lieferkette – Software oder materielle Güter – vor Produktfälschung oder Manipulation zu schützen, andererseits ermöglicht die Digitalisierung der Lieferkette neue Geschäftsmodelle, erweiterte Analysen und automatisierte Kooperationen.

Auch hier entstehen neue Angriffsflächen und Einfallstore, die tief in die Unternehmen bis in die Produktionsumgebung reichen können. Welche gravierenden Auswirkungen dies auf ganze Unternehmensnetzwerke haben kann, zeigt beispielsweise der SolarWinds-Hack (vgl. Vorfall *SolarWinds*, Seite 30). Das Beispiel macht klar, dass IT-Sicherheit auch eine Gemeinschaftsaufgabe ist. Für den gemeinsamen Austausch und abgestimmte Reaktionsmechanismen müssen tiefgreifende, wettbewerbsrechtlich konforme Austausch- und Zusammenarbeitsformate entwickelt werden.

Durch das IT-Sicherheitsgesetz 2.0 wird dem Thema Cyber-Sicherheit u. a. in der Lieferkette weiter Nachdruck verliehen. Das Gesetz führt den Begriff der Unternehmen im besonderen öffentlichen Interesse ein, wovon Unternehmen mit bestimmter wirtschaftliche Bedeutung erfasst und welche daher zukünftig ähnlich den KRITIS-Betreibern besonderen Schutz- und Meldevorschriften unterliegen werden.

Aber auch kleine und mittlere Unternehmen (KMU) müssen ihre Geschäftsprozesse digitalisieren, andernfalls sind sie bei digitalisierten Lieferketten vom Markt ausgeschlossen. Erschwerend kommt hinzu, dass KMU über weniger Ressourcen oder Wissen (Stichwort: Fachkräftemangel) verfügen, um die Herausforderungen der Cyber-Sicherheit zu bewältigen (vgl. Kapitel *Besondere Situation der KMU in Deutschland*).

Strategie

Eine digitalisierte Lieferkette darf keinen geschlossenen Markt bilden, der bestimmte Teilnehmer ausschließt. Um dennoch allen Daten und allen Teilnehmerinnen und Teilnehmern in der Lieferkette vertrauen zu können, muss hinreichende Cyber-Sicherheit erlangt werden.

Daher gestaltet das BSI zusammen mit Akteuren aus Forschung und Wirtschaft die Digitalisierung der Lieferkette. Dies geschieht beispielsweise in der Plattform Industrie 4.0, die mehr als 300 Akteure aus über 150 Unternehmen, Verbänden, Gewerkschaften, Wissenschaft und Politik in ihre Arbeit einbindet. Gesteuert und geleitet wird die Plattform vom Bundesministerium für Wirtschaft und Energie und vom Bundesministerium für Bildung und Forschung in Zusammenarbeit mit hochrangigen Vertreterinnen und Vertretern aus Wirtschaft, Wissenschaft und Gewerkschaften.

Darüber hinaus treibt das BSI die Standardisierung und Zertifizierung von Sicherheitsmaßnahmen auf allen Unternehmensebenen voran. Um KMU bei der Digitalisierung und bei der Einrichtung von Sicherheitsmaßnahmen zu unterstützen, erarbeitet das BSI Best-Practice-Guides mit Handlungsempfehlungen und Checklisten für konkrete Technologien und Standards, bspw. eIDAS oder IEC 62443.

Europäische & internationale Zusammenarbeit

Zusammen mit der japanischen Robot Revolution & Industrial *IoT* Initiative (RRI) entwickeln die Plattform Industrie 4.0 und das BSI einen Trustworthiness Profile-Demonstrator für den Austausch von eIDs und digitalisierten Unternehmenszertifikaten.

In der Internationalen Organisation für Normung (ISO) wirkt das BSI an der Standardisierung einer Programmierschnittstelle für Sicherheitselemente in Industriegeräten mit (ISO/IEC TS 30168 ED1. *Internet of Things (IoT)* – Generic Trust Anchor Application Programming Interface for Industrial *IoT* Devices).

2.2.8 Besondere Situation der KMU in Deutschland

In Deutschland existieren nach EU-Klassifikation etwa 2,6 Millionen Unternehmen, die dem Bereich KMU zuzurechnen sind, das sind 99,4 Prozent aller Unternehmen in Deutschland. Das BSI orientiert sich bei der Klassifikation von KMU ergänzend an der Definition des Bonner Instituts für Mittelstandsforschung (IfM), das die Grenze für Mittlere Unternehmen nicht bei 249, sondern bei 499 Beschäftigten zieht, da sich die deutsche Besonderheit der mittelständischen Familienunternehmen damit besser darstellen lässt. Viele dieser familien- bzw. eigentümergeführten Unternehmen zählen zur Gruppe der Hidden Champions, die in Deutschland etwa 1.500 Unternehmen umfasst - und damit etwa die Hälfte aller Hidden Champions weltweit ausmacht.

Die Gruppe der KMU stellt einen wesentlichen Erfolgsfaktor der deutschen Wirtschaft dar. Mängel bei der IT-Sicherheit von KMU können sich daher merklich und unmittelbar auf die Wirtschaftsleistung der Bundesrepublik Deutschland auswirken. Anders als typische Großunternehmen beschäftigen KMU in der Regel keine dedizierten IT-Sicherheitsteams. Oftmals verfügen sie nicht einmal über einen eigenen IT-Betrieb. Daraus folgt vielfach eine mangelnde Beurteilungskompetenz für IT-Sicherheitsgefährdungen. Zudem fehlt auf Managementebene häufig das grundsätzliche Bewusstsein für die Risiken und Abhängigkeiten, die der Einsatz von Informationstechnik mit sich bringt. Dadurch sind KMU gegenüber Bedrohungen aus dem Cyber-Raum besonders anfällig. Durch den stetig zunehmenden Grad an Digitalisierung verschärft sich die Gefährdungslage kontinuierlich. Dies spiegelt sich auch in den Analysen des BSI zum Updateverhalten von Unternehmen

wider. So konnte beispielsweise im Rahmen einer Warnaktion des BSI im März 2021 zu Schwachstellen im Produkt Microsoft Exchange-Server eine große Zahl von verwundbaren Systemen in Deutschland identifiziert werden. (siehe auch Vorfall *Kritische Schwachstellen in Microsoft Exchange*, S. 27). Viele davon waren nicht nur durch die Anfang März bekannt gewordenen Schwachstellen angreifbar, sondern auch durch bereits länger bekannte, für die seit geraumer Zeit *Patches* zur Verfügung standen. In der überwiegenden Zahl der Fälle betrafen diese Schwachstellen die Systeme von KMU.

Zur Stärkung der KMU in Deutschland ist in diesem Bereich aufgrund von erhöhtem staatlichen Interesse ein verstärktes Handeln dringend erforderlich. Dem trägt das BSI durch Ausbau seines Engagements für diese Zielgruppe Rechnung.

2.2.9 Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme

Im Zuge der Digitalisierung werden Geschäftsvorfälle heutzutage immer häufiger elektronisch erfasst. Die Nutzung unterschiedlichster Arten von Registrierkassen etwa prägt den Einzelhandel deutlich. Von der klassischen Kasse, über Tablets und Smartphones hin zu Kassen in Serverfarmen sind alle erdenklichen Typen vertreten. Dadurch haben sich die technischen Herausforderungen für die Steuerprüfung stark verändert, da nachträgliche Manipulation an elektronischen Aufzeichnungen ohne geeignete Schutzmaßnahmen kaum feststellbar sind.

Um solchen Manipulationen entgegenzuwirken, müssen elektronische Aufzeichnungssysteme nach Abgabenordnung und Kassensicherungsverordnung seit 2020 mit einer zertifizierten Technischen Sicherheitseinrichtung geschützt werden. Diese wird vom elektronischen Aufzeichnungssystem angesprochen, übernimmt die Absicherung der aufzuzeichnenden Daten und speichert die gesicherten Aufzeichnungen in einem einheitlichen Format. Dazu enthält die Technische Sicherheitseinrichtung ein Sicherheitsmodul, das gewährleistet, dass Aufzeichnungen nachträglich nicht unerkannt geändert, gelöscht oder erzeugt werden können.

Die gesetzliche Neuregelung fördert explizit eine technologieoffene Ausgestaltung der Technischen Sicherheitseinrichtung. Durch eine einheitliche digitale Schnittstelle wird die Integration in existierende und zukünftige Kassensysteme vereinfacht und die notwendige Interoperabilität im Rahmen der Steuerprüfung gewährleistet. Besondere Anforderungen an die physikalische Schnittstelle werden nicht gestellt, so dass übliche Standardschnittstellen, wie zum Beispiel USB, Ethernet und (micro-)SD-Karten, verwendet werden können. Zusätzlich zu den rein lokalen Sicherheitseinrichtungen sind von Beginn an durch eine optionale Client-Server-Architektur des Sicherheitsmoduls auch skalierbare Lösungen berücksichtigt worden, etwa zum Einsatz in Filialen oder als Onlinedienst ausgestaltet.

Die technischen Anforderungen und Prüfvorschriften an die Komponenten der Technischen Sicherheitseinrichtung werden vom BSI in Technischen Richtlinien und Schutzprofilen festgelegt.

Sieben verschiedene Technische Sicherheitseinrichtungen haben die Zertifizierung bereits erfolgreich bestanden und sind auf dem Markt verfügbar. Vier von ihnen lassen sich als USB-Sticks und (micro-)SD-Karten direkt in Kassen und Mobilgeräte einbinden. Drei weitere Lösungen können als sogenannte *Cloud*-TSE in Rechenzentren eingebunden werden.

2.2.10 IT-Sicherheitszertifizierung als Instrument für eine nachweislich sichere Digitalisierung

Die durch die COVID-19-Pandemie hervorgerufene Fokussierung auf Digitalisierungsthemen bringt die Notwendigkeit mit sich, Dienstleistungen und Produkten ein Mindestmaß an Informationssicherheit mitzugeben. Um Anbieter und Betreiber digitaler Lösungen zu unterstützen, bietet das BSI Zertifizierungsprogramme an, über die eine Organisation nachweisen kann, dass ein Produkt oder eine Dienstleistung definierten Sicherheitsanforderungen entspricht. Die unabhängige Prüfung durch das BSI schafft Vertrauen und weist Integrität, Vertraulichkeit und Authentizität transparent nach.

Die Produkt-Zertifizierung kann grundsätzlich von Herstellern oder Anbietern von IT-Produkten beantragt werden. Eine Prüfung ist nach den international anerkannten Common Criteria (CC), einer Technischen Richtlinie (TR) oder dem neuen Verfahren der Beschleunigten Sicherheitszertifizierung (BSZ) möglich. Die Produktzertifizierung nach CC oder TR bestätigt, dass eine Produktversion bestimmte funktionale und sicherheitstechnische Eigenschaften erfüllt, die in Schutzprofilen, Sicherheitsvorgaben oder Technischen Richtlinien spezifiziert sind. Die BSZ verfolgt einen penetrationstestgetriebenen Ansatz mit festen Evaluierungszeiträumen und geringem Dokumentationsaufwand, um eine Sicherheitsaussage zu tätigen.

Neben der Produktzertifizierung bietet das BSI als zweite elementare Säule die Zertifizierung von Managementsystemen für Informationssicherheit (ISMS) an. Diese ist an die weit verbreitete Zertifizierung nach ISO/IEC 27001 angelehnt und wird auf Basis des im BSI entwickelten IT-Grundschutzes durchgeführt. Auch im Bereich der Personenzertifizierung ist das BSI breit aufgestellt: Audi-

toren zu unterschiedlichen Fachthemen, IS-Revisoren und IT-Grundschutz-Berater sind nur einige der nachgefragten Zertifizierungen.

Aktuelle Herausforderungen

Im Juni 2019, mit Inkrafttreten des Cybersecurity Act (CSA), hat die Europäische Kommission den Grundstein für die europaweite Anerkennung und Harmonisierung von IT-Sicherheitszertifizierungen gelegt. Eine Herausforderung für das BSI ist, die hohen und etablierten Anforderungen aus nationalen Digitalisierungsprojekten, aber auch aus dem bisherigen Anerkennungsabkommen SOGIS-MRA, in das neue, EU-weite Schema zu überführen. Die nachfolgende Auflistung zeigt Beispiele für schon etablierte, aber auch neue Digitalisierungsprojekte der Bundesregierung und der EU, in denen eine Zertifizierung fest verankert ist: Digitalisierung des Gesundheitswesens, Hoheitliche Dokumente, Digitalisierung der Energiewende, Digitale Fahrtenschreiber, Digitale Signaturen und der Schutz vor Manipulation an digitalen Grundaufzeichnungen (Registrierkassen).

Zertifizierung in Zahlen

Im Berichtszeitraum hat das BSI im Bereich der Common Criteria insgesamt 69 Produkt-, 19 Standort- und 6 Schutzprofilzertifikate ausgestellt. Zusätzlich gab es 5 ALC Reevaluierungen und 21 CC-Maintenance-Verfahren.

Im internationalen Vergleich nimmt das BSI im Bereich der CC-Zertifizierung einen Spitzenplatz ein und ist je nach gewählter Vertrauenswürdigkeitsstufe des Zertifikats oder des Anwendungsbereichs immer unter den Top 3 Nationen mit den am meisten ausgestellten CC-Zertifikaten.

Außerdem wurden 77 Verfahren nach Technischen Richtlinien in 14 Prüfbereichen abgeschlossen, wobei 51 Erst- und Rezertifizierungen, 15 Maintenance-Verfahren sowie 11 Überwachungsaudits durchgeführt wurden.

Im Bereich des IT-Grundschutzes wurden im Berichtszeitraum insgesamt 87 Verfahren erfolgreich abgeschlossen, wovon 31 ISO 27001 Zertifikate auf Basis von IT-Grundschutz waren. Zusätzlich wurden 56 Überwachungsaudits durchgeführt. Die Beschleunigte Sicherheitszertifizierung befindet sich derzeit in der Pilotierung.

2.2.11 IT-Grundschutz: Lösungen für Informationssicherheit

Die vielfältigen und dynamischen Angriffe, die in Kapitel 1 beschrieben werden, verdeutlichen einmal mehr, wie wichtig ein ganzheitliches Vorgehen ist, um zu einem bedarfsgerechten Sicherheitsniveau für alle Geschäftsprozesse und der darin verarbeiteten Informationen in einer Institution zu gelangen. Als wirksamstes Vorgehen hat sich erwiesen, ein Managementsystem für Informationssicherheit (ISMS) nach IT-Grundschutz zu etablieren. Die Anwendung des IT-Grundschutzes trägt dazu bei, Gefährdungen zu erkennen, Risiken zu reduzieren und mit adäquaten Maßnahmen das Niveau der Informationssicherheit deutlich anzuheben.

Inzwischen können Unternehmen und Behörden auf die Expertise von über 100 ausgebildeten IT-Grundschutz-Beraterinnen und -Beratern zurückgreifen. Diese sind durch das BSI zertifiziert und können bei der Entwicklung von Sicherheitskonzepten unterstützen oder bei der Einführung eines ISMS begleiten. Wenn für die ersten Schritte zur Informationssicherheit personelle oder zeitliche Ressourcen knapp sind, kann ein IT-Grundschutz-Berater hier unterstützen und einen wichtigen Beitrag zur Prävention leisten. Im operativen Tagesgeschäft können die Expertinnen und Experten mit den zuständigen Mitarbeiterinnen und Mitarbeitern auf Basis des IT-Grundschutzes Maßnahmen definieren und im Betrieb umsetzen.

Im Krisenfall gut aufgestellt: Business Continuity Management

Die Bedeutung eines gut aufgestellten Business Continuity Managements (BCM) zeigt sich vor allem, wenn das Schutzziel Verfügbarkeit verletzt wird. Eine Vielzahl von Angriffen führte bei Institutionen zu Ausfällen kritischer Geschäftsprozesse. Besonders *Ransomware*-Angriffe haben sich zu einer ernsthaften Bedrohung entwickelt. Dies zeigt die Notwendigkeit, neben einem ISMS auch ein BCM zu etablieren, um in jeder Situation reaktionsfähig zu bleiben. So schaffen Institutionen nachhaltig *Resilienz*, auch im Not- oder Krisenfall. Aufgrund der Bedeutung des Themas bei der fortschreitenden Effizienzsteigerung und Abhängigkeit von funktionierenden Geschäftsprozessen, auch über Standorte hinweg, hat das BSI den BSI-Standard 100-4 einer grundlegenden Prüfung und Überarbeitung unterzogen. Der künftige Standard 200-4 legt schon im Titel den Fokus auf Business Continuity Management. Ziel eines BCM ist es sicherzustellen, dass der Geschäftsbetrieb selbst bei massiven Schadensereignissen nicht unterbrochen wird oder nach einem Ausfall in angemessener Zeit fortgeführt werden kann. So betrachtet BCM sowohl einen präventiven als auch einen reaktiven Ansatz. Die Etablierung eines ISMS sowie eines BCM sind im IT-Grundschutz als langfristige Prozesse angelegt mit klar verteilten Verantwortlichkeiten, Prozessen und Aufgaben für nachhaltige *Resilienz* in Unternehmen und Behörden.

2.2.12 IT-Sicherheit im Homeoffice

Die zum Teil sehr kurzfristigen Umstellungen auf Homeoffice zu Beginn der COVID-19-Pandemie bringen neue technische und organisatorische Herausforderungen mit sich. Das BSI hat frühzeitig konkrete Maßnahmen zur Absicherung des Homeoffice bereitgestellt. Gleichzeitig wurden die Herausforderungen der veränderten Arbeitswelt in der Umfrage IT-Sicherheit im Homeoffice unter besonderer Berücksichtigung der COVID-19-Pandemie untersucht.
Hier finden Sie die Ergebnisse der Umfrage:[u]

Technische und organisatorische Maßnahmen im Homeoffice

Obwohl Homeoffice aktuell und zukünftig eine maßgebliche Rolle in unserem Arbeitsalltag einnimmt, werden zu wenig technische und organisatorische Sicherheitsmaßnahmen getroffen, um das Homeoffice ausreichend gegen Cyber-Angriffe zu sichern. Besonders Kleinst- und Kleinunternehmen haben hier einen großen Nachholbedarf. Nur 66 Prozent der Umfrageteilnehmer setzten Virtual Private Network (*VPN*) ein. Ebenso hat lediglich knapp die Hälfte der befragten Unternehmen Mehr-Faktor-*Authentisierung* implementiert, und nur 38 Prozent der Unternehmen verwalten aktuell ihre mobilen Endgeräte (Handys, Tablets) zentral über Mobile Device Management (MDM). Viele Unternehmen scheinen aber zu verstehen, wie wichtig Awareness für Cyber- und Informationssicherheit im Unternehmen ist und dass ihre Mitarbeitenden als Sicherheitsfaktor Mensch ein zentraler Baustein ihrer IT-Sicherheitsstrategie sind. Immerhin 81 Prozent der Unternehmen haben vor und während der Pandemie in Awareness-Maßnahmen investiert und sensibilisieren ihre Mitarbeitenden. Schulungen alleine reichen aber nicht aus. Ebenso zentral ist das regelmäßige Üben von Cyber- bzw. IT-Notfällen. Hier zeigt sich ein großer Nachholbedarf. Nur 24 Prozent der befragten Unternehmen üben regelmäßig ihre Abläufe im Falle eines IT-Notfalls. Vor allem fällt auf, dass sich nur rund 50 Prozent der Umfrageteilnehmer an dem entscheidenden Leitgedanken für IT-Sicherheit im Unternehmen orientieren - nämlich, dass Cyber-Sicherheit Chefinnen- und Chefsache ist.

Bedrohungslage und IT-Budget

In der Zeit von Homeoffice aufgrund von COVID-19 mussten acht Prozent der Unternehmen aktiv auf Cyber-Angriffe reagieren. Hier bewerteten vor allem KMU den Schaden als schwerwiegend. Für Unternehmen mit weniger als 50 Beschäftigten hatte eine von vier Cyber-Attacken sogar schwere oder existenzbedrohende Folgen. Die Umfrage hat auch ergeben, dass bislang zu wenig investiert wird: Mehr als die Hälfte der Unternehmen (55 Prozent) investiert gerade einmal zehn Prozent oder weniger ihres IT-Budgets in Informationssicherheit. Das BSI empfiehlt, 20 Prozent der IT-Ausgaben für Cyber- und Informationssicherheit zu verwenden. Nur 16 Prozent der Unternehmen haben mit einer Erhöhung des Budgets für Informationssicherheit auf die Corona-Krise reagiert.

Unterstützungsangebot im Homeoffice

Das BSI hat schon frühzeitig Unterstützungsangebote für die Ad-hoc-Umstellung ins Homeoffice sowie Tipps für erste Sicherheitsmaßnahmen und eine Checkliste für die Unternehmensleitung bereitgestellt. Damit können Unternehmen das eigene Informationssicherheitsniveau schnell überprüfen und gegebenenfalls mit den bereitgestellten Angeboten anheben.

Während der Pandemie hat die Nutzung von Videokonferenzlösungen zugenommen. Hier hat das BSI das Kompendium zur Nutzung von Videokonferenzsystemen und einen Community Draft zu Mindeststandards von Videokonferenzlösungen entwickelt. Die Moderationskarten der Allianz für Cyber-Sicherheit unterstützen zusätzlich bei der virtuellen Kommunikation und haben sich bereits mehrfach als analoges Fallback-System als hilfreich erwiesen – beispielsweise bei einem Tonausfall. Das Homeoffice stellt auch einen Schwerpunkt der bundesweiten IT-Sicherheitskampagne #einfachaBSIchern dar.
Auf der Webseite des BSI sind wichtige Tipps und Hinweise zum sicheren Arbeiten zuhause zu finden.[v]

Abbildung 13: Einfache Maßnahmen für mehr IT-Sicherheit im Homeoffice
Quelle: BSI

2.2.13 Allianz für Cyber-Sicherheit

Die Allianz für Cyber-Sicherheit (ACS) ist die größte öffentlich-private Kooperationsplattform für Cyber-Sicherheit mit der Wirtschaft in Europa. Dem stetig wachsenden Bedarf an Informationen trägt die Initiative sowohl mit bewährten als auch neuen digitalen Formaten, wie dem Cyber-Sicherheits-Web-Talk und dem ACS-Podcast CYBERSNACS, Rechnung. Hier gelangen Sie zum Podcast:[w]

Getreu dem Motto „Netzwerke schützen Netzwerke“ bietet die ACS im Schulterschluss mit über 150 Partnern und 100 Multiplikatoren aus der Wirtschaft zahlreiche Informations- und Austauschangebote an: Unternehmen haben im Rahmen von Partnerangeboten wie (Online-)Seminaren, Schulungen und Publikationen zu verschiedenen Fachthemen die Möglichkeit, ihre Cyber-Sicherheitsexpertise mit dem Netzwerk zu teilen und zu erweitern. Ein weiterer wichtiger Informationskanal ist der Newsletter, der regelmäßig mehr als 7.000 Abonnentinnen und Abonnenten erreicht. Mit dem Sondernewsletter zu den Microsoft-Exchange-Lücken konnte die Zielgruppe Wirtschaft auch auf diesem Kanal zeitnah erreicht werden.

Seit April 2021 verzeichnet die Initiative über 5.000 Teilnehmer – Tendenz weiterhin steigend. Die ACS richtet sich an alle IT-anwendenden Unternehmen und Organisationen in Deutschland.

2.2.14 Sonstige Lösungen / Angebote für die Wirtschaft

BAFA Ausfuhrkontrolle

Das BSI unterstützt das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) bei Anträgen auf Ausfuhr- und Verbringungsgenehmigung. Dabei stellt das Außenwirtschaftsgesetz (AWG), die Außenwirtschaftsverordnung (AWV) und die EG-Dual-Use-Verordnung die gesetzliche Grundlage der Kontrollbefugnisse insgesamt dar. Der Schwerpunkt dieser vom BSI erbrachten Unterstützungsleistung liegt auf dem Gebiet der Krypto-Exportkontrolle und gliedert sich im Einzelnen in folgende Themenbereiche:

1. die Unterstützung aber auch der (Selbst-)Schutz der deutschen Krypto-Industrie,

2. Schutz zugelassener IT-Sicherheitsprodukte und Komponenten wie Smartcards etc. und Technologie (vor Re-Engineering Manipulation etc.).

Das BSI hat im Berichtzeitraum 96 Anträge bearbeitet, die einen Gesamtumsatz von rund 70 Mio. € darstellten.

Investitionsprüfung

Das BSI wird vom Bundesministerium des Innern, für Bau und Heimat (BMI) bei der Prüfung von ausländischen Direktinvestitionen in inländische Unternehmen nach §§ 4ff. des Außenwirtschaftsgesetzes (AWG) bzw. §§ 55ff. und §§ 60ff. der Außenwirtschaftsverordnung (AWV) beteiligt. Die seit 2015 zu verzeichnende enorme Zunahme von Prüfvorgängen setzte sich auch 2020 weiter fort, und für 2021 wird eine weitere Steigerung erwartet. Der Grund hierfür liegt in der erweiterten rechtlichen Prüfgrundlage sowie der erhöhten öffentlichen Sensibilität hinsichtlich handelspolitischer Auswirkungen auf die nationale Sicherheitslage und technologische Souveränität.

Auf Initiative von Deutschland, Frankreich und Italien wurde auf europäischer Ebene die EU-Screening-Verordnung 2019/452 mit dem Ziel vorangetrieben, Direktinvestitionen durch Unionsfremde effektiver überprüfen zu können und einen europäischen Regelungsrahmen zu setzen. Am 17. Juli 2020 trat nach der parlamentarischen Befassung des Bundestages zur Umsetzung der EU-VO 452/2019 das novellierte AWG in Kraft, die zugehörigen 16. und 17. Änderungsnovellen der AWV wurden in 2020 und 2021 verabschiedet.

Wesentliche Änderungen der EU-Screening-VO bzw. des novellierten deutschen Rechtsrahmens sind insbesondere:

- die Absenkung der Begründungsschwelle für Eingriffe auf nun voraussichtliche Beeinträchtigung statt einer Gefährdung der öffentlichen Ordnung oder Sicherheit,

- die neu eingeführte Meldepflicht im Bereich von Schlüsselindustrien,

- die in vielen Bereichen folgende Absenkung der Schwellwerte der Beteiligungshöhe von 25 auf 20 bzw. 10 Prozent,

- die Berücksichtigung von atypischen Übernahmen / Beherrschungsverhältnissen,

- die ausdrückliche Nennung zu berücksichtigender Faktoren wie z. B. staatlich gesteuerte Übernahmen sowie

- die Etablierung eines EU-Kooperationsmechanismus.

Diese erhebliche Erweiterung der Prüfgrundlage und auch die neuen Fallgruppen, die die Zuständigkeit des BSI betreffen (wie z. B. IT-Sicherheitsunternehmen) werden zu einem weiteren Anstieg der durch das BSI zu begleitenden Investitionsvorhaben führen – wobei bereits in den zurückliegenden Jahren ein signifikanter Anstieg der Fallzahlen zu verzeichnen war. Wurden 2020 beim federführenden BMWi über 180 Fälle registriert, bedeutet das gegenüber 2016 mehr als eine Vervierfachung der Fallzahlen – wobei sich die Effekte der neuen Rechtslage hier noch kaum auswirken und für 2021 ein noch stärkerer Anstieg erwartet wird.

Das BSI wird bei Verfahren mit einem möglichen Cyber-Sicherheitsbezug durch das BMI zur Gefahrenbewertung bzw. -abwehr beteiligt und erhält hierzu entsprechende Prüfaufträge (Erlasse). Bei komplexen oder besonders sensiblen Erwerbsvorgängen, bei denen beispielsweise Unterlagen nachgefordert, tiefere Analysen zur Gefahrenbewertung

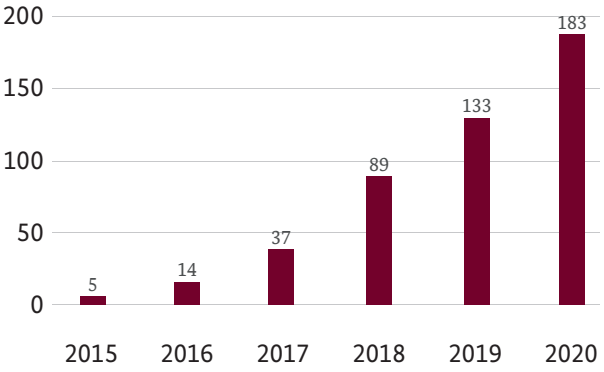


Abbildung 14: Entwicklungen der Prüfaufträge / Erlasse im Rahmen von AWG-Verfahren
Quelle: BSI

oder auch Verhandlungen mit den Erwerbsparteien und anderen potenziell betroffenen Stellen durchgeführt oder Vertragsverhandlungen bzgl. etwaiger Auflagen entwickelt werden müssen, können die verschiedenen Verfahrensschritte zu jeweils neuen Prüfaufträgen für das BSI führen.

Unter Berücksichtigung der jeweiligen wirtschaftlichen, rechtlichen und technologischen Situation des Erwerbers und der Zielgesellschaft analysiert und bewertet das BSI mögliche Gefährdungssituationen und erarbeitet Positions- und Lösungsvorschläge zur Gefahrenabwehr. Mögliche IT-Sicherheitsgefährdungen können u. a. im Abfluss von sensiblen Informationen an unbefugte Dritte, dem Einbau oder der Verheimlichung von Schwachstellen, der Gefährdung von kritischen Infrastrukturen oder dem Verlust von Technologieträgern im Bereich von Schlüsseltechnologien liegen. Der auch durch die EU-Screening-VO betonte Schutz von Schlüsseltechnologien, wie im Bereich der Halbleiter, Telekommunikation, Quantenmechanik oder der Künstlichen Intelligenz, wird 2021 und darüber hinaus in den Investitionsprüfverfahren eine große und neue Herausforderung darstellen. Da diese Schlüsseltechnologien u. a. auch den IT-Bereich betreffen, fällt dies zum großen Teil in die Zuständigkeit des BSI.

Sicherheit von Cloud-Diensten

Der BSI-Kriterienkatalog für *Cloud Computing* C5 wurde im letzten Jahr überarbeitet, aktualisiert und als BSI C5:2020 veröffentlicht (vgl. *Quellenverzeichnis*[61]). Es gibt bereits erste Testate, die entsprechend ausgestellt wurden, und die Gesamtzahl der testierten *Cloud*-Dienste wächst weiterhin, genauso wie die Anzahl der Wirtschaftsprüferinnen und -prüfer, die Testate nach dem C5 ausstellen.

Die Sicherheit von *Cloud*-Diensten zu bewerten, ist kein einfaches Unterfangen: Die Serviceangebote verändern sich ständig, bauen auf andere Dienste auf, und daher ist nie ganz klar, welche Daten damit verarbeitet werden. Das BSI C5-Testat besteht daher aus einem Report (nach dem Wirtschaftsprüfungsstandard ISAE300), der es den Nutzenden erlaubt, sich selbst ein Bild von der Sicherheit des *Cloud*-Dienstes und der Vertrauenswürdigkeit des anbietenden Unternehmens zu machen. Da diese Reports sehr umfangreich sind und unterschiedlich aufgebaut sein können, hat das BSI zur Unterstützung einen Auswertungsleitfaden (vgl. *Quellenverzeichnis*[62]) veröffentlicht. Dieses Dokument beschreibt einen strukturierten Weg, die Informationen zu extrahieren, die für *Cloud*-Nutzende notwendig sind. Darauf basierend kann dann eine fundierte Entscheidung getroffen werden, ob die Sicherheit des *Cloud*-Dienstes den gewünschten Anforderungen im Anwendungsfall genügt.

EU *Cloud*-Zertifizierung und BSI C5:2020

Im Rahmen des Cybersecurity Acts der EU wird momentan ein *Cloud*-Zertifizierungsschema erstellt (EUCS, EU *Cloud* Services Scheme). In dem schon mehr als zwei Jahre dauernden Prozess hat das BSI aktiv mitgewirkt und konnte dabei wesentliche Teile des C5 einbringen. Beispielsweise basieren die Security Objectives and Requirements for *Cloud* Services des Zertifizierungsschemas zum Großteil auf den Sicherheitskriterien des BSI C5:2020. Auch viele weitere Elemente, wie die Wirksamkeitsprüfung von Kontrollen, Einbindung von Subdienstleistern sowie die Prüfmethodik, konnten in den Entwurf erfolgreich eingebracht werden. Sie stammen aus den Wirtschaftsprüfungsstandards, auf denen der BSI C5 aufbaut und die für *Cloud* Service eine breite Anwendung finden. Eine der großen verbleibenden Herausforderungen im Standardisierungsprozess ist, diese Prüfmethodik in ein Zertifizierungsschema zu übernehmen, das den Regelungen der Norm ISO 17065 Konformitätsbewertung - Anforderungen an Stellen, die Produkte, Prozesse und Dienstleistungen zertifizieren entspricht. Diese Norm wird durch den EU Cybersecurity Act vorgegeben. Da Anforderungen des EU Cybersecurity Acts bereits in den BSI C5:2020 eingefügt wurden, bedeutet dies, dass die nach C5:2020 testierten *Cloud*-Dienste dem momentanen Entwurf des EUCS so nahekommen wie sonst kein anderer Sicherheitsnachweis am Markt.

Mindeststandard für die Bundesverwaltung

Wenn Bundesbehörden Dienste aus der Public *Cloud* nutzen möchten, gilt für sie der BSI-Mindeststandard Nutzung externer *Cloud*-Dienste (vgl. *Quellenverzeichnis*[63]). Dieser beschreibt die notwendigen Schritte bei der Auswahl von *Cloud*-Diensten. Das BSI unterstützt Behörden dabei fachlich, sodass diese die Vorteile des *Cloud Computing* sicher nutzen können.

2.3 Staat und Verwaltung

Eine Kernaufgabe des BSI ist die Abwehr von Cyber-Angriffen auf Regierungsnetze und die Bundesverwaltung. Einrichtungen in Bund, Ländern und anderen Verwaltungssegmenten profitieren zudem vom modernisierten IT-Grundschutz, von Mindeststandards und Angeboten im Bereich der Informationssicherheitsberatung, Zertifizierung und Zulassung sowie von der Unterstützung bei IT-Sicherheitsvorfällen durch das *CERT-Bund*, durch mobile Einsatzteams (MIRT) oder das Nationale Cyber-Abwehrzentrum. Zentraler Ansprechpartner für Länder und Kommunen ist das nationale Verbindungswesen mit Verbindungsstellen in Hamburg, Berlin, Bonn, Wiesbaden und Stuttgart.

2.3.1 Die Gefährdungslage in der Bundesverwaltung

Die Regierungsnetze sind Tag für Tag Angriffen aus dem Cyber-Raum ausgesetzt. Dabei handelt es sich sowohl um ungezielte Massenangriffe als auch um gezielte Angriffe gegen die Behörden des Bundes.

Die Angreifer setzen dabei überwiegend auf Angriffe mittels Schadprogrammen. Diese werden einerseits als E-Mail-Anhänge verbreitet, andererseits hinter Download-Links in E-Mails, Social-Media-Accounts oder auf Webseiten versteckt (vgl. Kapitel *Schadprogramme*, Seite 10). Grundsätzlich basiert das Vorgehen der Angreifer darauf, dass Nutzerinnen und Nutzer mittels Social-Engineering-Methoden zum Klicken verleitet werden. In der Folge wird versucht, ein Schadprogramm auf dem System zu installieren. Das BSI setzt verschiedene, sich gegenseitig ergänzende Maßnahmen zum Schutz der Regierungsnetze vor diesen Angriffen ein.

Durch Webfilter werden Webseiten mit Schadcode für Zugriffe aus der Bundesverwaltung zentral gesperrt und somit das Nachladen von Schadprogrammen unterbunden. Im aktuellen Berichtszeitraum mussten insgesamt knapp 74.000 *maliziöse* Webseiten zusätzlich gesperrt werden. Das war ein Zuwachs von 42 Prozent gegenüber dem vergangenen Berichtszeitraum. Wie der Abwehr-Index über die neuen Sperrungen zeigt, haben Angreifer besonders im September sowie im November des vergangenen Jahres viele neue Webseiten mit Schadcode geschaltet. Allein im September 2020 mussten dreimal so viele *maliziöse* Webseiten gesperrt werden, wie noch im Durchschnitt des Jahres 2018 (vgl. *Abbildung 15*)

Wie schon in früheren Jahren waren auch im Jahr 2020 im Spätsommer und im Herbst Angriffswellen mit Schadprogrammen via E-Mail zu beobachten. Diese Wellen fielen im Vergleich zum Vorjahr sehr stark aus. Der Abwehr-Index über die Schadprogramm-Angriffe auf die Bundesverwaltung lag im Durchschnitt des Berichtszeitraums bei durchschnittlich 94 Punkten, dabei waren jedoch starke Schwankungen zu verzeichnen. Während der Angriffswellen von August bis November 2020 erreichte der Indikator zeitweise fast 180 Punkte (vgl. *Abbildung 16,* Seite 70). Bei der im März 2021 detektierten Angriffswelle handelte es sich um Bounce. Angreifer hatten E-Mail-Adressen der Bundesverwaltung als gefälschte Absender-Adressen in einer *Malware-Spam*-Kampagne angegeben, um die E-Mails vertrauenswürdig erscheinen zu lassen. Die angegriffenen E-Mail-Adressen existierten jedoch zum großen Teil nicht und wurden deshalb von den Mail-Servern mit einer Fehlermeldung „zurückgeschickt", und zwar an die von den Angreifern angegebenen Absender-Adressen aus der Bundesverwaltung. Da die E-Mail-Anhänge schadcodebehaftet waren, wurden sie als *Malware*-Angriffe detektiert und zentral abgewehrt.

Durchschnittlich wurden im Berichtszeitraum pro Monat rund 44.000 E-Mails mit Schadprogrammen mittels automatisierter Antivirus-Schutzmaßnahmen in den Regierungsnetzen abgefangen, bevor sie die Postfächer

Index über die neuen Sperrungen *maliziöser* Webseiten

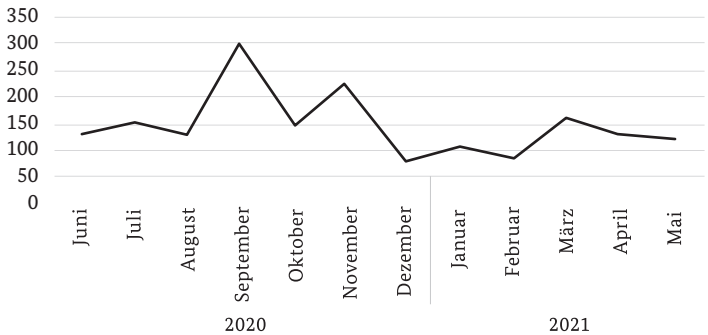
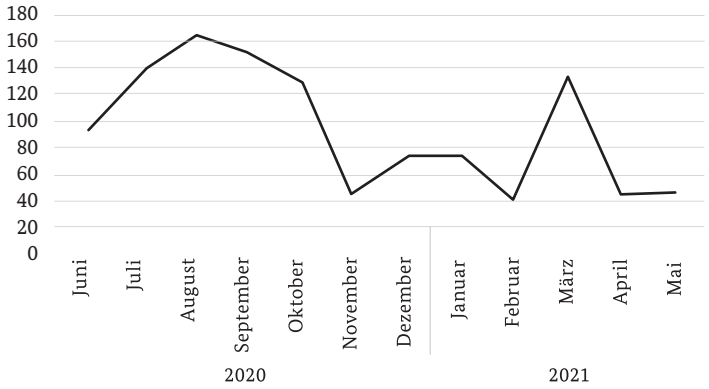


Abbildung 15: Index über die neuen Sperrungen *maliziöser* Webseiten
Quelle: BSI-Auswertung eigener Quellen

Index über die Schadprogramm-Angriffe auf die Bundesverwaltung[III)]

Abbildung 16: Index über die Schadprogramm-Angriffe auf die Bundesverwaltung
Quelle: BSI-Auswertung eigener Quellen



[III)] Ohne Behörden, die nicht an den zentralen Schutzmaßnahmen des BSI teilnehmen.

der Empfängerinnen und Empfänger erreichten. Eigens durch das BSI erstellte Antivirus-Signaturen trugen mit durchschnittlich rund 9.700 abgefangenen E-Mails pro Monat erheblich zum Gesamtergebnis dieser Schutzmaßnahme bei.

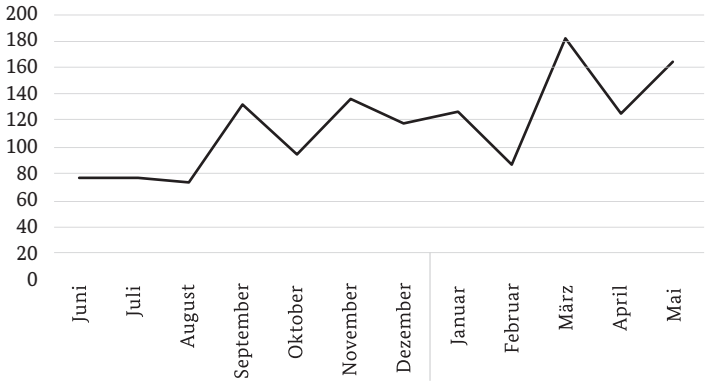
Nachgelagert zu den automatisierten Antivirus-Schutzmaßnahmen betreibt das BSI ein weiteres System zur Detektion von Schadprogrammen im Datenverkehr der Regierungsnetze. Die Aufgabe des Systems ist das Aufspüren von gezielten Angriffen und neuartigen Schadprogramm-Varianten. Dazu wird eine Kombination aus automatisierten Testverfahren und manueller Analyse genutzt. Mit diesem System gelang es den Analysten des BSI, durchschnittlich weitere 5.100 Angriffe pro Monat zu detektieren. Diese Angriffe waren nicht durch die kommerziellen Produkte der oben genannten automatisierten Antivirus-Schutzmaßnahmen erkannt oder blockiert worden.

Ergänzend wird die Sicherheit der Regierungsnetze mit einem zentralen Schutz vor unerwünschten *Spam*-E-Mails erhöht. Diese Maßnahme wirkt nicht nur gegen unerwünschte Werbe-E-Mails. Auch Cyber-Angriffe, wie *Phishing*-E-Mails, werden damit erkannt.

Die *Spam*-Quote, also der Anteil unerwünschter E-Mails an allen eingegangenen E-Mails lag im Berichtszeitraum bei durchschnittlich 58 Prozent.

Spam-Mail-Index für die Bundesverwaltung[III)]

Abbildung 17: *Spam*-Mail-Index
Quelle: BSI-Auswertung eigener Quellen



[III)] Ohne Behörden, die nicht an den zentralen Schutzmaßnahmen des BSI teilnehmen.

2.3.2 Nationales Cyber-Abwehrzentrum

Das Nationale Cyber-Abwehrzentrum (Cyber-AZ) ist auf Bundesebene die Informations- und Kooperationsplattform zum operativen Austausch zwischen Behörden mit (unterschiedlichen) Zuständigkeiten im Bereich Cyber-Sicherheit. Als Kernbehörden arbeiten darin das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), das Bundesamt für den Militärischen Abschirmdienst (BAMAD), das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Bundesamt für Verfassungsschutz (BfV), das Bundeskriminalamt (BKA), der Bundesnachrichtendienst (BND), das Bundespolizeipräsidium (BPOLP) sowie das Kommando Cyber- und Informationsraum (KdoCIR) der Bundeswehr zusammen. Weitere staatliche Einrichtungen sind als assoziierte Stellen beteiligt. Darüber hinaus werden zusätzliche

Partner aus verschiedenen Bereichen jeweils anlassbezogen eingebunden. Auf Ebene der Bundesländer sind das beispielsweise die Länder-*CERTs*, Landeskriminalämter, Landesämter für Verfassungsschutz und perspektivisch auch Staatsanwaltschaften. Das BSI ist mit mehreren Verbindungsbeamtinnen und -beamten im Cyber-AZ vertreten und stellt zudem als gastgebende Behörde Personal für die Geschäftsstelle des Cyber-AZ, die Räumlichkeiten sowie die gemeinsame IT-Infrastruktur am Standort in Bonn zur Verfügung.

Im Cyber-AZ tauschen sich die beteiligten Einrichtungen über cyber-sicherheitsrelevante Informationen sowie über laufende und geplante Maßnahmen aus. Dabei folgt das Cyber-AZ einem ganzheitlichen Ansatz, der verschiedene Arten von Gefährdungen im und aus dem Cyber-Raum im Blick hat, darunter Spionage, Sabotage, Terrorismus und Kriminalität.

Einen wichtigen Tätigkeitsbereich im Cyber-AZ bildet neben der Lagebeobachtung die behördenübergreifende Koordination bei der operativen Bearbeitung konkreter Vorfälle. Die Bearbeitung selbst wird dann durch die Fachreferate der beteiligten Behörden in deren jeweiligem Zuständigkeitsbereich geleistet. Erkenntnisse und Ergebnisse werden fortlaufend im Cyber-AZ zusammengeführt, bewertet und an die entsprechenden Stellen berichtet.

Durch die verstärkte Verlagerung vieler Aktivitäten ins Internet während der COVID-19-Pandemie lag im Berichtszeitraum ein besonderer Schwerpunkt auf der gemeinsamen Beurteilung der Entwicklung der Cyber-Sicherheitslage und der Koordination von Maßnahmen zum Schutz gefährdeter systemrelevanter Einrichtungen. Dazu zählen insbesondere Unternehmen aus dem Pharmasektor und Organisationen aus dem medizinischen Bereich (vgl. Kapitel *Gefährdungen der Cyber-Sicherheit durch die COVID-19-Pandemie*, Seite 38). Im Rahmen der neu gegründeten Arbeitsgruppe Zukunftsbild des Cyber-AZ fand im vergangenen Jahr eine umfassende Weiterentwicklung in Bezug auf die behördliche Zusammenarbeit statt.

2.3.3 Computer Emergency Response Team für Bundesbehörden

Das *Computer Emergency Response Team* für Bundesbehörden (*CERT-Bund*) wurde ursprünglich als internes Notfallteam der Bundesverwaltung gegründet, um bei IT-Sicherheitsvorfällen in den entsprechenden Behörden diese bei deren Bewältigung zu unterstützen. Schnell wurde jedoch deutlich, dass die zunehmende Digitalisierung der Gesellschaft und die damit einhergehende Verflechtung der Informations- und Kommunikationstechnik einen breiteren Ansatz erfordern. Mit der kontinuierlichen gesetzlichen Aufgabenerweiterung des BSI hat sich auch die Zuständigkeit des *CERT-Bund* auf weitere Zielgruppen ausgeweitet. Besonders hervorzuheben sind die Kritischen Infrastrukturen. Aber auch für KMU sowie für die Öffentlichkeit werden Dienstleistungen bereitgestellt.

Im Berichtszeitraum wurden rund 70 IT-Sicherheitsvorfälle bearbeitet. In zehn Fällen rückte ein MIRT des BSI aus, um Betroffene vor Ort unterstützen und beraten zu können.

Zudem wurden über das Portal des Warn- und Informationsdienstes (WID) vom *CERT-Bund* des BSI sowie dem ebenfalls vom BSI betreuten Bürger-*CERT* im Berichtszeitraum etwa 1.050 Einzel- und Sammelmeldungen über Schwachstellen bereitgestellt (ohne Update-Meldungen). Weiterhin wurden etwa 40 Sachverhalte als besonders relevant für einzelne Zielgruppen eingestuft, die dann eine Cyber-Sicherheitswarnung erhalten haben.

In einzelnen Fällen unterstützt das BSI Sicherheitsforscherinnen und -forscher bzw. Entdeckerinnen und Entdecker von Schwachstellen sowie die Hersteller bei der Behebung von Schwachstellen. Wird eine solche in einem Produkt gefunden, stellt deren unkoordinierte Veröffentlichung eine besondere Bedrohung dar, da Angreifer oftmals erst durch die Veröffentlichung einer Schwachstelle auf die Angreifbarkeit von Systemen aufmerksam werden.

Im Berichtszeitraum hat das BSI 25 von Externen gemeldete Coordinated-Vulnerability-Disclosure-Fälle unterstützt und weitere im Rahmen von Sicherheitsstudien des BSI detektierte Schwachstellen an Hersteller gemeldet. Dazu gehörten unter anderem Schwachstellen in verschiedenen Büroanwendungen, Energiemess- sowie industriellen Steuerungssystemen (Smart Meter, Industrial Control Systems), in Medizingeräten und in Verwaltungs- und Informationssoftware des Gesundheitswesens.

Nach den Erfahrungen des BSI sind bislang wenige Hersteller darauf vorbereitet, CVD-Prozesse selbstständig durchzuführen. Oftmals ist bereits die Kontaktaufnahme zur verantwortlichen Ansprechpartnerin bzw. zum verantwortlichen Ansprechpartner innerhalb eines betroffenen Unternehmens ein schwieriges Unterfangen. Gleichzeitig werden mehr und mehr CVD-Prozesse durchlaufen, bei denen die Zahl der betroffenen Hersteller aufgrund einer zunehmenden Integration externer Softwarekomponenten vergleichsweise hoch ist. Koordinierende Stellen, wie das BSI, unterstützen Hersteller und Sicherheitsforschung regelmäßig bei der Durchführung, indem sie die beteiligten Parteien als neutrale Dritte durch den Prozess leiten. Das Vorgehen gemäß CVD beruht weitestgehend auf

einem kooperativen Ansatz. Den betroffenen Herstellern wird üblicherweise eine Frist vor der Veröffentlichung eingeräumt. Für eine erfolgreiche Reaktion auf eine gemeldete Sicherheitslücke innerhalb der Frist müssen insbesondere seitens des Herstellers Vorbereitungen getroffen werden. So sind bspw. benötigte Kontaktdaten zu veröffentlichen, Analyse- und Reaktionsprozesse vorzubereiten und letztlich eine effektive Information der Nutzerinnen und Nutzer zu gewährleisten (vgl. Infokasten *Common Security Advisory Framework (CSAF)*. Darüber hinaus empfiehlt das BSI Anbietern die Veröffentlichung einer unternehmensspezifischen CVD-Policy. Eine solche Richtlinie schafft Transparenz und veranschaulicht, ähnlich wie ein Bug-Bounty-Programm, den Rahmen für das Melden von Schwachstellen. Um sich organisatorisch besser auf die Handhabung von Schwachstellen vorbereiten zu können, hat das BSI ein Dokument mit Empfehlungen veröffentlicht:[x)]

Einen regelmäßigen Service für Internetprovider und Netzbetreiber stellen die *CERT-Bund*-Reports dar. Diese informieren erstens über Systeme, die mit hoher Wahrscheinlichkeit mit einem Schadprogramm infiziert sind (vgl. Kapitel *Botnetze*, Seite 19), zweitens über Systeme, die kritische Sicherheitslücken enthalten (vgl. Vorfall *Kritische Schwachstellen in MS Exchange*, Seite 27) und drittens über Systeme, die offen aus dem Internet erreichbar sind oder offen konfigurierte Server-Dienste aufweisen, die ggf. für Angriffe missbraucht werden können (vgl. Kapitel *Schadprogramme und Daten-Leaks*, Seite 25). Aufgrund der gewaltigen Anzahl solcher Systeme werden die Reports automatisiert erstellt. Im Berichtszeitraum wurden durchschnittlich täglich rund 9.100 solcher Reports versendet.

Insgesamt wurden so im gesamten Berichtszeitraum unter anderem rund 14.8 Millionen Schadprogramm-Infektionen deutscher Systeme an die Netzbetreiber gemeldet.[**]

Mit all seinen Facetten leistet *CERT-Bund* damit einen wichtigen Beitrag zur sicheren Digitalisierung in Deutschland.

Common Security Advisory Framework (CSAF)

Eine gemeldete und behobene Schwachstelle ist erst der Anfang des Schwachstellen-Behandlungsprozesses auf Betreiberseite. Um als Anwenderin oder Anwender vor der Schwachstelle geschützt zu sein, muss das entsprechende Update installiert werden. Da die Installation von Updates weitreichende Folgen haben kann, ist eine vorherige Risikobetrachtung sinnvoll. Um diese durchführen zu können, müssen den Anwenderinnen und Anwendern zeitnah und effizient alle relevanten Informationen zu der Schwachstelle bereitgestellt werden. Bislang werden dazu menschenlesbare Sicherheitsinformationen, so genannte Security Advisories, von den Herstellern oder den koordinierenden Stellen veröffentlicht.

Um die Risiken für ihre IT-Infrastruktur und die eingesetzten Produkte bewerten zu können, müssen Betreiber diese Security Advisories sichten. Dabei ist die Recherche von neu veröffentlichten Advisories und die Evaluierung, ob diese für sie relevant sind, regelmäßig mit hohem zeitlichen und personellen Aufwand verbunden. Dies begründet sich darin, dass zum einen Hersteller und andere veröffentlichende Stellen die unterschiedlichsten Notifikationswege für ihre Kundinnen und Kunden bzw. die Öffentlichkeit verwenden. So werden E-Mail-Benachrichtigungen teilweise verzögert versandt oder es existiert ein RSS Feed, der abonniert werden muss oder neue Advisories erscheinen lediglich auf einer (ggf. geschützten) Webseite, die manuell abgerufen werden muss. Zum anderen veröffentlichen immer mehr Stellen eine steigende Anzahl an Security Advisories. Darüber hinaus ist die Prüfung, insbesondere, ob die in den Advisories referenzierten Produkte in dem zu verantwortenden Bereich überhaupt eingesetzt werden, in der Regel nicht trivial.

Da sich Security Advisories verschiedener Quellen hinsichtlich Dateiformat, Strukturierung und Qualität der Information sowie Formatierung meist unterscheiden, ist eine automatisierte Verarbeitung nicht oder nur eingeschränkt möglich. Die manuelle Verarbeitung hingegen bindet gut ausgebildete Fachkräfte an triviale Aufgaben. Zudem skaliert das bisherige Vorgehen bei der steigenden Anzahl an Security Advisories nicht, d. h. bei gleichbleibender Personalkapazität müssen immer mehr und immer komplexere Advisories analysiert werden. Daher wird diese wichtige Informationsquelle durch die Betreiber oftmals nicht ständig oder regelmäßig ausgewertet, sondern nur anlassbezogen, beispielsweise nach medialer Berichterstattung oder Hinweisen des BSI.

** Enthalten waren hier wie auch in den Jahren zuvor Mehrfachmeldungen von noch nicht bereinigten Systemen.

Zusammen mit nationalen und internationalen Partnern arbeitet das BSI deshalb an einer Lösung, Anwenderinnen und Anwendern das Auffinden sowie die Bewertung und Umsetzung von Security Advisories zu erleichtern. Das maschinell verarbeitbare Format für Security Advisories, das sogenannte Common Security Advisory Framework (CSAF) 2.0, wird einen entscheidenden Beitrag dazu leisten, dass Unternehmen den Überblick behalten und ihre Anlagen absichern können. Die Security Advisories können dabei automatisiert von den Herstellern abgerufen und mit der eigenen Inventardatenbank abgeglichen werden. Das erste Tool zum Erstellen von CSAF-Dokumenten (Secvisogram) hat das BSI bereits auf seiner GitHub-Seite veröffentlicht (https://secvisogram.github.io). Das BSI trägt mit diesen Aktivitäten dazu bei, die Informationssicherheit in den Unternehmen zu erhöhen und die Digitalisierung in Deutschland erfolgreich zu gestalten.

2.3.4 IT-Konsolidierung Bund: Neuer Informationssicherheitsbeauftragter

Mit dem seit 2015 laufenden Großprojekt IT-Konsolidierung Bund zielt die Bundesregierung darauf ab, die gemeinsame Informationstechnik und IT-Beschaffungen des Bundes bei wenigen zentralen Dienstleistern zu bündeln. Von Anfang an begleitete das BSI das Projekt insbesondere durch Beratung der Beteiligten und Mitwirkung in Gremien.

Mit dem Beschluss der Informationssicherheitsrichtlinie IT-Konsolidierung Bund am 10. Dezember 2020 durch den Lenkungsausschuss IT-Konsolidierung Bund des IT-Rats wurde eine wesentliche Anforderung des UP Bund 2017 umgesetzt. Die Richtlinie wurde 2020 unter Federführung des BSI als Cyber-Sicherheitsbehörde des Bundes gemeinsam mit dem Bundesministerium des Innern, für Bau und Heimat, dem Bundesministerium der Finanzen sowie dem Netzdienstleister BDBOS und dem zentralen IT-Dienstleister ITZBund erstellt.

Einen Tag nach dem Beschluss hat das BSI Christoph Lauffer zum Informationssicherheitsbeauftragten für die IT-Konsolidierung Bund (ISB ITKB) bestellt und Sven Schneider zu seinem ständigen Vertreter. Aufgabe des Informationssicherheitsbeauftragten ist, die verschiedenen Informationssicherheitsaktivitäten an zentraler Stelle zu koordinieren und die bestehenden Informationssicherheitsmanagementsysteme zu verzahnen, um ein angemessenes Informationssicherheitsniveau in der IT-Konsolidierung Bund zu erreichen. Ein Verbundrisikomanagement schafft Transparenz bezüglich der Cyber-Risiken und ermöglicht so die laufende Überwachung und Verbesserung des Informationssicherheitsniveaus der konsolidierten IT.

2.3.5 Nationales Verbindungswesen

Die Gestaltung der Informationssicherheit in der Digitalisierung kann nur gemeinsam von Bund und Ländern zum Erfolg geführt werden. Deshalb hat das BSI seine Unterstützungsmöglichkeiten für die Bundesländer ausgebaut und fördert die Zusammenarbeit zwischen Bund und Ländern auf verschiedenen Ebenen. Ziel dieser verstärkten Zusammenarbeit ist die Erhöhung des Cyber-Sicherheitsniveaus in Deutschland.

Das nationale Verbindungswesen mit seinen Verbindungsstellen in Berlin, Bonn, Hamburg, Stuttgart und Wiesbaden erleichtert mit seinen direkten Ansprechpartnern für alle 16 Bundesländer den Austausch erheblich und trägt so zu einer verstärkten Zusammenarbeit bei. Über diese Verbindungsstellen werden die Produkte und Dienstleistungen des BSI für die Zielgruppen Staat, Wirtschaft und Gesellschaft und somit das Thema Informationssicherheit in die Fläche getragen.

Die enge Zusammenarbeit zwischen Bund und Ländern spiegelt sich darin wider, dass in 2021 erste Kooperationsvereinbarungen mit Ländern geschlossen werden. Auf dieser Basis werden konkrete Kooperationsprojekte umgesetzt, die das Cyber-Sicherheitsniveau in Bund und Ländern maßgeblich erhöhen.

2.3.6 Realisierung Umsetzungsplan Bund (UP Bund)

Der Umsetzungsplan Bund (UP Bund) ist die Leitlinie für Informationssicherheit in der Bundesverwaltung. Übergeordnetes Ziel des UP Bund ist die kontinuierliche Verbesserung der Informationssicherheit in der Bundesverwaltung durch Monitoring und gezielte, ressortübergreifende Steuerung. Die Realisierung des UP Bund wird daher jährlich evaluiert. Nach Inkrafttreten des neuen UP Bund 2017 wurde die Erhebung auf Basis eines prozessorientierten Ansatzes neu konzipiert und im vergangenen Jahr zum zweiten Mal durchgeführt.

Mit Hilfe der gewählten Reifegradmethodik konnten konkrete Maßnahmen identifiziert und priorisiert in Berichtsform dargestellt werden, um die Informations-

sicherheit in Einrichtungen und Ressorts effektiv und effizient zu erhöhen. Die Aufteilung in zwei Bereiche – Reifegradmethodik und flexible Erhebung einzelner beispielsweise quantitativer Daten außerhalb des Reifegradmodells – hat sich bewährt und wird daher in jährlich optimierter Form weiterverfolgt. Darüber hinaus konnten im Rahmen der zweiten Durchführung konkrete Entwicklungen im Einzelvergleich aufgezeigt werden.

Unterstützt wird die Evaluierung auch durch eine engmaschige Nutzerbetreuung während der Erhebung, beispielsweise durch begleitende Dokumente oder FAQ, aber auch durch die Möglichkeit einer individuellen Kontaktaufnahme.

Die jährliche Durchführung der Sachstandserhebung legt somit einrichtungsübergreifende, ressortweite Trends in der Informationssicherheit offen, welche die effektive und effiziente Priorisierung, Planung und Implementierung von Maßnahmen fördert und die Ziele des UP Bund nachhaltig unterstützt.

2.3.7 Cyber-Sicherheit von Bundestags- und Landtagswahlen

Wahlen bilden in Demokratien die Grundlage jeglicher Legitimation für Regierungen und parlamentarisches Handeln. 2021 fanden neben der Bundestagswahl im September auch sechs Landtagswahlen statt. 2022 folgen vier weitere Landtagswahlen, und mit der Sozialwahl im Jahr 2023 eine weitere bundesweite Wahl. Cyber-Angriffe in anderen Ländern mit Wahlbezug zeigen, dass staatliche und nichtstaatliche Akteure versuchen, demokratische Prozesse anzugreifen, sie zu stören oder gar zu sabotieren. Beispiele, wie der sogenannte Macron-Hack bei den Präsidentenwahlen in Frankreich 2017, führen die Gefährdung von Wahlen durch Cyber-Angriffe vor Augen: Angreifer hatten einen Tag vor der Stichwahl mehr als 20.000 gestohlene E-Mails aus dem Wahlkampfteam einer der Kandidaten veröffentlicht.

Neben staatlich gesteuerten Angriffsversuchen, die sich gezielt sowohl gegen das Wahlumfeld als auch den öffentlichen Meinungsbildungsprozess richten (vgl. Kapitel *Advanced Persistent Threats*, Seite 28), bedrohen auch Cybercrime-Aktivitäten, wie *Ransomware*-Angriffe (vgl. Kapitel *Big Game Hunting mit Ransomware*, Seite 12) und *Malware*-Spam, das Wahlumfeld. Das Interesse der letztgenannten Angreifer besteht nicht darin, demokratische Wahlen zu stören oder zu unterwandern, sondern darin Löse- oder Schutzgelder zu erpressen; und zwar in diesem Fall von am Wahlprozess beteiligten Institutionen. Solche Aktivitäten können das Vertrauen in die korrekte Durchführung von Wahlen erheblich stören. So könnte ein *Ransomware*-Angriff gegen eine Stadt- oder Kreisverwaltung dafür sorgen, dass es zu Verzögerungen bei der Durchführung oder Auszählung der Wahl kommt, wenn beispielsweise E-Mail-Kommunikation aufgrund des Angriffs nicht verfügbar ist. Der Vertrauensverlust innerhalb der Bevölkerung gegenüber dem Wahlprozess wird als Kollateralschaden von den Angreifern billigend in Kauf genommen oder sogar als Ziel angestrebt.

Auch wenn in Deutschland die eigentliche Wahlstimmenabgabe analog – mit Stift und Papier – erfolgt, wird im Rahmen des Wahlprozesses, des Wahlumfelds und des Informationsumfelds großflächig Informationstechnik eingesetzt. So wird IT unter anderem für die interne und externe Kommunikation von öffentlichen und nichtöffentlichen Informationen genutzt. Zudem werden Prozesse im Wahlprozess und Wahlumfeld zunehmend digitalisiert. Dieser Trend wird gegenwärtig durch die COVID-19-Pandemie zusätzlich verstärkt: Parteitage werden digital abgehalten, Bürgerinnen und Bürger informieren sich immer häufiger im Internet über Wahloptionen, und der Wahlkampf findet bereits seit mehreren Jahren unter anderem auch in den sozialen Medien statt.

Während Institutionen und Akteure im Rahmen ihrer Kommunikation mit den Bürgerinnen und Bürgern bzw. Wählerinnen und Wählern bewusst öffentliche Informationen, wie Wahlprogramme oder Informationen zum Wahlablauf, digital veröffentlichen und verbreiten, verarbeiten sie gleichzeitig auch interne, nichtöffentliche Daten, die nur für einen eingeschränkten Beteiligtenkreis vorgesehen und freigegeben sind. Diese Daten gelten in unterschiedlichster Form als schützenswert.

Informationstechnik wird aber auch genutzt, um Angriffe auf Staat, Wirtschaft und Gesellschaft durchzuführen. Angriffe auf den Wahlprozess, das Wahlumfeld und das Informationsumfeld können dabei die Verfügbarkeit, die Vertraulichkeit, die Integrität sowie die Authentizität der Informationstechnik in diesen Bereich bedrohen.

- Zur Absicherung des formalen Wahlprozesses und seiner IT-Unterstützung arbeitet das BSI eng mit dem Bundeswahlleiter und den Landeswahlleitern zusammen. Für die zahlreichen an den Wahlen beteiligten Parteien und Kandidatinnen und Kandidaten bietet das BSI über sein Web- und Zielgruppenangebot (Öffentliche Verwaltung, Verbraucherinnen und Verbraucher, Unternehmen und Kritische Infrastrukturen) umfangreiche Informationen und Empfehlungen, etwa zur weiteren Verbesserung der existierenden Schutzmaßnahmen, zur Vernetzung als Quelle für aktuelle Informationen und Warnungen, zum Einsatz von IT-Dienstleistern und einiges mehr.

- Die nach Bundeswahlgesetz besonders relevanten Parteien und deren Spitzenkandidatinnen und -kandidaten sind aufgrund ihrer Öffentlichkeitswirksamkeit einer besonderen Bedrohung durch Cyber-Angriffe ausgesetzt. Daher unterbreitet das BSI ihnen intensivere Unterstützungsangebote beispielsweise bei der Absicherung ihrer Social-Media-Kanäle.

- Hinzu kommt die Erweiterung begleitender Maßnahmen. Diese umfassen insbesondere die Erweiterung der täglichen 24/7-Lagebeobachtung der verschiedenen öffentlichen, nichtöffentlichen und sozialen Medien. Zudem arbeitet das BSI in den verschiedenen Bundesarbeitsgruppen zur Bedrohungsfeststellung und -bewertung mit und ist an der Gestaltung konkreter Maßnahmen beteiligt. Entsprechende Berichte, Hinweise, Informationen etc. werden über die verschiedenen Kanäle des BSI den unterschiedlichen Zielgruppen bereitgestellt.

2.3.8 Informationssicherheitsberatung

Die Informationssicherheitsberatung für den Bund berät die Stellen des Bundes zu allen Fragen der Informationssicherheit. Die Pandemie setzte im vergangenen Jahr die Themenschwerpunkte. Standen zunächst Fragen zur sicheren Ausgestaltung des Homeoffice und der Absicherung mobiler Arbeitsplätze im Vordergrund, so lag anschließend ein Schwerpunkt auf den Arbeiten am Sicherheitskonzept für die Corona-Warn-*App* sowie aktuell zum digitalen Impfnachweis. Zudem leistete die Sicherheitsberatung einen Beitrag zur Absicherung von bundesweiten parlamentarischen Wahlen. Konzepte und Handreichungen für Betroffene von unbefugten Veröffentlichungen im Internet wurden vom BSI stetig angepasst, ergänzt und aktualisiert. Auf dem Feld der Digitalisierung unterstützte das BSI insbesondere die Justiz. Durch eine intensive Zusammenarbeit mit der Bundesakademie für öffentliche Verwaltung wurde schließlich auch die Aus- und Weiterbildung von Informationssicherheitsbeauftragten mitgetragen.

Die Informationssicherheitsberatung für Länder und Kommunen berät auf Landes- und kommunaler Ebene zielgruppenspezifisch Bedarfsträger zu allen Fragen der Informationssicherheit mit den thematischen Schwerpunkten Informationssicherheitsmanagement, Sicherheitskonzeption und IT-Grundschutz.

Im vergangen Jahr konnte die Zusammenarbeit zwischen Bund, Ländern und Kommunen weiter ausgebaut und bei der Entwicklung praxisorientierter Lösungsansätze vertieft werden. Dazu gehörte insbesondere die Unterstützung bei der Entwicklung des Anforderungskatalogs zur Informationssicherheit bei der Ermittlung des vorläufigen Wahlergebnisses bundesweiter parlamentarischer Wahlen und die Durchführung der dazugehörigen Workshops im Rahmen von Informationssicherheit bei Landtagswahlen.

2.3.9 Smart Borders und hoheitliches Identitätsmanagement

Ziel des europäischen Smart-Borders-Programms und der übergreifenden Verordnungen zur Interoperabilität der europäischen IT-Systeme im Bereich Sicherheit, Migration und Grenzen ist die sichere Identifikation und Überprüfung von Drittstaatsangehörigen an der Grenze und innerhalb des Schengen-Raums. Hierzu werden das Europäische Ein-/Ausreiseregister (Entry-Exit-System, EES) und das Europäische Reiseinformations- und -genehmigungssystem (European Travel Information and Authorisation System, ETIAS) mit dem polizeilichen Schengen-Informationssystem (SIS), dem Visa-Informationssystem (VIS) und weiteren IT-Systemen auf europäischer Ebene technisch verbunden. So wird das Identitätsmanagement für Drittstaatsangehörige europäisch zentralisiert, standardisiert und einheitlich handhabbar. Neben der Erhöhung der Sicherheit im Schengen-Raum, insbesondere im Kontext grenzüberschreitender Kriminalität, illegaler Migration und Epidemien, ist ein weiteres Ziel die Etablierung effizienterer Grenzkontrollprozesse.

Die Bekämpfung von Pandemien ist 2020 zum beherrschenden Thema in der Öffentlichkeit geworden. Die ETIAS-Verordnung griff dies bereits in seiner 2018 verabschiedeten Fassung auf. Themen wie die Bekämpfung grenzüberschreitender Kriminalität und illegaler Migration finden weiterhin Beachtung, da die Passagierzahlen im Luftverkehr bei Auslandsflügen zwischen 2009 und 2019 um etwa 50 Prozent gestiegen sind (vgl. *Quellenverzeichnis*[64]). Der Bedarf an einer effizienten Grenzkontrolle wird daher nach überstandener Pandemie weiterhin hoch sein.

Das BSI gestaltet die Umsetzung der europäischen Vorhaben aktiv mit. Deutschland stellte 2020, maßgeblich durch BSI-Expertise, den mit Abstand größten Anteil an Anmerkungen zu den technischen Spezifikationen der EU-Systeme. Bei der europäischen Arbeit an den weiterführenden Rechtsakten behielt das BSI die Sicherheit digitaler Identitäten im Blick und wies auf mögliche logische Schwachstellen in systemübergreifenden Prozessen des europäischen Identitätsmanagements hin (siehe Kapitel *Diebstahl und Missbrauch von Identitätsdaten*, Seite 24). National wurde im November 2020 die Version 5.1 der Technischen Richtlinie TR-03121 veröffentlicht, die insbesondere die neuen Biometrieanforderungen

für Grenzkontrollprozesse berücksichtigt und bereits als Grundlage für nationale Ausschreibungen diente. 2021 wurde mit weiteren Bundesbehörden unter Federführung des BSI ein Konzept für das digitale Identitätsmanagement beim Umgang mit den neuen europäischen Registern für die Ausländerbehörden erstellt. Das BSI betreibt parallel zur Ausgestaltung der Spezifikation den Aufbau der Datenanalyse für hoheitliche Systeme, um die korrekte und effiziente Umsetzung der Komponenten auf allen Ebenen zu unterstützen.

2.3.10 Technologie-Verifikations-Programm

Durch das Technologie-Verifikations-Programm (TVP) steht das BSI im Kontakt mit zahlreichen Herstellern von Informations- und Kommunikationstechnik und intensiviert den technischen Dialog über sogenannte Security Labs. Diese Labs dienen zum einen als Austauschplattform, um Meetings und Videokonferenzen zu den Entwicklungsabteilungen rund um den Globus durchzuführen, zum anderen können dort tiefere technische Diskussionen und Einblicke bis hin zur Einsichtnahme auf Quellcodeebene realisiert werden. Hierbei werden die BSI-Mitarbeiterinnen und -Mitarbeiter unter anderem von auf Codeaudits spezialisierte Expertinnen und Experten akkreditierter Prüflabore unterstützt. Durch diesen engen Austausch mit den Entwicklungsabteilungen des Herstellers lassen sich frühzeitig Trends und Risiken erkennen. Hauptzielgruppe des TVP sind vor allem Bedarfsträger aus der öffentlichen Verwaltung. Das BSI kommt mit dem TVP damit seiner Verantwortung für die Gestaltung der Informationssicherheit in Deutschland nach.

Das TVP legt den Schwerpunkt auf den Hersteller. Das bedeutet, dass das BSI in Fragen der IT-Sicherheit eng mit dem Hersteller in Belangen der Cyber-Sicherheit kooperiert und somit einen sehr tiefen Einblick in dessen Arbeitsweise und interne Strukturen erhält. Es beinhaltet regelmäßige Termine bei den Firmenzentralen und die aktive Vertretung von BSI-Positionen gegenüber verschiedener Stellen im Konzern.

Im Rahmen des Technologie-Verifikations-Programms findet ein regelmäßiger technischer Austausch mit internationalen Herstellern der Informations- und Kommunikationstechnik-Industrie (IuK-Industrie) statt, mit Fokus auf technische Themen zur Vertiefung des technischen Know-hows bei ausgewählten Schlüsseltechnologien. Dazu gehören Plattformsicherheit, Virtualisierungstechnologien, Hardware-Sicherheitschips und KI-Technologien. Durch die enge Zusammenarbeit mit den Forschungsabteilungen der Hersteller kann aktiv bei der Gestaltung neuer Technologien mitgewirkt werden, um Sicherheitsstandards branchenweit zu etablieren. Ziel ist auch die Herstellung einer Verbindung der verifizierten Schlüsseltechnologie und der operativen Netze von Bedarfsträgern. Da die Ziele nur mit Unterstützung der Hersteller erreicht werden können, wird in langfristige Kooperationen investiert.

Im Berichtszeitraum wurde die Implementierung von Schlüsseltechnologien vornehmlich bei Netzkomponenten von 5G-Netzen untersucht. Aktuell wird eine Technische Richtlinie dazu erstellt. Zusätzlich werden zurzeit Prüfkataloge basierend auf bereits existierenden Technischen Richtlinien erarbeitet.

2.3.11 App-Testing für mobile Lösungen

Der Einsatz von *Apps* erweitert die Möglichkeiten mobiler Geräte, birgt aber auch Sicherheitsrisiken sowohl für die verarbeiteten Daten als auch für die Gesamtlösung. Diese Risiken müssen bewertet werden.

Der vom BSI zur Verfügung gestellte *App*-Testing-Dienst für Bundesbehörden, der zusammen mit der Firma Deutsche Telekom Security GmbH geleistet wird, bietet eine Entscheidungsgrundlage dafür, ob und unter welchen Bedingungen eine *App* eingesetzt werden kann.

Bei den *App*-Prüfungen werden sowohl sicherheitstechnische als auch datenschutzrelevante Aspekte berücksichtigt. Die Prüfberichte enthalten unter Umständen auch Hinweise und Empfehlungen für die Nutzerinnen und Nutzer darüber, welche Einstellungen sie für eine sichere Nutzung einer *App* beachten sollen.

Sofern erforderlich, rät das BSI gegenüber der Bundesverwaltung auch von der Verwendung einer *App* explizit ab, wenn die Prüfergebnisse dies nahelegen.

Die behördlichen Nutzerinnen und Nutzer des *App*-Testings können auf einen großen Bestand vorhandener Prüfergebnisse zurückgreifen und bei Bedarf neue Prüfungen anstoßen. Dabei besteht die Möglichkeit, *Apps* fortlaufend prüfen zu lassen, damit einmal zur Nutzung freigegebene *Apps* auf dem aktuellen Stand gehalten werden können.

Derzeit wird der *App*-Testing-Dienst von registrierten Nutzerinnen und Nutzern aus mehr als 50 Behörden und Organisationen verwendet. Für mehr als 650 geprüfte *Apps* stehen Prüfergebnisse zum Abruf bereit.

Bei rund 70 Prozent der Prüfergebnisse wurden Hinweise und Empfehlungen gegeben, die bei einer Nutzung der betreffenden *App* beachtet werden sollten. Bei jeder sechsten *App* wurde von einer Verwendung abgeraten.

2.3.12 Lauschabwehr

Zu den Aufgaben der BSI-Lauschabwehr gehört die Beratung zur Abhörsicherheit und die Prüfung von abhörgeschützten Räumen im Geltungsbereich der Verschlusssachenanweisung des Bundes, bei Behörden des Bundes und der geheimschutzbetreuten Wirtschaft sowie als Amtshilfe bei den Bundesländern. Außerdem wird die Lauschabwehr bei Konferenzen auf politischer Ebene oder von besonderer Bedeutung hinzugezogen, nach deren Tagesordnung Themen von besonderer Geheimhaltung besprochen werden.

Im vergangenen Zeitraum fanden coronabedingt keine Vor-Ort-Konferenzen auf hoher politischer Ebene statt, bei denen VS-eingestufte Inhalte unter notwendiger Begleitung des BSI erörtert wurden. Ebenso konnten nur sehr eingeschränkt Lauschabwehrprüfungen vor Ort durchgeführt werden. Der Fokus lag in dieser Zeit auf der Weiterentwicklung der Grundlagen sowie der Projekte.

2.3.13 Verschlusssachen-Zulassung und Herstellerqualifizierung

Das BSI stellt auf Grundlage der allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA) Zulassungen für IT-Sicherheitsprodukte aus. Mit der Zulassung wird diesen Produkten bescheinigt, dass sie im Rahmen des Geheimschutzes zum Schutz von elektronischen Verschlusssachen in angemessen sicherer Weise verwendet werden können.

Ähnlich wie in den Jahren zuvor hat das BSI im Berichtszeitraum 91 Zulassungen ausgesprochen oder verlängert. Die Anzahl der zugelassenen IT-Sicherheitsprodukte bzw. Produktversionen beläuft sich damit auf 209. Allgemein zugelassene Produkte können der tagesaktuellen BSI-Schrift 7164 entnommen werden.

Bedingt durch die COVID-19-Pandemie, stellte das BSI einen sprunghaft gestiegenen Bedarf an zugelassenen Lösungen fest, die ein sicheres Arbeiten und die Handhabung elektronischer Verschlusssachen (VS) auch im Homeoffice ermöglichen. Insbesondere das durch § 51 VSA gegebene Instrument der Freigabeempfehlung konnte hier in effizienter Weise zur kurzfristigen und zielgerichteten Versorgung behördlicher Bedarfsträger genutzt werden. Für die Bundeswehr wurde in diesem Kontext mehrfach das Verfahren zur szenariospezifischen Freigabegenehmigung (VSF) angewendet. Durch das Aussprechen von Freigabeempfehlungen konnte das BSI die VS-Arbeitsfähigkeit der Bundeswehr im Homeoffice innerhalb von Tagen legitimieren.

Zur Umsetzung der 2018 in Kraft getretenen VSA hat das BSI zum einen die Technische Leitlinie TL - IT 01 Mitwirkungspflichten in Zulassungsverfahren sowie den Katalog der für eine Zulassung relevanten Produktklassen und -typen veröffentlicht. Die BSI TL - IT 01 regelt dabei auf Basis der VSA § 52 Abs. 1 die Mitwirkungspflichten aller an einem Zulassungsverfahren beteiligter Parteien. Bei dem Katalog der Produktklassen und -typen handelt es sich um ein flexibel anpassbares Nachschlagewerk darüber, welche Arten von IT-Sicherheitsprodukten einer Zulassung unterzogen werden müssen und welche Sicherheitsleistungen diese erbringen müssen.

Weiterführende Hinweise zur Zulassung, die oben genannten Publikationen und die BSI-Schrift 7164 ist auf der Webseite des BSI zu finden:[y)]

Herstellerqualifizierung

Eine erfolgreich absolvierte Herstellerqualifizierung ist die Voraussetzung dafür, dass IT-Sicherheitsprodukte das Qualifizierte Zulassungsverfahren für die Geheimhaltungsstufe VS - NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) durchlaufen können. In diesem Verfahren wird einem Hersteller nach erfolgreicher Bewertung der Entwicklungsprozesse durch das BSI das Vertrauen ausgesprochen, Produkte sicher im Sinne der VS-Zulassung entwickeln zu können. Damit ist ein qualifizierter Hersteller in der Lage, eine Produktzulassung schneller durchlaufen zu können, als dies bei einem herkömmlichen Zulassungsverfahren der Fall wäre. Die Effizienz des Verfahrens konnte bereits in einer Vielzahl von Zulassungsverfahren bestätigt werden, in denen eine Produktzulassung innerhalb von vier bis acht Wochen erfolgte. Derzeit haben vier Hersteller eine Herstellerqualifizierung erfolgreich absolviert, vier weitere durchlaufen aktuell das Qualifizierungsverfahren.

VS-Anforderungsprofile

VS-Anforderungsprofile (VS-AP) beschreiben IT-Sicherheitsanforderungen an zuzulassende IT-Sicherheitsprodukte. Sie werden in einem kooperativen Vorgehen gemeinsam von Bedarfsträgern, Betreibern und dem BSI erstellt. Auf diese Weise wird sichergestellt, dass Sicherheitsanforderungen in harmonisierter, bedarfsgerechter und effizienter Weise festgeschrieben werden.

Inzwischen gibt es 16 abgeschlossene VS-Anforderungsprofile zu verschiedenen Produkttypen und bereits eine Reihe von IT-Sicherheitsprodukten, die konform zu diesen BSI-Anforderungen sind. Im Berichtszeitraum wurden drei VS-APs publiziert und mit der Erstellung von zwei weiteren VS-APs begonnen. Da VS-Anforderungsprofile

einen Standard darstellen, der immer an den Stand der Technik angepasst wird, befindet sich ein VS-Anforderungsprofil in der Überarbeitung und Anpassung. Darüber hinaus sind eine Vielzahl weiterer VS-APs in Vorbereitung.

Eine detaillierte Beschreibung und Auflistung vorhandener und in Arbeit befindlicher VS-APs sind auf der Seite des BSI zu finden:[z)]

2.3.14 Messenger-Dienste für sichere VS-Kommunikation

Die Nutzungsmöglichkeiten von zeitgemäßen Kommunikationsmitteln im Umfeld der Bundesverwaltung sind vielfältig - sei es zur flexiblen Erreichbarkeit im Homeoffice, zum behördenübergreifenden Austausch bei Sicherheitsvorfällen oder zur Kommunikation mit Wirtschaft, Bürgerinnen und Bürgern oder europäischen Partnerbehörden. Im Behördenumfeld spielen dabei neben Datenschutzaspekten erhöhte Sicherheitsanforderungen eine Rolle, beispielsweise wenn es um den Versand sensibler oder im Sinne der VSA als VS-NfD eingestufte Informationen geht (vgl. Kapitel *Verschlussachenzulassung und Herstellerqualifizierung*, S. 77). Aus diesem Grund evaluiert das BSI bereits seit einiger Zeit Messaging-Lösungen, darunter insbesondere den Messenger Wire.

Rechtzeitig vor Beginn der deutschen EU-Ratspräsidentschaft wurde Anfang Juni 2020 eine VS-NfD-Freigabeempfehlung für den On-Premises-Einsatz von Wire in der Bundesverwaltung erteilt. Aktuell steht neben einer Weiterentwicklung des Produktes eine tiefergehende Evaluierung mit dem Ziel der VS-NfD-Zulassung an. Weitere Messenger, die perspektivisch eine VS-NfD-Zulassung anstreben, sind der auf dem Matrix-Protokoll basierende BwMessenger der Bundeswehr und der SecureCOM-Messenger der Firma Virtual Solution AG.

Bei Wire handelt es sich um einen vollwertigen Messenger, der neben dem Versand von Text- und Sprachnachrichten, Dateien und Bildern auch das Durchführen von Audio- / Videokonferenzen sowie das Teilen von Bildschirminhalten ermöglicht. Den hohen Sicherheitsanforderungen wird bei Wire Rechnung getragen, indem sämtliche Daten Ende-zu-Ende-verschlüsselt werden und die Erhebung von Metadaten auf ein Minimum reduziert wird. Für die Verschlüsselung wird das Double-Ratchet-Protokoll (vgl. *Quellenverzeichnis*[65]) eingesetzt, das derzeit als State-of-the-Art im Bereich des Messagings gilt.

Nicht nur im Behördenumfeld, sondern auch in Wirtschaft und Gesellschaft besteht reges Interesse an einer sicheren Kommunikation im Austausch mit Ämtern oder untereinander, um beispielsweise Wirtschaftsspionage zu verhindern oder dem Abfluss persönlicher Daten vorzubeugen. Diesem Bedarf soll im Rahmen des Wire-Projekts zukünftig mit der Möglichkeit der Föderation verschiedener Systeme begegnet werden. Einen wesentlichen Aspekt stellt dabei die Umstellung des kryptografischen Protokolls auf den MLS-Standard (Messaging Layer Security) (vgl. *Quellenverzeichnis*[66]) dar, der derzeit im Rahmen einer IETF-Arbeitsgruppe (vgl. *Quellenverzeichnis*[67]) finalisiert wird und unter anderem die Interoperabilität verschiedener Messaging-Lösungen ermöglichen soll.

2.3.15 Umsetzung des Onlinezugangsgesetzes

Das 2017 in Kraft getretene Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz – OZG) verpflichtet Bund, Länder und Kommunen, ihre Verwaltungsleistungen bis Ende 2022 auch elektronisch über Verwaltungsportale anzubieten und diese miteinander zu einem Portalverbund zu verknüpfen. Um diese Dienste in Anspruch nehmen zu können, ist es essenziell, dass sich Bürgerinnen und Bürger sowie Institutionen mittels der im OZG verankerten Nutzerkonten von Bund und Ländern online sicher identifizieren und authentisieren können.

Vorgaben für die sichere Anbindung von Identifizierungs- und Authentisierungsverfahren an die Nutzerkonten gibt Teil 1 der Technischen Richtlinie TR-03160 Servicekonten des BSI. Damit wird den an die Nutzerkonten angebundenen Fachverfahren die Identität der Nutzerin bzw. des Nutzers auf dem jeweiligen Vertrauensniveau garantiert, ohne dass sie Details der Identifizierung und *Authentifizierung* kennen müssen. Teil 2 der TR-03160 macht Vorgaben zur Interoperabilität der Lösungen von Bund und Ländern, um zu gewährleisten, dass Nutzerinnen und Nutzer sich nur bei einem Bundesland identifizieren müssen und anschließend auch Leistungen eines anderen Bundeslandes bzw. des Bundes in Anspruch nehmen können. Beide Teile wurden mit Bund und Ländern als Betreiber abgestimmt und auf der Webseite des BSI veröffentlicht.

Für die Anbindung des elektronischen Identitätsnachweises auf Smartphones (Smart-eID) an die Servicekonten von Bund und Ländern wurde ein Handlungsleitfaden zur Integration der Smart-eID in ein Nutzerkonto veröffentlicht (vgl. *Quellenverzeichnis*[68]).

Für die elektronische Zustellung der in Fachverfahren erstellten Bescheide stellen die Nutzerkonten des OZG Postfächer zur Verfügung. Anforderungen an Sicherheit und Interoperabilität der unterschiedlichen Postfachlösungen werden zurzeit in der Technischen Richtlinie TR-03160-3 Interoperable Postfächer zusammengeführt.

Um Bescheide auch dann noch auf ihre Integrität prüfen zu können, wenn sie ausgedruckt vorliegen oder auf mobilen Geräten vorgezeigt werden, können sie mit kryptografisch gesicherten Barcodes versehen werden. Solche digitalen Siegel gemäß TR-03137 werden bereits auf hoheitlichen Dokumenten wie Ankunftsnachweisen verwendet, um die Echtheit der aufgedruckten Daten zweifelsfrei verifizieren zu können. Die neue Technische Richtlinie TR-03171 ermöglicht auch die Absicherung von Urkunden, Bescheiden und anderen Verwaltungsdokumenten von Bund, Ländern und Kommunen mittels optisch verifizierbarer digitaler Siegel.

2.4 Internationale und europäische Zusammenarbeit

Das Thema IT-Sicherheit macht vor Grenzen nicht halt. Um Bedrohungen im Cyber-Raum effektiv begegnen zu können, ist eine Bündelung der Kräfte auf internationaler Ebene notwendig. Es ist die Überzeugung des BSI, dass die Cyber-Sicherheit in Deutschland durch internationale Zusammenarbeit und weltweiten Austausch gestärkt wird. Aus diesem Grund arbeitet das BSI seit seiner Gründung vor 30 Jahren mit Partnern weltweit zusammen: bilateral, multilateral sowie in Gremien und Arbeitsgruppen. Dabei sind die Expertinnen und Experten des BSI als Gesprächs- und Diskussionspartner sowie Vortragende gefragt.

Ziel des BSI ist, neben seiner nationalen Aufgabe als Cyber-Sicherheitsbehörde des Bundes die Cyber-Sicherheit auch international mitzugestalten sowie die eigene technologische Beurteilungsfähigkeit zu stärken. Um seiner Verantwortung angemessen nachzukommen, intensiviert und erweitert das BSI kontinuierlich seine Beziehungen zu Behörden, Organisationen und Unternehmen sowie Akteuren der Wissenschaft und Zivilgesellschaft weltweit – seit Dezember 2019 auch mit einem Verbindungsbeamten in Brüssel. Die Arbeit in diversen Fachgremien zu Informations- und Cyber-Sicherheit im EU-, NATO- und internationalen Kontext ist ein wesentlicher Bestandteil des internationalen Engagements des BSI.

2.4.1 Engagement des BSI im EU-Rahmen

Im Berichtszeitraum war die deutsche EU-Ratspräsidentschaft im zweiten Halbjahr 2020 der prägende Ankerpunkt des BSI-Engagements in der Europäischen Union. Das BSI war maßgeblich an der inhaltlichen Entwicklung und Begleitung des Fokusthemas im Bereich der Cyber-Sicherheit beteiligt – der Definition von Mindestanforderungen an die Sicherheit vernetzter Geräte (vgl. Kapitel *Sicherheit im Internet der Dinge, Smart Home und Smart Cities*, Seite 50). Diese Anforderungen wurden im Zuge einer digitalen EU-Cyber-Sicherheitskonferenz mit über 400 Teilnehmerinnen und Teilnehmern europäischer Cyber-Sicherheitsbehörden beworben, die das BSI gemeinsam mit dem BMI organisiert hatte. Die deutsche Initiative mündete in der Verabschiedung von Ratsschlussfolgerungen. Seitdem steht das Thema auf der europäischen Agenda und wurde beispielsweise auch in der neuen Cybersicherheitsstrategie der Europäischen Kommission und des Hohen Vertreters der Europäischen Union für Außen- und Sicherheitspolitik adressiert.
Die deutsche Ratspräsidentschaft erreichte Ende 2020, auch unter Mitwirkung des BSI-Verbindungsbeamten im deutschen Verhandlungsteam, eine Einigung mit Europäischen Parlament zum Europäischen Kompetenzzentrum für Industrie, Technologie und Forschung im Bereich der Cyber-Sicherheit. Bei den Vorbereitungen für die Einrichtung des entsprechenden Nationalen Koordinierungszentrums spielte das BSI eine aktive Rolle (vgl. Kapitel Nationales Koordinierungszentrum für europäische Forschungsvorhaben, Seite 80)

Seit Anfang 2021 wird der Vorschlag einer Richtlinie über Maßnahmen für ein hohes gemeinsames Cyber-Sicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148, der sogenannten NIS-Richtlinie 2.0, verhandelt. Hier brachte sich das BSI unter Federführung des BMI aktiv in die Verhandlungen ein. Parallel dazu war das BSI in verschiedenen Gremien europäischer Cyber-Sicherheit aktiv, u. a. der NIS-Kooperationsgruppe, dem CSIRT-Netzwerk, der European Cybersecurity Certification Group sowie verschiedenen Gremien und Arbeitsgruppen der Agentur der Europäischen Union für Cyber-Sicherheit (ENISA).

2.4.2 Multilaterales und bilaterales Engagement des BSI

Das multilaterale und bilaterale Engagement des BSI zeigt sich vielfältig und umfangreich. So besteht mit vielen Partnerbehörden im Ausland eine direkte und vertrauensvolle Zusammenarbeit. Das Spektrum reicht dabei von operativem Informationsaustausch über fachlich technische Dialoge bis hin zu strategischen Diskussionen im Policy-Kontext.

Auch in und gegenüber der NATO erfüllt das BSI in seinen Rollen als die Nationale Kommunikationssicherheits-

behörde (National Communication Security Authority, NCSA) und die Nationale Cyber-Sicherheitsbehörde (National Cyber Defence Authority, NCDA) für Deutschland eine wichtige Funktion. In den entsprechenden NATO-Gremien bringt sich das BSI durch seine nationalen Erfahrungen und Ansätze ein und wirkt bei der Gestaltung zentrale Themen der Cyber- und Informationssicherheit der Allianz mit.

Das Jahr 2020 stand auch im Zeichen des Brexit. Aus Sicht des BSI ist eine gute Zusammenarbeit mit Großbritannien wichtig für das Thema IT-Sicherheit im internationalen Umfeld und für Europas Streben nach digitaler Souveränität. In diesem Sinne wurde der Austausch mit der britischen Partnerbehörde des BSI, dem National Cyber Security Center (NCSC), zu technischen Themen vertieft. Rund ein Jahr nach dem Brexit ist die Bilanz sehr positiv. Das langjährige Arbeits- und Vertrauensverhältnis zwischen NCSC und BSI war dabei sicher ein hilfreicher Faktor. In dem im März 2021 von Premier Boris Johnson präsentierten Integrated Review, einer strategischen Neuausrichtung Großbritanniens im Bereich Außen- und Sicherheitspolitik, spielen Technologieführerschaft und Digitalisierung eine zentrale Rolle. Diese Entwicklungen werden vom BSI aufmerksam und mit dem Ziel verfolgt, zusätzliche Kooperationsprojekte beispielsweise im Bereich der sicheren Ausgestaltung neuer Technologien auszuloten.

Besonders hervorzuheben war im Jahr 2020 die Zusammenarbeit mit dem polnischen Digitalministerium im Bereich Umsetzung der EU-Toolbox für 5G-Sicherheit. Im Rahmen der NIS-Kooperationsgruppe engagierte sich das BSI zusammen mit Polen federführend für die Umsetzung der Maßnahmen im Bereich Zertifizierung und Standardisierung und erreichte unter anderem die Beauftragung von europaweiten Zertifizierungsschemata durch die EU-Kommission im Rahmen des Cybersecurity Acts.

2.4.3 Nationales Koordinierungszentrum für europäische Forschungsvorhaben

Der Rat und das Europäische Parlament haben Ende 2020 die Einrichtung eines europäischen Kompetenzzentrums für Cyber-Sicherheit in Industrie, Technologie und Forschung (Kompetenzzentrum) und eines Netzes von Nationalen Koordinierungszentren (Koordinierungszentren) beschlossen. Die entsprechende Verordnung ist im Mai 2021 in Kraft getreten. Das Kompetenzzentrum wird seinen Sitz in Bukarest haben und der Bündelung von Investitionen in Forschung, Technologie und industrieller Entwicklung dienen. Insbesondere die Planungen der europäischen Förderprogramme Horizont Europa (HEP) und Digitales Europa (DEP) im Bereich Cyber-Sicherheit sollen damit besser aufeinander abgestimmt werden.

Darüber hinaus soll das Kompetenzzentrum auch Forschungs- und Innovationsmaßnahmen (unterstützt durch HEP) sowie Maßnahmen zum Kapazitätsaufbau (unterstützt durch DEP) eigenverantwortlich durchführen. Außerdem sollen sich das Kompetenzzentrum und das Netz nationaler Koordinierungszentren um stärkere Synergien und eine enge Abstimmung zwischen den zivilen Sektoren und dem Verteidigungssektor im Bereich der Cyber-Sicherheit bemühen. Bei all diesen Aktivitäten sind insbesondere die Belange der KMU zu berücksichtigen.

Das Kompetenzzentrum wird durch die Mitgliedstaaten und die Europäische Kommission verwaltet. Dafür wird ein Verwaltungsrat eingerichtet, in dem für Deutschland das BSI mitwirken wird. Das Kompetenzzentrum soll eine stärkere Koordinierung von Forschung und Innovation sowie von Einführungsstrategien auf europäischer und nationaler Ebene gewährleisten. Die Mitgliedstaaten werden über gemeinsame Maßnahmen und Projekte entscheiden.

Das Netzwerk der nationalen Koordinierungszentren soll dabei den Austausch zwischen den Mitgliedstaaten intensivieren, damit besser und schneller mögliche internationale Projektpartnerschaften gefunden und geschlossen werden können und damit die digitale Souveränität in Europa gestärkt wird. Die zugehörigen nationalen Koordinierungszentren werden den Austausch innerhalb der Mitgliedstaaten zu relevanten nationalen Stellen im Forschungs- und Wirtschaftssektor im Bereich Cyber-Sicherheit und Cyber-Verteidigung fördern und den Informationsfluss zum Kompetenzzentrum bündeln, um die nationalen Cyber-Sicherheitsgemeinschaften bestmöglich zu unterstützen. Gleichzeitig können so auch nationale Interessen in die Planungen der europäischen Forschungsprogramme eingebracht werden.

Das deutsche nationale Koordinierungszentrum für Cyber-Sicherheit in Industrie, Technologie und Forschung (NKCS) wird als gemeinsame Kooperationsplattform von BMI, BMWi, BMVg und BMBF eingerichtet. Dabei wird das BSI die Rolle der Kopfstelle und des Single Point of Contact (SPoC) wahrnehmen. Bereits in den Ressorts und Institutionen etablierte Strukturen, beispielsweise zur Vergabe von Fördermitteln, können unmittelbar genutzt werden.

Durch das nationale Koordinierungszentrum wird ein umfangreicher Dienstekatalog erstellt, in dem auf bereits auf Bundesebene vorhandene Dienstleistungen hingewiesen wird und offene Dienstleistungen zur Unterstützung der Cyber-Sicherheitsgemeinschaft angeboten werden. So soll im Bereich Cyber-Sicherheit

ein nationales digitales Ökosystem geschaffen werden, und das nationale Koordinierungszentrum mit dem BSI als Kopfstelle alle relevanten Informationen, die zur Förderung der deutschen Cyber-Sicherheitsforschung und –entwicklung notwendig sind, bündeln.

In dieser Rolle wird das BSI sowohl mit den beteiligten Ressorts als auch mit dem europäischen Kompetenzzentrum und den Koordinierungszentren anderer Nationen eng zusammenarbeiten. So soll für die deutsche Cyber-Sicherheitsgemeinschaft ein breiter Überblick über Ansprechpartner, Unterstützungsangebote, Veranstaltungen, Projekte, Forschungsinstitute bzw. potentielle Forschungspartner, Forschungsprogramme, Geldvergaben und Forschungsvorhaben bereitgestellt werden. Durch diese neue Rolle kann das BSI noch aktiver Einfluss nehmen, zur zielgerichteten Vergabe von europäischen Fördermitteln beitragen und Forschungsrichtungen sowohl aus nationaler als auch europäischer Perspektive unterstützen. So wird ein unmittelbarer Beitrag zur Erhöhung der Cyber-Sicherheit in Deutschland und Europa geleistet.

2.4.4 eID: Europaweite Anerkennung der Online-Ausweisfunktion

Für die Umsetzung der Digitalisierung ist die sichere Identifizierung von Personen und Dingen von entscheidender Bedeutung (vgl. Kapitel *Sichere elektronische Identitäten auf dem Smartphone*, Seite 55). Daher wurden bereits 2014 mit Hinblick auf die Digitalisierung des europäischen Binnenmarkts im Rahmen der eIDAS-Verordnung einheitliche, europaweit geltende Rahmenbedingungen für die grenzüberschreitende gegenseitige Anerkennung von elektronischen Identifizierungsmitteln und Vertrauensdiensten auf EU-Ebene festgelegt.

Unter intensiver Mitarbeit des BSI hat Deutschland mit der Online-Ausweisfunktion des Personalausweises und des elektronischen Aufenthaltstitels das der Anerkennung vorgelagerte Notifizierungsverfahren bereits 2017 als erstes Land erfolgreich abgeschlossen. Die Notifizierung der Online-Ausweisfunktion auf dem höchsten Vertrauensniveau gemäß der eIDAS-Verordnung wurde anschließend im September 2017 im Amtsblatt der EU veröffentlicht. Diese Notifizierung wurde 2020 um die neue Unionsbürgerkarte erweitert. Daher gilt bereits seit 2017 (für die Unionsbürgerkarte erst ab Ende 2021) die gegenseitige Anerkennungspflicht. Alle EU/EWR-Mitgliedstaaten, die über entsprechende Onlinedienste verfügen, sind verpflichtet, die Online-Ausweisfunktion für Anwendungen des öffentlichen Sektors, insbesondere im E-Government, anzuerkennen und anzubinden.

Infolgedessen haben bis April 2021 mit technischer Unterstützung durch das BSI bereits 18 Staaten (Belgien, Dänemark, Estland, Finnland, Griechenland, Italien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Österreich, Schweden, Slowakei, Slowenien, Spanien, Tschechische Republik, Kroatien) und die Europäische Kommission die Online-Ausweisfunktion erfolgreich in ihr eID-Schema eingebunden. Damit ist es bereits jetzt möglich, die Online-Ausweisfunktion für Onlinedienste in mehr als der Hälfte der EWR-Staaten zu verwenden. Obwohl nicht alle verbleibenden Staaten über Online-Dienste verfügen und somit von der Anerkennungsverpflichtung befreit sind, befinden sich acht Staaten (Stand April 2021) im Testbetrieb oder in Vorbereitung dazu, sodass ein weiteres Wachstum der Abdeckung zu erwarten ist.

Aber auch andere Länder zeigen Bestrebungen, ihre eID-Schemata zu notifizieren. So haben bis Ende April 2021 bereits 14 weitere Staaten eID-Schemata notifiziert (Belgien, Dänemark, Estland, Großbritannien, Italien, Kroatien, Lettland, Luxemburg, Niederlande, Portugal, Slowakei, Spanien, Tschechische Republik, Litauen). Weitere Verfahren sind auf den Weg gebracht oder fast abgeschlossen.

Die eID-Schemata der verschiedenen Länder unterscheiden sich teils stark. Viele der begutachteten eID-Systeme nutzen tatsächlich die nationalen, auf Chipkarten basierenden Ausweisdokumente. Andere gründen auf die Verwendung von zertifizierten SIM-Karten oder anderen Hard- bzw. Software-basierten Sicherheitseigenschaften von Endgeräten. Immer mehr an Bedeutung gewinnen hierbei *App*-basierte Verfahren, deren Bewertung jedoch stark von den eingesetzten Sicherheitsfunktionalitäten des Mobilgerätes abhängt. Die unterschiedlichen Ansätze bringen die verschiedensten Bewertungen im Rahmen der zum Notifizierungsverfahren gehörenden Begutachtungen mit sich, die sich über die gesamte Breite der möglichen Vertrauensniveaus verteilen.

Die notifizierten elektronischen Identitäten der anderen Staaten werden im deutschen E-Government mit Hilfe der Nutzerkonten bzw. Bürgerportale im Rahmen der Umsetzung des Onlinezugangsgesetzes angebunden und so anerkannt.

Im Jahr 2020 hat eine Revision der eIDAS-Verordnung begonnen, in deren Rahmen rückblickend die Erfolge und Misserfolge der Verordnung betrachtet und, wenn nötig, Änderungen entwickelt werden. Im Jahr 2021 hat die EU-Kommission einen Vorschlag für eine Überarbeitung der eIDAS-Verordnung vorgelegt.

2.4.5 Krypto-Modernisierung für Satellitensysteme

Das Funktionieren unseres Staates, unserer Wirtschaft und unserer Gesellschaft ist immer stärker abhängig von digitalen Diensten für Kommunikation, Navigation, Position und Zeitbestimmung sowie Klimaüberwachung und Wettervorhersage. Die Realisierung dieser Dienste ist in vielen Bereichen nur durch satellitengestützte Infrastrukturen möglich.

Informationen bilden die Grundlage für Planungen, Wissen und Entscheidungen im privaten, wirtschaftlichen und behördlichen Umfeld. Das reizt Hacker oder kriminelle Gruppen, diese Informationen abzugreifen oder falsche Informationen zu verbreiten. Die Verfügbarkeit, aber auch die Integrität und Vertraulichkeit von Systemen, Diensten und Informationen sind für unsere Gesellschaft essenziell.

Das BSI bedient das Gebiet Cyber- und IT-Sicherheit für Satelliten intensiv. Im Fokus steht dabei das europäische Navigationssystem GALILEO. Grundsätzlich betrachtet das BSI aber alle Satellitensysteme. Zusammen mit anderen Mitgliedsstaaten wurde unter der Federführung des BSI ein Anforderungskatalog erstellt, um Satellitensysteme und deren Kommunikationsinfrastrukturen zukunftssicher zu machen. Eine wesentliche Forderung ist die Resistenz gegenüber der Bedrohung durch Quantencomputer. Diese Anforderungen an die Modernisierung der IT- und Cyber-Sicherheit für Satelliten und deren Bodeninfrastrukturen konnten 2020 erfolgreich in die Entwicklung der zweiten Generation des europäischen Navigationssystems GALILEO eingebracht werden. Die ersten Satelliten mit modernisierter Kryptografie sollen 2024 starten.

2.5 Aktuelle Trends und Entwicklungen in der IT-Sicherheit

Die rasante technologische Entwicklung stellt IT-Sicherheitsbehörden vor immer neue Herausforderungen, auf die verbindliche Antworten gefunden werden müssen. Diese Antworten lassen sich zum Teil aber auch aus den neuen Technologien selbst ableiten, die auch den Sicherheitsexpertinnen und -experten neue Optionen an die Hand geben, sicherheitsrelevante Vorfälle rechtzeitig zu erkennen und zu verhindern. Das BSI arbeitet in Bereichen wie Künstliche Intelligenz (KI), *Blockchain*, Quantencomputing oder Kryptografie eng mit Universitäten, Fachhochschulen und anderen Forschungseinrichtungen zusammen, um neue Antworten auf aktuelle Sicherheitsfragen zu finden.

2.5.1 Künstliche Intelligenz

Methoden aus dem Gebiet der Künstliche Intelligenz (KI) sind aufgrund ihrer Leistungsfähigkeit in vielen Anwendungsdomänen längst zur Schlüsseltechnologie herangereift. Sie durchdringen zunehmend Bereiche in Staat, Wirtschaft und Gesellschaft und leisten einen wesentlichen Beitrag zur Digitalisierung. Viele Fragestellungen zu den Sicherheitseigenschaften von KI-Systemen sowie den Anwendungspotentialen von KI in der IT-Sicherheit sind derzeit aber noch ungeklärt. Ihrer Beantwortung kommt das BSI im Rahmen seiner Verantwortung für die sichere Ausgestaltung von Technologie nach.

Um den sicheren Einsatz von KI zu ermöglichen, sind sowohl organisatorisch-prozedurale als auch technische Anforderungen an die Entwicklung und den Betrieb von KI-Systemen notwendig. Hinsichtlich der technischen Anforderungen setzte das BSI im zurückliegenden Berichtszeitraum seine umfassenden Analysen zu den Sicherheitseigenschaften von KI-Systemen fort. In einem Überblicksdokument das als erster Ansatzpunkt für KI-Anbieter und professionelle Anwenderinnen und Anwender dienen kann, wurden unter Berücksichtigung der beiden genannten Anforderungsaspekte Probleme, Maßnahmen und Handlungsbedarfe für den sicheren, robusten und nachvollziehbaren Einsatz von KI zusammenfassend vorgestellt.
Mehr zum Thema finden Sie hier:[aa)]

KI in der Normung, Standardisierung und Zertifizierung

Das BSI nutzt seine Expertise und Arbeitsergebnisse auch für Normungs- und Standardisierungsaktivitäten auf nationaler sowie internationaler Ebene. Dazu wirkt das BSI an KI-bezogenen Initiativen und Gremien des DIN, der Arbeitsgruppe ISG SAI (Securing Artificial Intelligence) (vgl. *Quellenverzeichnis*[69]) bei der ETSI sowie der Ad-hoc-Arbeitsgruppe zum Thema KI der ENISA (vgl. *Quellenverzeichnis*[70]) mit. Insbesondere die Ende 2020 auf dem Digital-Gipfel vorgestellte erste Version der Normungsroadmap KI (vgl. *Quellenverzeichnis*[71]) an deren Erarbeitung das BSI beteiligt war, stellt einen bedeutenden nationalen Beitrag zur Entwicklung und Etablierung KI-spezifischer Normen und Standards dar. In Zukunft wird das BSI zudem die Standardisierung für und Umsetzung des Artificial Intelligence Acts der EU eng begleiten.

Um die Verwendung von KI nachweislich sicher und vertrauenswürdig zu gestalten, ist die Entwicklung entsprechender Prüfkriterien, -verfahren und -methoden entscheidend. Das BSI arbeitete dafür eng mit Wirtschaft und Wissenschaft zusammen. Einen Meilenstein

auf diesem Weg markierte die Unterzeichnung einer strategischen Kooperationsvereinbarung zwischen dem BSI und dem Fraunhofer IAIS im November 2020 zur gemeinsamen Entwicklung von Prüfverfahren. Das initiale Vorhaben der Kooperation wurde Anfang 2021 mit dem Auftakt des von der Kompetenzplattform KI der NRW-Landesregierung (KI.NRW) geförderten Flagship-Projektes Zertifizierte KI beschlossen. (vgl. *Quellenverzeichnis*[72]). Die angestrebten Resultate des Projektes bilden die Grundlage für einheitliche und prüfbare Normen und Standards.

Domänen- und anwendungsspezifische Ergebnisse

Die Erarbeitung von Prüfverfahren und -methoden sowie von Normen und Standards erfolgt unter Berücksichtigung domänen- und anwendungsspezifischer Charakteristika der KI-Systeme. In zwei wesentlichen Anwendungsdomänen, Mobilität und *Cloud*-Service, hat das BSI den sicheren Einsatz von KI in den relevanten Anwenderkreisen vorangetrieben.

Im Kontext der Digitalisierung spielen KI-Methoden insbesondere bei der Ausführung sicherheitskritischer Aufgaben eine immer bedeutendere Rolle. So sind diese beispielsweise bei der biometrischen Identifikation und Verifikationen von Personen (siehe Kapitel *Biometrie im Zeitalter der Künstlichen Intelligenz*, S. 56) bereits allgegenwärtig. Auch im Bereich der Mobilität, z. B. im (teil-) autonomen Fahren, kommen KI-Methoden verstärkt zum Einsatz. Dies betrifft u. a. die Verarbeitung von Bilddaten, etwa zur Detektion und Klassifikation von Verkehrsschildern oder anderen Verkehrsteilnehmerinnen und -teilnehmern. Das BSI betreibt bereits seit 2019 eine Arbeitsgruppe mit dem Verband der TÜVs (VdTÜV), in der Konzepte für den sicheren Einsatz von KI-Verfahren im Bereich Automotive entwickelt werden. Von der Arbeitsgruppe wurde im Oktober 2020 ein internationaler Workshop unter Beteiligung renommierter Vortragender ausgerichtet, der sich mit der Frage der Auditierung von KI-Verfahren befasste. Die Ergebnisse des Workshops wurden im Mai 2021 in einem Whitepaper veröffentlicht. Daneben hat das BSI exemplarisch Robustheitstests für KI-Verfahren zur Verkehrsschildklassifikation durchführen lassen (vgl. *Quellenverzeichnis*[73]). Das BSI sieht derartige Tests als eine Komponente zur Gewährleistung des sicheren Einsatzes von KI-Verfahren im Bereich Automotive und plant die Weiterentwicklung der Tests sowie die Verallgemeinerung auf weitere Anwendungsfälle.

Mit der Veröffentlichung des Kriterienkatalogs AIC4 (AI *Cloud* Service Compliance Criteria Catalogue) (vgl. *Quellenverzeichnis*[74]) im Februar 2021 hat das BSI einen wesentlichen ersten Schritt getan, um mittels organisatorisch-prozeduraler Anforderungen die Informationssicherheit bei der Verwendung von Verfahren des maschinellen Lernens in *Cloud*-Diensten zu stärken. Der Katalog stellt eine Erweiterung des etablierten BSI C5 (vgl. Kapitel *Sicherheit von Cloud-Diensten*, Seite 68) über KI-spezifische Anforderungen dar. Er definiert ein Mindestniveau für sichere und vertrauenswürdige KI *Cloud*-Dienste und formuliert dazu Kriterien, die im Rahmen einer standardisierten Prüfung auditiert werden können. Ein entsprechender Prüfbericht schafft nicht nur ein hohes Maß an Transparenz zwischen *Cloud*-Anbietern und professionellen *Cloud*-Nutzerinnen und -nutzern, sondern liefert bei sachgerechter Auswertung eine Grundlage zur selbstständigen Bewertung der Informationssicherheit eines Dienstes. Der Kriterienkatalog wird durch das BSI in einem breiten Beteiligungsprozess schrittweise weiterentwickelt sowie an den aktuellen Stand der Forschung angepasst. Weiterführende Informationen finden Sie hier:[bb)]

KI in der Kryptografie und Seitenkanalanalyse

Das BSI verfolgt weiterhin die Anwendung von KI-Methoden auf Fragestellungen in der Krypto- sowie der Seitenkanalanalyse, und hat dazu erneut wesentliche fachliche Beiträge geleistet. So nahm beispielsweise ein Team des BSI im September 2020 mit großem Erfolg an der CHES***-Challenge teil. Dabei kamen KI-Methoden zum Einsatz, um speziell gegen *Seitenkanalangriffe* geschützte Implementierungen zu brechen. Im Ergebnis gewann das BSI-Team sämtliche zu vergebenden Preise und sicherte sich damit den Gesamtsieg. Die Resultate beider Gebiete, der Krypto- sowie der Seitenkanalanalyse, werden verwendet, um bestehende Anforderungen an die Sicherheit kryptografischer Verfahren und Implementierungen anzupassen und zu ergänzen.

Ausbau des Bereichs KI am Stützpunkt Saarbrücken

Die bisherigen Tätigkeiten des BSI zum Thema KI werden durch die Errichtung eines neuen BSI-Stützpunktes in Saarbrücken weiter intensiviert und um neue Aufgabenschwerpunkte ergänzt. Neben der Ausweitung der technischen Betrachtungen zur KI-Sicherheit werden in Saarbrücken auch die technischen Grundlagen für den digitalen Verbraucherschutz im Bereich KI erarbeitet. Der neue Stützpunkt ermöglicht zudem einen verstärkten Austausch mit französischen und weiteren europäischen Partnern, um die Entwicklung von KI-Sicherheitsstandards auch auf internationaler Ebene voranzutreiben.

***Conference on Cryptographic Hardware and Embedded Systems

2.5.2 Kryptografie

Als Alternative zu klassischen Public Key-Verfahren wie RSA und ECC werden zurzeit Verfahren entwickelt und standardisiert, die voraussichtlich auch mit Quantencomputern nicht gebrochen werden können (Post-Quanten-Kryptografie). Diese quantencomputerresistenten Verfahren beruhen auf mathematischen Problemen, für deren effiziente Lösung heute weder klassische Algorithmen noch Quantenalgorithmen bekannt sind.

Die Standardisierung solcher Verfahren geschieht im Wesentlichen in einem vom US-amerikanischen National Institut for Standards and Technology (NIST) initiierten Prozess mit internationaler Beteiligung. Erste Draft Standards hat NIST für 2022/23 angekündigt. Neben der Standardisierung von Verfahren laufen zurzeit viele Aktivitäten zur Migration auf Post-Quanten-Kryptografie. Aber auch im Bereich Public Key-Infrastrukturen bzw. in Anwendungsbereichen digitaler Zertifikate nimmt das Thema Quantencomputerresistenz an Fahrt auf. Hier werden zurzeit verschiedene Ansätze (hybride Zertifikate, mixed PKI, alternative Signatur etc.) diskutiert.

Neben ersten quantencomputerresistenten Verfahren zum Schlüsseltransport werden in der Technischen Richtlinie TR-02102 seit März 2021 auch die hashbasierten Signaturverfahren LMS und XMSS empfohlen. Das BSI hat zudem seine Handlungsempfehlungen zur Migration zu Post-Quanten-Kryptografie (vgl. *Quellenverzeichnis*[75]) im August 2020 aktualisiert. Eine Langfassung dieser Handlungsempfehlungen soll im Herbst 2021 veröffentlicht werden.

Weitere Informationen zum Thema sind auf der Webseite des BSI zu finden:[cc)]

2.5.3 Quantum Key Distribution

Unter Quantum Key Distribution (QKD) versteht man Verfahren für quantencomputerresistente Schlüsseleinigung, deren theoretische Sicherheit auf quantenphysikalischen Prinzipien beruht. Das BSI betrachtet QKD als mögliche Ergänzung zu Post-Quanten-Schlüsseleinigungsverfahren. Dies betrifft allerdings eher spezielle Anwendungsfelder, da die technischen Voraussetzungen für QKD stark limitierend sind.

Im Gegensatz zu klassischen und Post-Quanten-Algorithmen zur Schlüsseleinigung wird für den Einsatz von QKD spezielle Hardware benötigt, um Quantenzustände auszutauschen. Neben der theoretischen Sicherheit von QKD ist die Implementierungssicherheit zu berücksichtigen. Deshalb ist es wichtig, Evaluierungskriterien für QKD-Module zu entwickeln. Das BSI lässt derzeit in Zusammenarbeit mit ETSI ein Protection Profile nach den Common Criteria erstellen. Dieses beschränkt sich aber auf Punkt-zu-Punkt-Verbindungen und eine bestimmte Klasse von QKD-Protokollen, sogenannte Prepare-and-Measure-Protokolle. Sowohl verschränkungsbasierte QKD als auch Netzwerkaspekte bleiben vorerst offen. Das PP soll dem Evaluation Assurance Level EAL4+AVA_VAN.5+ALC_DVS.2 entsprechen, womit dem

Entwicklungsstand Quantencomputer

Um eine fundierte Einschätzung zum aktuellen Entwicklungsstand und der zukünftigen Verfügbarkeit von Quantencomputern zu erhalten, wurde vom BSI die Studie Entwicklungsstand Quantencomputer an Forscherinnen und Forscher der Universität des Saarlandes und der Florida Atlantic University in Auftrag gegeben und in den Jahren 2017 bis 2020 durchgeführt. Die Studie beleuchtet technologische Ansätze sowie quantenalgorithmische Innovationen und deren Implikationen im Kontext aktuell eingesetzter Kryptografie wie RSA und ECC. Bei den beiden Revisionen der Studie 2019 und 2020 hat sich gezeigt, dass algorithmische und technologische Fortschritte die Anzahl der benötigten physikalischen Quantenbits (Qubits) sowie die Größe der benötigten Quantenschaltkreise für eine gegebene Aufgabe reduzieren können. Speziell in der zweiten Revision 2020 wurde das Google-Experiment zur Quantenüberlegenheit (Quantum Supremacy) und weitere Heuristiken zur Optimierung beschrieben und im kryptografischen Kontext bewertet. Die Studie und eine Zusammenfassung stehen auf der Webseite des BSI zur Verfügung. Eine Fortsetzung der Studie ist in Planung.[dd)]

Einsatzbereich angemessen ein hohes Angriffspotenzial angenommen und der Lebenszyklus des Produktes mitberücksichtigt wird. Erste Entwürfe wurden unter anderem in der ETSI QKD Industry Specification Group verteilt und kommentiert. Für die spätere Anwendbarkeit des Protection Profile ist ein Zertifizierungsökosystem für QKD-Produkte aufzubauen, in dem Prüfkriterien und Bewertungsmethoden – beispielsweise für Seitenkanalangriffe – abgestimmt und weiterentwickelt werden.

Zurzeit werden in Deutschland und Europa zahlreiche Projekte im Bereich QKD gefördert. Im europäischen Projekt EuroQCI, dem mittlerweile 25 EU-Mitgliedsstaaten beigetreten sind, soll ein europäisches Quantenkommunikationsnetzwerk aufgebaut werden. Geplant sind eine terrestrische und eine satellitengestützte Komponente. Das BSI ist in der Security Group des Projekts vertreten. Zurzeit wird im Rahmen von EuroQCI eine Architekturstudie für ein Quantenkommunikationsnetzwerk erarbeitet, an der das BSI beratend beteiligt ist.

Die vom Bundesministerium für Bildung und Forschung (BMBF) geförderte Initiative QuNET erforscht verschiedene Aspekte der Quantenkommunikation. Für die neue Projektphase sind einige Demonstratorstrecken geplant. Das BSI begleitet die Forschungsinitiative als Mitglied im Beirat. Außerdem ist das BSI im Beirat des vom BMBF geförderten Projekts Q.Link.X beteiligt, in dessen Rahmen sogenannte Quantenrepeater erforscht werden. Diese sollen mittelfristig Ende-zu-Ende-Sicherheit fasergebundener QKD über längere Strecken sicherstellen.

In Hinblick auf die hohe Aufmerksamkeit und starke Förderung, die QKD zurzeit erfährt, besteht aus Sicht des BSI in vielen Feldern Handlungsbedarf, um die hohen Sicherheitsziele geplanter Implementierungen zu erreichen. Unter anderem sollten die Standardisierungsaktivitäten im Bereich QKD intensiviert sowie die Erforschung und Evaluierung der Implementierungssicherheit weiter vorangetrieben werden. Ferner sollten sich im Sinne der digitalen Souveränität auch europäische Hersteller von QKD-Produkten auf dem Markt etablieren. Das BSI selbst plant, einige Aspekte der theoretischen und praktischen Sicherheit von QKD in Studien weiter zu untersuchen.

2.5.4 Blockchain-Technologie

Im Bereich der Informationssicherheit gehört *Blockchain* immer noch zu den häufig diskutierten Themen. Wie bei allen neuen Technologien sollte auch bei der *Blockchain*-Technologie Sicherheit von Anfang an mitberücksichtigt und *Security by Design* angestrebt werden.

Ein Anwendungsgebiet für *Blockchain* wird im Bereich der Kryptowährungen gesehen. Daher hat das BSI 2021 im Rahmen seiner Veröffentlichungsreihe „*Blockchain* sicher gestalten“ ein Eckpunktepapier zur Sicherheit von DLT-basierten Kryptowährungen veröffentlicht. DLT steht für Distributed Ledger Technology und realisiert ein öffentlich zugängliches, dezentral geführtes Kontobuch; *Blockchain* ist ein Beispiel für DLT.

Das BSI hat in früheren Publikationen bereits die sichere Gestaltung von DLT-Anwendungen ausführlich thematisiert. Aufgrund der Aktualität des Themas werden in diesem Eckpunktepapier noch einmal explizit jene Aspekte zusammengestellt, die sich als die zentralen Faktoren für die IT-Sicherheit DLT-basierter Kryptowährungen herausgestellt haben.

In der Studie Sicherheitsuntersuchung ausgewählter *Blockchain*-Anwendungen hat das BSI einen Marktüberblick zu *Blockchain*-Anwendungen erstellt und ausgewählte Produkte aus unterschiedlichen Produktklassen exemplarisch evaluieren lassen. Die Hauptresultate der Studie sind auf der Webseite des BSI veröffentlicht:[ee)]

Hier stehen auch alle anderen Veröffentlichungen des BSI zur *Blockchain*-Technologie zum Download zur Verfügung.

3 Fazit

3 Fazit

Digitalisierung braucht Sicherheit

Auch in diesem Jahr steht der Bericht zur Lage der IT-Sicherheit in Deutschland unter dem Eindruck der COVID-19-Pandemie. Sie hat mit ihren gesamtgesellschaftlichen Auswirkungen auch Folgen für die Arbeitssituation in praktisch allen Behörden, Organisationen und Unternehmen. Dabei haben sich nicht nur mit der enormen Zunahme der Arbeit im Homeoffice neue Herausforderungen für die Informationssicherheit ergeben. Unternehmen fanden sich durch ihre besondere Rolle bei der Bekämpfung der Pandemie plötzlich mit einer ganz neuen Bedrohungslage konfrontiert – und die damit einhergehenden notwendigen Schutzmaßnahmen hatten sich schlagartig geändert. Diese neue Situation hat natürlich auch die Arbeit des BSI im vergangenen Jahr geprägt.

So hat etwa die Homeoffice-Studie des BSI gezeigt, welchem Risiko Unternehmen ausgesetzt sind: Bis zu 25 Prozent der befragten Unternehmen, die aktiv einen Cyber-Angriff abwehren mussten, beschrieben diesen als schwerwiegend oder existenzbedrohend. In Corona-Testzentren wurden wiederholt gravierende Schwachstellen in Webanwendungen gefunden: Sensible Daten wie Testergebnisse und Anschriften waren über das Internet missbräuchlich einsehbar. Und von besonderer Bedeutung waren Angriffe auf essentielle Einrichtungen wie die Europäische Arzneimittelagentur, Hersteller von Impfstoffen oder Krankenhäuser.

Das BSI arbeitet eng mit IT-Sicherheitsforscherinnen und -forschern zusammen, erkennt und reagiert auf derartige Angriffsversuche und Angriffe und kann so oftmals Schlimmeres verhindern. Das Grundproblem aber bleibt: Aus der Not geborene Digitalisierungsprojekte vernachlässigen die Informationssicherheit und gefährden damit ganze Unternehmensnetzwerke. Hastig zusammengeschusterte Software-Anwendungen gefährden die Sicherheit sensibler Daten – ein Risiko, das die betroffenen Verbraucherinnen und Verbraucher oftmals gar nicht erkennen können. Allzu oft wird schnelle Funktionalität über Sicherheit gestellt. Ein Risiko, das sich rächen kann und den Erfolg der Digitalisierung gefährdet.

Dass es auch schnell UND sicher funktioniert, hat die Corona-Warn-*App* (CWA) eindrucksvoll bewiesen. Entwicklungsbegleitend ist das BSI in die Sicherheitskonzeption eingebunden, prüft und testet die Anwendung regelmäßig. Bis heute sind keine IT-Sicherheitsvorfälle in Verbindung mit der CWA bekannt geworden. Auch für sicheres Homeoffice, sichere Unternehmensnetzwerke und für viele weitere digitale Anwendungen hat das BSI konkrete Empfehlungen bereitgestellt. Als Cyber-Sicherheitsbehörde des Bundes versteht sich das BSI als Gestalter einer sicheren Digitalisierung, die nur in dieser Kombination erfolgreich sein kann: Informationssicherheit und Digitalisierung sind zwei Seiten derselben Medaille und des BSI.

Cyber-Erpressungen entwickeln sich zur größten Bedrohung

Die Gefährdungslage wird allerdings nicht nur durch nachlässige IT-Sicherheitsmaßnahmen bestimmt. So konnte das BSI beobachten, dass nicht nur die Anzahl der Schadprogramm-Varianten zeitweise rasant anstieg, auch die Qualität der Angriffe nahm weiterhin beträchtlich zu. Insbesondere nehmen Cyber-Erpressungen inzwischen einen immer größeren Stellenwert ein. Cyber-Kriminelle verschlüsseln immer häufiger Daten von Unternehmen und Institutionen in ausgefeilten mehrstufigen Angriffen, um Lösegelder zu erpressen. Die Folgen sind oftmals fatal und können tage- oder wochenlange Netzwerkausfälle bedeuten, in denen Produktion oder Dienstleistungsangebote nur eingeschränkt oder gar nicht mehr zur Verfügung stehen.

Die Schadsoftware Emotet hat dabei eine entscheidende Rolle gespielt. Nach Schätzungen von Sicherheitsexpertinnen und -experten hat alleine Emotet weltweit einen Schaden von rund 2,5 Milliarden US-Dollar versursacht, der sich aus lahmgelegten IT-Infrastrukturen und erpressten Lösegeldern zusammensetzt. Und auch wenn es im Januar 2021 gelang, die Infrastruktur dieser Schadsoftware zu übernehmen und sie zu zerschlagen, ist die Gefahr nicht gebannt. Der BSI-Lagebericht zeigt deutlich, wie Cyber-Kriminelle ihre Angriffsmethoden weiterentwickeln.

Schwachstellen als eine der größten Herausforderungen

Eine erst im März 2021 geschlossene Lücke in Exchange-Servern von Microsoft steht dabei sinnbildlich für eine der größten Herausforderungen in der Informationssicherheit: den Umgang mit Schwachstellen. Cyber-Kriminelle sind aufgrund ihrer technischen Möglichkeiten sehr gut in der Lage, solche Schwachstellen auszunutzen. Das Besondere: Während Emotet noch auf einen Klick auf Links oder Dateianhang angewiesen war, kann in solchen Fällen eine Ausnutzung ohne weiteres Zutun der Anwenderinnen und Anwender erfolgen.

Direkt nach Bekanntwerden der Lücke wurden großflächig Versuche beobachtet, verwundbare Exchange-Server aufzuspüren und zu kompromittieren. Das BSI hat diese Lage als extrem kritisch eingeschätzt und die zweithöchste Krisenstufe („begrenzte IT-Krise“) ausgerufen. Es war erst das dritte Mal in seiner Geschichte, dass das BSI eine Warnung dieser Kategorie veröffentlicht hat. Zwar konnte der hohe Anteil verwundbarer Server von 98 Prozent (insgesamt waren in Deutschland rund 65.000 Server betroffen) nach zwei Wochen auf unter zehn Prozent gesenkt werden – allerdings bedurfte es dafür dringender Warnungen durch BSI und Microsoft an die betroffenen Unternehmen. Trotz allem waren im Mai 2021 noch immer mehr als 4.000 verwundbare Server auffindbar. Und auch wenn die Sicherheitslücke mit einem Update geschlossen wurde, müssen weitere Maßnahmen getroffen werden: Das BSI hält es für plausibel, dass es bereits zu Schadsoftware-Infektionen gekommen ist, bevor die Schwachstelle geschlossen wurde. Diese bestehenden Kompromittierungen können noch Wochen oder Monate später zu Cyber-Angriffen mit Schadenswirkung führen. Bei den Betroffenen können somit buchstäblich Zeitbomben in den Servern ticken.

Über den Warn- und Informationsdienst (WID) des *Computer Emergency Response Teams* der Bundesverwaltung (*CERT-Bund*) liefert das BSI regelmäßig, zeitnah und für die Empfänger in Staat, Wirtschaft und Gesellschaft kostenlos Informationen zu Schwachstellen und Sicherheitslücken sowie zu aktuellen Bedrohungen für IT-Systeme. Damit die Angebote des BSI aber wirken, ist es notwendig, dass Unternehmen und Institutionen sowie Privatpersonen diese Bedrohungen ernst nehmen und die erforderlichen Maßnahmen umsetzen. Dass dies leider noch nicht im ausreichenden Maße der Fall ist, zeigt sich am Fall „Exchange“, konnte aber auch im Rahmen der BSI-Studie zur Sicherheit im Homeoffice nachgewiesen werden. Vor allem kleine und mittlere Unternehmen ergreifen immer noch zu wenige Sicherheitsmaßnahmen, um das Homeoffice ausreichend gegen Cyber-Angriffe zu sichern.

Cyber-Sicherheit made in Germany

Cyber-Sicherheit als Wettbewerbsvorteil für Unternehmen in Deutschland rückt damit mehr und mehr in den Fokus. Sowohl die Absicherung der Geschäftstätigkeiten der Unternehmen (Business Continuity) als auch die Sicherheit von IT-Produkten stellen dabei Ansatzpunkte für die Unterstützungsangebote des BSI dar. Dabei ist klar: Informationssicherheit muss zum Verkaufsargument werden! Sie schafft Vertrauen und sie schafft Akzeptanz bei Verbraucherinnen und Verbrauchern.

Das betrifft etwa das autonome Fahren, für das zwingend sichere Netze und sichere Technologien notwendig sind – niemand wird selbstfahrende Pkw nutzen, wenn die Sicherheit der Passagiere und der anderen Verkehrsteilnehmer nicht gewährleistet ist. Das BSI wirkt in zahlreichen nationalen wie internationalen Gremien und Ausschüssen an der Normung, Standardisierung und Zertifizierung dort verwendeter Technologien wie der Künstlichen Intelligenz (KI) mit und kooperiert dafür eng mit Wirtschaft und Wissenschaft. Zudem hat das BSI für das autonome Fahren und weitere Anwendungsbereiche der KI mit dem „Kriterienkatalog für KI-basierte *Cloud*-Dienste (AIC4)“ eine wichtige Grundlage geschaffen zur Steigerung der Cyber-Sicherheit für KI. Ein vergleichbarer einsetzbarer Prüfstandard für sichere KI-Systeme existierte bis dahin nicht.

Ein weiterer Punkt ist die Sicherheit von Medizinprodukten, die ebenfalls durch die zunehmende Vernetzung und durch den Einsatz von KI verbessert werden können, aber nur dann wirklich in der Praxis einsetzbar sind, wenn sie die Sicherheit der Patientinnen und Patienten nicht gefährden. Erfolgreiche BSI-Projekte wie „ManiMed – Manipulation von Medizinprodukten“ sind immens wichtig, können aber gegenwärtig nur einzelne Teilaspekte des großen Themas Cyber-Sicherheit im Gesundheitswesen beleuchten.

Darum blickt das BSI auch immer in die Zukunft. Neben der gemeinsam mit Forscherinnen und Forschern der Universität des Saarlandes und der Florida Atlantic University durchgeführten Studie „Entwicklungsstand Quantencomputer“ ist das BSI unter anderem bei der Bewertung der sogenannten Quantum Key Distribution (QKD) aktiv, evaluiert und begleitet deren Einsatz. Die Liste der wissenschaftlichen Begleitung neuer Technologien lässt sich fortführen – um *Blockchain*, Smart Home und Smart City zum Beispiel.

Um seine Expertise für wichtige Themen zu bündeln, baut das BSI zudem Kompetenzzentren an seinen Standorten bzw. Stützpunkten auf. So wird in Freital ein Tätigkeitsschwerpunkt auf 5G/6G gelegt. Das BSI profitiert dabei von der starken Vernetzung mit dem Know-how vor Ort, das durch die Ansiedlung von weiteren wichtigen Technologieunternehmen in der Region noch einmal verstärkt wurde. Mit der Eröffnung des Stützpunktes in Saarbrücken im Juni 2021 treibt das BSI seine Aktivitäten im Bereich Künstliche Intelligenz weiter voran.

Doch so wichtig die Arbeit im Bereich der Forschung, Information und Prävention auch ist, sie allein reicht nicht aus. Es wird bei aller Prävention auch in Zukunft nicht möglich sein, sich vollständig gegen Angriffe zu schützen. Gerade der vergangene Berichtszeitraum zeigt wieder, wie schnell die Entwicklung voranschreitet und mit welcher Professionalität Cyber-Kriminelle inzwischen vorgehen.

Für Behörden, Unternehmen und andere Organisationen bedeutet dies, sich auf den Ernstfall vorzubereiten. Informationssicherheit muss strukturiert und mithilfe eines Informationssicherheitsmanagementsystems wie dem IT-Grundschutz implementiert und dauerhaft als Investition in den Unternehmenserfolg verstanden werden. Es ist zwingend erforderlich, den jeweiligen Stand der Technik umzusetzen, um die Geschäftsfähigkeit zu schützen. Nur so kann die Digitalisierung erfolgreich sein.

Blick in die Zukunft

Die vergangenen zwölf Monate haben unterstrichen, dass die Bedrohung durch Cyber-Kriminelle für eine digitale Gesellschaft weiter ansteigt. Zum einen verursachen sie hohe Schäden, wie im Fall des Angriffs auf die Ölversorgung in den USA, durch den eine tagelange Ölknappheit in einigen Regionen hervorgerufen wurde. Angriffe auf Unternehmen können zu starken Umsatzeinbußen bis hin zu einer Insolvenz führen. Cyber-Angriffe auf Krankenhäuser können im schlimmsten Fall Menschenleben in Gefahr bringen. Zum anderen untergraben Cyber-Kriminelle auch das Vertrauen in digitale Technologien. Ohne die Akzeptanz der Anwenderinnen und Anwender kann die Digitalisierung nicht erfolgreich umgesetzt werden. Sie kann darum nur erfolgreich verlaufen, wenn Cyber-Bedrohungen aktiv bekämpft werden und die Menschen in Deutschland, im Privaten und im Arbeitsumfeld, aufmerksam, informiert und umsichtig agieren können. Das aktive Eintreten gegen Cyber-Bedrohungen und die Sensibilisierung und Unterstützung der Menschen in Deutschland sind Kernaufgaben des BSI, das als Gestalter einer sicheren Digitalisierung eine zentrale Rolle innehat.

Bundeskanzlerin Dr. Angela Merkel hat diese Rolle in ihrem Grußwort zum diesjährigen Deutschen IT-Sicherheitskongress auf den Punkt gebracht: „Digitalisierung und Informationssicherheit gehören zusammen. Wir müssen in beiden Bereichen stark sein. Das entscheidet wesentlich darüber, wie erfolgreich Deutschland in Zukunft sein wird. Vor diesem Hintergrund zeigt sich, welch wichtige Rolle das BSI spielt und auch in Zukunft spielen wird."

Die sichere Entwicklung der Corona-Warn-*App*, die Entwicklung des weltweit ersten Standards für sichere KI-Anwendungen AIC4 und die Fortschreibung des IT-Sicherheitsgesetzes unterstreichen die Worte der Kanzlerin und zeigen die Möglichkeiten des BSI. Dem gegenüber steht jedoch die rasante Entwicklung im Bereich der Cyber-Bedrohungen: Angriffe mit höherer Durchschlagskraft, ein wachsender Anteil an Cyber-Erpressung und im Februar 2021 der höchste jemals gemessene durchschnittliche Tageszuwachs an neuen Schadprogramm-Varianten. Begünstigt wird diese Entwicklung durch die zunehmende Vernetzung, die mit immer weiteren digitalen Abhängigkeiten einhergeht - bei gleichzeitig immer noch zu beobachtender digitaler Sorglosigkeit. So bringt die Digitalisierung mit all ihren Chancen und Möglichkeiten auch viele Gefahren und eine wachsende Angriffsfläche mit sich.

Diese Entwicklung ist nicht nur in Deutschland sichtbar. Weltweit beobachten wir ein rasantes Fortschreiten der Digitalisierung. Der sprunghafte Anstieg der Datenvolumina ist nur ein Anzeichen dafür. Und diese Entwicklung wird nicht abreißen. Dennoch: 80 Jahre nachdem Konrad Zuse mit der Z3 den ersten funktionsfähigen Computer der Welt in Betrieb genommen hat, muss die Digitalisierung neu gedacht werden! Informationssicherheit muss einen deutlich höheren Stellenwert einnehmen und zur Grundlage aller Digitalisierungsprojekte werden. Der vorliegende Bericht zeigt deutlich wie nie zuvor, dass es eine erfolgreiche Digitalisierung von Staat, Wirtschaft und Gesellschaft nur mit einem richtigen Maß an Cyber-Sicherheit geben wird.

4 Glossar

Advanced Persistent Threats
Bei *Advanced Persistent Threats* (APT) handelt es sich um zielgerichtete Cyber-Angriffe auf ausgewählte Institutionen und Einrichtungen, bei denen sich ein Angreifer persistenten (dauerhaften) Zugriff zu einem Netzwerk verschafft und diesen in der Folge auf weitere Systeme ausweitet. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten aufseiten der Angreifer aus und sind in der Regel schwierig zu detektieren.

Affiliates
Bei *Cybercrime-as-a-Service* wird der Cyber-Kriminelle, der den Service in Anspruch nimmt, in der Regel als Affiliate bezeichnet. Der Begriff leitet sich aus dem Affiliate-Marketing ab, bei dem ein kommerzieller Anbieter seinen Vertriebspartnern (*Affiliates*) Werbematerial zur Verfügung stellt und eine Provision anbietet. Im Kontext des Cybercrime wird statt Werbematerial beispielsweise eine *Ransomware* zur Verfügung gestellt und dem Affiliate eine Beteiligung am Lösegeld versprochen.

Angriffsvektor
Als *Angriffsvektor* wird die Kombination von Angriffsweg und -technik bezeichnet, mit der sich ein Angreifer Zugang zu IT-Systemen verschafft.

Applikation / App
Eine *Applikation*, kurz *App*, ist eine Anwendungssoftware. Der Begriff *App* wird oft im Zusammenhang mit Anwendungen für Smartphones oder Tablets verwendet.

Authentifizierung
Die *Authentifizierung* bezeichnet den Vorgang, die Identität einer Person oder eines Rechnersystems anhand eines bestimmten Merkmals zu überprüfen. Dies kann u. a. durch Passworteingabe, Chipkarte oder Biometrie erfolgen.

Authentisierung
Authentisierung bezeichnet den Nachweis der Authentizität. Die *Authentisierung* einer Identität kann u. a. durch Passworteingabe, Chipkarte oder Biometrie erfolgen, die *Authentisierung* von Daten z. B. durch kryptografische Signaturen.

Backdoor
Ein *Backdoor* ist ein üblicherweise durch Viren, Würmer oder Trojanische Pferde installiertes Programm, das Dritten einen unbefugten Zugang (Hintertür) zum Computer verschafft, jedoch versteckt und unter Umgehung der üblichen Sicherheitseinrichtungen.

Backup
Unter Backup versteht man das Kopieren von Dateien oder Datenbanken auf physischen oder virtuellen Systemen an einen sekundären Speicherort, um diese im Falle eines Geräteausfalls oder einer Katastrophe für eine Wiederherstellung zu nutzen und bis dahin sicher vorzuhalten.

Bitcoin
Bitcoin (BTC) ist eine digitale Währung, sie wird auch Kryptowährung genannt. Durch Zahlungen zwischen pseudonymen Adressen wird die Identifizierung der Handelspartner deutlich erschwert.

Blockchain
Blockchain beschreibt eine verteilte, synchronisierte, dezentrale und konsensuale Datenhaltung in einem Peer-to-Peer-Netzwerk. Dabei wird redundant in allen Netzwerkknoten eine hashverkettete Liste von Datenblöcken geführt, die mit Hilfe eines Konsensverfahrens aktualisiert wird. *Blockchain* ist die technologische Grundlage für Kryptowährungen wie Bitcoin.

Bot / Botnetz
Als *Botnetz* wird ein Verbund von Rechnern (Systemen) bezeichnet, die von einem fernsteuerbaren Schadprogramm (*Bot*) befallen sind. Die betroffenen Systeme werden vom *Botnetz*-Betreiber mittels eines *Command-and-Control-Servers* (*C&C-Server*) kontrolliert und gesteuert.

CEO-Fraud
Als *CEO-Fraud* werden gezielte *Social Engineering*-Angriffe auf Mitarbeiterinnen und Mitarbeiter von Unternehmen bezeichnet. Der Angreifer nutzt hierbei zuvor erbeutete Identitätsdaten (z. B. Telefonnummern, Passwörter, E-Mail-Adressen etc.), um sich als Vorstandsvorsitzender (CEO), Geschäftsführung o. Ä. auszugeben und Mitarbeiterinnen und Mitarbeiter zur Auszahlung hoher Geldsummen zu veranlassen.

CERT / Computer Emergency Response Team
Computer-Notfallteam, das aus IT-Spezialisten besteht. In vielen Unternehmen und Institutionen sind mittlerweile *CERTs* etabliert, die sich um die Abwehr von Cyber-Angriffen, die Reaktion auf IT-Sicherheitsvorfälle sowie um die Umsetzung präventiver Maßnahmen kümmern.

CERT-Bund
Das *CERT-Bund* (*Computer Emergency Response Team* der Bundesverwaltung) ist im BSI angesiedelt und fungiert als zentrale Anlaufstelle für Bundesbehörden zu präventiven und reaktiven Maßnahmen bei sicherheitsrelevanten Vorfällen in Computersystemen.

Cloud / Cloud Computing
Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen

erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die im Rahmen von *Cloud Computing* angebotenen Dienstleistungen umfassen das komplette Spektrum der Informationstechnik und beinhalten u. a. Infrastrukturen (Rechenleistung, Speicherplatz), Plattformen und Software.

Command-and-Control-Server (C&C-Server)
Server-Infrastruktur, mit der Angreifer die in ein *Botnetz* integrierten infizierten Computersysteme (*Bots*) steuern. *Bots* (infizierte Systeme) melden sich in der Regel nach der Infektion bei dem C&C-Server des Angreifers, um dessen Befehle entgegen zu nehmen.

Cybercrime-as-a-Service (CCaaS)
Cybercrime-as-a-Service (*CCaaS*; Cybercrime als Dienstleistung) beschreibt einen Phänomenbereich des Cybercrime, bei dem Straftaten von Cyber-Kriminellen auftragsorientiert begangen bzw. dienstleistungsorientiert ermöglicht werden. So wird beispielsweise bei der dem *CCaaS* untergeordneten *Malware*-as-a-Service (*MaaS*) einem Cyber-Kriminellen von einem Außenstehenden oder einer darauf spezialisierten Angreifergruppe die *Malware* für die Begehung einer Straftat gegen Entgelt zur Verfügung gestellt und ggf. auch mit Updates und weiteren ähnlichen Servicen versorgt, ganz so, wie die legale Software-Industrie. Eine Art des *MaaS* ist *Ransomware*-as-a-Service *(RaaS)*, bei dem oft die *Malware* für die Verschlüsselung eines infizierten Systems, Aktualisierungen dieser *Malware*, die Abwicklung der Lösegeldverhandlungen und -zahlungen und weitere Erpressungsmethoden gegen Entgelt zur Verfügung gestellt werden. Die mit *CCaaS* einhergehende Zergliederung eines Cyber-Angriffs in einzelne Services ermöglicht auch wenig IT-affinen Angreifern technisch anspruchsvolle Cyber-Angriffe.

Deepfake
Der Begriff „*Deepfake*" ist eine umgangssprachliche Bezeichnung für Methoden, die dazu verwendet werden können, Identitäten in medialen Inhalten mit Hilfe von Methoden aus dem Bereich der künstlichen Intelligenz gezielt zu manipulieren. Ein Beispiel hierfür sind Verfahren, welche das in einem Video befindliche Gesicht einer Person mit dem Gesicht einer anderen Person tauschen, dabei jedoch die Gesichtsbewegungen unverändert lassen.

DoS / DDoS-Angriffe
Denial-of-Service (*DoS*)-Angriffe richten sich gegen die Verfügbarkeit von Diensten, Webseiten, einzelnen Systemen oder ganzen Netzen. Wird ein solcher Angriff mittels mehrerer Systeme parallel ausgeführt, spricht man von einem verteilten *DoS*- oder *DDoS* (Distributed Denial of Service)-Angriff. *DDoS-Angriffe* erfolgen häufig durch eine sehr große Anzahl von Computern oder Servern.

Drive-by-Download / Drive-by-Exploits
Drive-by-Exploits bezeichnen die automatisierte Ausnutzung von Sicherheitslücken auf einem PC. Dabei werden beim Betrachten einer Webseite ohne weitere Nutzerinteraktion Schwachstellen im Webbrowser, in Zusatzprogrammen des Browsers (*Plug-ins*) oder im Betriebssystem ausgenutzt, um Schadsoftware unbemerkt auf dem PC zu installieren.

Exploit
Als *Exploit* bezeichnet man eine Methode oder einen Programmcode, mit dem über eine Schwachstelle in Hard- oder Software-Komponenten nicht vorgesehene Befehle oder Funktionen ausgeführt werden können. Je nach Art der Schwachstelle kann mithilfe eines *Exploits* z. B. ein Programm zum Absturz gebracht, Benutzerrechte ausgeweitet oder beliebiger Programmcode ausgeführt werden.

Exploit-Kit
Exploit-Kits oder *Exploit*-Packs sind Werkzeuge für Cyber-Angriffe und werden auf legitimen Webseiten platziert. Mithilfe verschiedener *Exploits* wird automatisiert versucht, eine Schwachstelle im Webbrowser oder dessen *Plug-ins* zu finden und zur Installation von Schadprogrammen zu verwenden.

Firmware
Als *Firmware* bezeichnet man Software, die in elektronische Geräte eingebettet ist. Je nach Gerät kann *Firmware* den Funktionsumfang von z. B. Betriebssystem oder Anwendungssoftware enthalten. *Firmware* ist speziell auf die jeweilige Hardware zugeschnitten und nicht beliebig austauschbar.

Hashwert
Ein *Hashwert* ist eine aus der Anwendung einer bestimmten Hashfunktion resultierende Zeichenkette aus Ziffern und Buchstaben. Der *Hashwert* besitzt eine definierte Länge und ermöglicht es daher, große Datenmengen (z. B. ein Schadprogramm) exakt in vergleichsweise wenigen Zeichen abzubilden. Bei der Hashfunktion handelt es sich um eine mathematische Funktion zur Umrechnung von Daten. Eine anschließende Rückrechnung des *Hashwertes* in die ursprünglichen Daten ist praktisch kaum, bzw. nur unter extrem hohem Rechenaufwand möglich.

Internet der Dinge / Internet of Things / IoT
Unter *Internet der Dinge / Internet of Things (IoT)* versteht man informations- und sensortechnisch aufgerüstete Gegenstände, die aus der physischen und virtuellen Welt Daten erfassen, verarbeiten und speichern und miteinander vernetzt sind.

MaaS
Malware-as-a-Service (siehe auch *CCaaS*).

Maliziös
Boshaft, schädlich. In der IT-Sicherheit werden Programme oder Webseiten, die schädliche Operationen auf einem Computersystem ausführen können, als *maliziös* bezeichnet. Die englische Bezeichnung für Schadsoftware, *Malware*, ist ein Kunstwort aus Mal(icious) und (Soft)ware.

Malware
Die Begriffe Schadfunktion, Schadprogramm, Schadsoftware und *Malware* werden häufig synonym benutzt. *Malware* ist ein Kunstwort, abgeleitet aus Malicious Software und bezeichnet Software, die mit dem Ziel entwickelt wurde, unerwünschte und meistens schädliche Funktionen auszuführen. Beispiele sind Computerviren, Würmer und Trojanische Pferde. Schadsoftware ist üblicherweise für eine bestimmte Betriebssystemvariante konzipiert und wird daher meist für verbreitete Systeme und Anwendungen geschrieben.

Patch / Patch-Management
Ein *Patch* (Flicken) ist ein Software-Paket, mit dem Software-Hersteller Sicherheitslücken in ihren Programmen schließen oder andere Verbesserungen integrieren. Das Einspielen dieser Updates erleichtern viele Programme durch automatische Update-Funktionen. Als *Patch*-Management bezeichnet man Prozesse und Verfahren, die helfen, verfügbare *Patches* für die IT-Umgebung möglichst rasch erhalten, verwalten und einspielen zu können.

Payload
Allgemein bezeichnet *Payload* die Nutzlast bzw. die Nutzdaten einer Datenübertragung. Im Kontext der Informationssicherheit unterscheidet man zwischen Schadcode, der ein System für weitere Angriffe öffnet, Schadcode, der als temporäres Vehikel dient, und Schadcode, der letztlich auf dem System verbleiben soll. Letzterer Schadcode wird als *Payload* bezeichnet.

Phishing
Das Wort setzt sich aus Password und fishing zusammen, zu Deutsch: Nach Passwörtern angeln. Der Angreifer versucht dabei, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internetnutzers zu gelangen und diese für seine Zwecke meist zulasten des Opfers zu missbrauchen.

Phishing-Radar der Verbraucherzentrale NRW
Seit 2010 wertet die Verbraucherzentrale NRW betrügerische E-Mails aus, die Verbraucher an das *Phishing-Radar* weiterleiten (*phishing*@verbraucherzentrale.nrw). Auf Basis der täglich eingehenden 200-300 E-Mails - bei denen es sich um *Phishing*, sonstigen Cybercrime und Werbung handelt - wird auf der Homepage, auf Twitter und Facebook vor aktuellen Betrugsmaschen gewarnt. Seit dem Herbst 2017 findet eine Kooperation mit dem BSI statt, um unter anderem eine weitergehende statistische (anonymisierte) Auswertung zu ermöglichen.

Plug-in
Ein *Plug-in* ist eine Zusatzsoftware oder ein Software-Modul, das in ein Computerprogramm eingebunden werden kann, um dessen Funktionalität zu erweitern.

Potenziell unerwünschte Anwendung (PUA)
Anwendungssoftware (oft als Bundled-Software vertrieben), die nicht eindeutig als Schadsoftware klassifiziert werden kann. Eine *PUA* zeichnet sich insbesondere dadurch aus, dass sie in der Regel von Anwenderinnen und Anwendern zwar installiert wurde, jedoch ggf. nicht das erwartete Verhalten zeigt oder verdeckt Funktionen ausführt, die als unerwünscht angesehen werden, z. B. Informationssammlung und ggf. Weiterleitung des Anwenderverhaltens, Einblendung von Werbung oder Ähnliches.

Proliferation
Der Begriff stammt ursprünglich aus der militärischen Verteidigung und bezeichnet die Weitergabe von Massenvernichtungswaffen einschließlich ihres technischen Know-hows sowie des zu ihrer Herstellung benötigten Materials. In der IT-Sicherheit wird der Begriff entsprechend für die Weitergabe von Cyber-Waffen (Software und Methoden) unter Angreifern verwendet. Durch *Proliferation* können sich Angriffsmittel und -wege sehr schnell unter verschiedenen Angreifergruppierungen verbreiten, ohne dass diese jeweils spezifische technische Kompetenzen aufbauen müssen.

Provider
Dienstanbieter mit verschiedenen Schwerpunkten, z. B. Netzwerk-*Provider*, der als Mobilfunkprovider, Internet-Service-*Provider* oder Carrier die Infrastrukturen für den Daten- und Sprachtransport bereitstellt, oder Service *Provider*, der über die Netzwerkbereitstellung hinausgehende Dienstleistungen erbringt, beispielsweise den Netzbetrieb einer Organisation oder die Bereitstellung von Sozialen Medien.

Public-Key-Kryptografie
Bei der *Public-Key-Kryptografie* bzw. der asymmetrischen Verschlüsselung gibt es immer zwei sich ergänzende Schlüssel. Ein Schlüssel, der Public Key dient zur Verschlüsselung einer Nachricht, ein anderer – der Private Key – für das Entschlüsseln. Beide Schlüssel zusammen bilden ein Schlüsselpaar.

Ransomware
Als *Ransomware* werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes (Ransom) wieder freigeben. Es handelt sich dabei um einen Angriff auf das Sicherheitsziel der Verfügbarkeit und eine Form digitaler Erpressung.

RaaS
Ransomware-as-a-Service (siehe auch *CCaaS*).

Resilienz
Der Begriff bezeichnet im vorliegenden Zusammenhang die Widerstandsfähigkeit von IT-Systemen gegen Sicherheitsvorfälle oder Angriffe. Die *Resilienz* von Systemen ergibt sich aus einem komplexen Zusammenspiel von organisatorischen und technischen Präventivmaßnahmen wie zum Beispiel Fachpersonal, IT-Sicherheitsbudget, verfügbare technische Infrastrukturen u. Ä..

Responsible Disclosure
Als *Responsible Disclosure* wird ein Vorgang bezeichnet, bei dem nach dem Fund einer Sicherheitslücke zunächst der Hersteller des betroffenen Produkts detailliert informiert wird. Dies gibt dem Hersteller die Möglichkeit Gegenmaßnahmen zu entwickeln, z. B. in Form von Produktupdates, bevor die zur Ausnutzung der Lücke benötigten Informationen einer breiten Öffentlichkeit zugänglich gemacht werden. Dem Hersteller wird hierzu in der Regel ein fester Zeitrahmen vorgegeben, meist einige Monate, nach der spätestens eine Veröffentlichung erfolgt.

Security by Default
Ein Produkt, das nach *Security by Default* ausgeliefert wird, ist ohne zusätzliche notwendige Maßnahmen bereits in einem sicher vorkonfigurierten Auslieferungszustand.

Security by Design
Bei *Security by Design* werden Anforderungen aus der Informationssicherheit bereits bei der Entwicklung eines Produktes berücksichtigt.

Seitenkanalangriff
Angriff auf ein kryptografisches System, der die Ergebnisse von physikalischen Messungen am System (zum Beispiel Energieverbrauch, elektromagnetische Abstrahlung, Zeitverbrauch einer Operation) ausnutzt, um Einblick in sensible Daten zu erhalten. *Seitenkanalangriffe* sind für die praktische Sicherheit informationsverarbeitender Systeme von hoher Relevanz.

Sinkhole
Als *Sinkhole* wird ein Computersystem bezeichnet, auf das Anfragen von botnetzinfizierten Systemen umgeleitet werden. *Sinkhole*-Systeme werden typischerweise von Sicherheitsforscherinnen und -forschern betrieben, um Botnetzinfektionen aufzuspüren und betroffene Anwenderinnen und Anwender zu informieren.

Social Engineering
Bei Cyber-Angriffen durch *Social Engineering* versuchen Kriminelle, ihre Opfer dazu zu verleiten, eigenständig Daten preiszugeben, Schutzmaßnahmen zu umgehen oder selbstständig Schadprogramme auf ihren Systemen zu installieren. Sowohl im Bereich der Cyber-Kriminalität als auch bei der Spionage gehen die Angreifer geschickt vor, um vermeintliche menschliche Schwächen wie Neugier oder Angst auszunutzen und so Zugriff auf sensible Daten und Informationen zu erhalten.

Spam
Unter *Spam* versteht man unerwünschte Nachrichten, die massenhaft und ungezielt per E-Mail oder über andere Kommunikationsdienste versendet werden. In der harmlosen Variante enthalten *Spam*-Nachrichten meist unerwünschte Werbung. Häufig enthalten *Spam*-Nachrichten jedoch auch Schadprogramme im Anhang, Links zu verseuchten Webseiten oder sie werden für *Phishing*-Angriffe genutzt.

UP KRITIS
Der *UP KRITIS* (www.upkritis.de) ist eine öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen (KRITIS), deren Verbänden und staatlichen Stellen wie dem BSI.

VPN
Ein Virtuelles Privates Netz (*VPN*) ist ein Netz, das physisch innerhalb eines anderen Netzes (oft des Internets) betrieben wird, jedoch logisch von diesem Netz getrennt wird. In *VPNs* können unter Zuhilfenahme kryptografischer Verfahren die Integrität und Vertraulichkeit von Daten geschützt und die Kommunikationspartner sicher authentisiert werden, auch dann, wenn mehrere Netze oder Rechner über gemietete Leitungen oder öffentliche Netze miteinander verbunden sind.
Der Begriff *VPN* wird oft als Bezeichnung für verschlüsselte Verbindungen verwendet, zur Absicherung des Transportkanals können jedoch auch andere Methoden eingesetzt werden, beispielsweise spezielle Funktionen des genutzten Transportprotokolls.

Zwei- bzw. Mehr-Faktor-*Authentisierung*
Bei der *Zwei- bzw. Mehr-Faktor-Authentisierung* erfolgt die *Authentifizierung* einer Identität anhand verschiedener Authentifizierungsfaktoren aus getrennten Kategorien (Wissen, Besitz oder biometrischen Merkmalen).

5 Quellenverzeichnis

[1] *Die Lage der IT-Sicherheit in Deutschland 2020, Seite 11)*

[2] *https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2019.html*

[3] *https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound*

[4] *https://www.br.de/nachrichten/netzwelt/hacker-veroeffentlichen-passdaten-von-12-000-deutschen,SArrtc5*

[5] *https://www.bleepingcomputer.com/news/security/netwalker-ransomware-hits-argentinian-government-demands-4-million/*

[6] *https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-defenders-blog-netwalker/?hilite=%27ransomware%27%2C%27netwalker%27*

[7] *https://www.bleepingcomputer.com/news/security/princess-evolution-ransomware-is-a-raas-with-a-slick-payment-site/*

[8] *https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-defenders-blog-netwalker/?hilite=%27ransomware%27%2C%27netwalker%27*

[9] *https://www.bleepingcomputer.com/news/security/hackers-leak-files-stolen-in-pakistans-k-electric-ransomware-attack/*

[10] *https://www.heise.de/news/Hacker-veroeffentlichen-Daten-nach-Cyberangriff-auf-staedtische-IT-in-Oesterreich-4727538.html*

[11] *https://cyberflorida.org/threat-advisory/netwalker-ransomware-targets-philadelphia-health-system/*

[12] *https://www.br.de/nachrichten/netzwelt/hacker-veroeffentlichen-passdaten-von-12-000-deutschen,SArrtc5*

[13] *https://www.bleepingcomputer.com/news/security/netwalker-ransomware-hits-argentinian-government-demands-4-million/*

[14] *https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption)*

[15] *https://www.bleepingcomputer.com/news/security/largest-us-pipeline-shuts-down-operations-after-ransomware-attack/*

[16] *https://www.nytimes.com/2021/05/08/us/cyberattack-colonial-pipeline.html*

[17] *https://edition.cnn.com/2021/05/12/politics/colonial-pipeline-ransomware-payment/index.html*

[18] *https://www.intel471.com/blog/darkside-ransomware-shut-down-revil-avaddon-cybercrime*

[19] *https://www.intel471.com/blog/darkside-ransomware-shut-down-revil-avaddon-cybercrime*

[20] *https://www.bsi.bund.de/emotet*

[21] *https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2021/Presse2021/210127_pmEmotet.html*

[22] *Auswärtiges Amt, On the Application of International Law in Cyberspace, https://www.auswaertiges-amt.de/blob/2446304/2ae17233b62966a4b7f16d50ca3c6802/on-the-application-of-international-law-in-cyberspace-data.pdf*

[23] *FireEye, „Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor“, https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html*

[24] *Brad Smith, Microsoft, „A moment of reckoning: the need for a strong and global cybersecurity response“, https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/*

[25] *FireEye, „Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor“, https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html*

[26] *CrowdStrike, „SUNSPOT: An Implant in the Build Process“, https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/*

[27] *https://home.treasury.gov/news/press-releases/jy0127*

[28] *https://www.gov.uk/government/news/russia-uk-exposes-russian-involvement-in-solarwinds-cyber-compromise*

[29] *https://www.canada.ca/en/global-affairs/news/2021/04/statement-on-solarwinds-cyber-compromise.html*

[30] *Brad Smith, Microsoft, „A moment of reckoning: the need for a strong and global cybersecurity response“, https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/*

[31] *Paul R. Kolbe, New York Times, „With Hacking, the United States Needs to Stop Playing the Victim“, https://www.nytimes.com/2020/12/23/opinion/russia-united-states-hack.html*

[32] *Lawfare Blog, „The Strategic Implications of SolarWinds“, https://www.lawfareblog.com/strategic-implications-solarwinds*

[33] *https://www.link11.com/de/blog/20-jahre-ddos-ein-blick-zurueck-und-was-die-zukunft-bringt/*

[34] *https://it-online.co.za/2021/03/04/new-record-for-ddos-attacks-in-2020/*

[35] *https://www.link11.com/de/blog/bedrohungslage/ddos-report-angriffe-auf-rekordniveau-im-corona-jahr/*

[36] *https://techaeris.com/2015/11/08/protonmail-hit-massive-ddos-attack-pays-bitcoin-ransom/*

[37] *https://www.link11.com/de/blog/bedrohungslage/fancy-bear-warnung-ddos-erpressung/; https://blogs.akamai.com/sitr/2020/08/ransom-demands-return-new-ddos-extortion-threats-from-old-actors-targeting-finance-and-retail.html;*

[38] *https://blog.cloudflare.com/ransom-ddos-attacks-target-a-fortune-global-500-company/*

[39] *https://www.welivesecurity.com/deutsch/2020/08/28/ddos-erpresser-bedrohen-finanzunternehmen-und-einzelhaendler/*

[40] *https://www.zdnet.com/article/ddos-extortionists-target-nzx-moneygram-braintree-and-other-financial-services/*

[41] *https://ga.de/news/digitale-welt/schul-cloud-des-hpi-mit-ueber-einer-million-nutzern_aid-55700185*

[42] *https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Warn*
[43] *https://www.link11.com/de/blog/bedrohungslage/fancy-bear-warnung-ddos-erpressung/*
[44] *https://blogs.akamai.com/sitr/2020/08/ransom-demands-return-new-ddos-extortion-threats-from-old-actors-targeting-finance-and-retail.html*
[45] *https://www.link11.com/de/blog/bedrohungslage/armada-collective-ddos-erpressung-hostinganbieter/*
[46] *https://www.link11.com/de/blog/bedrohungslage/fancy-bear-warnung-ddos-erpressung/*
[47] *https://blogs.akamai.com/sitr/2020/08/ransom-demands-return-new-ddos-extortion-threats-from-old-actors-targeting-finance-and-retail.html*
[48] *https://www.link11.com/de/blog/bedrohungslage/armada-collective-ddos-erpressung-hostinganbieter/*
[49] *https://dd80b675424c132b90b3-e48385e382d2e5d17821a5e-1d8e4c86b.ssl.cf1.rackcdn.com/external/...*
[50] *https://belnet.be/fr/nouvelles-evenements/nouvelles/update-reseau-belnet-a-nouveau-disponible-nos-equipes-restent)*
[51] *Die Lage der IT-Sicherheit in Deutschland 2020*
[52] *Die Lage der IT-Sicherheit in Deutschland 2020, Seite 34*
[53] *http://de.statista.com/prognosen/801572/anzahl-der-smart-home-haushalte-nach-segmenten-in-europa*
[54] *https://www.bsi.bund.de/SharedDocs/Downloads/DE/ BSI/DigitaleGesellschaft/Pruefvorschrift_Produktgutachter_ePA-Frontend.pdf*
[55] *https://fachportal.gematik.de/ fileadmin/Fachportal/DVO/Informationsblatt_Betriebsarten-Konnektor_V1.0.0.pdf*
[56] *https://fachportal.gematik.de/ti-status/stoerung-vsdm*
[57] *https://e-health-com.de/details-news/ccc-hackt-bestellprozess-gematik-nimmt-stellung*
[58] *https://www.it-planungsrat.de/DE/Projekte/Koordinierungsprojekte/Portalverbund/Portalverbund_node.html*
[59] *https://www.heise.de/news/Deep-Fake-Politiker-fallen-auf-gefaketen-Nawalny-Vertrauten-rein-6027713.html*
[60] *Quelle: United Nations Economic Commission for Europe: ECE/TRANS/WP.29/2020/79 UN Regulation on uniform provisions concerning the approval of vehicles with regard to cyber security and of their cybersecurity management systems, Juni 2020*
[61] *https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5_AktuelleVersion/C5_Aktuelle Version_node.html*
[62] *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cloud-Computing/Anforderungskatalog/2020/C5_2020_Auswertungsleitfaden.xlsx*
[63] *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_Nutzung_externer_Cloud-Dienste.html*
[64] *https://www.destatis.de/DE/Themen/Branchen-Unternehmen/Transport-Verkehr/_Grafik/_Interaktiv/passagiere-luftverkehr.html*
[65] *https://signal.org/docs/specifications/doubleratchet/doubleratchet.pdf*
[66] *https://messaginglayersecurity.rocks/*
[67] *https://datatracker.ietf.org/wg/mls/about*
[68] *https://www.personalausweisportal.de/SharedDocs/downloads/Webs/PA/DE/informationsmaterial/weiterefuehrendes-material/Handlungsleitfaden_Integration_Smart-eID_Nutzerkonto.html*
[69] *https://www.etsi.org/committee/sai*
[70] *https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges*
[71] *https://www.din.de/de/forschung-und-innovation/ themen/kuenstliche-intelligenz/fahrplan-festlegen*
[72] *https://www.ki.nrw/flagships/zertifizierung/*
[73] *https://www.bsi.bund.de/SharedDocs/ Downloads/EN/BSI/Publications/ArtificialIntelligence/Empirical_robustness_testing_of_AI_systems_for_traffic_ sign_recognition.html*
[74] *https://www.bsi.bund.de/aic4*
[75] *http://www.bsi.bund.de/PQ-Migration*

Verzeichnis der im Dokument abgebildeten QR-Codes

a) *https://www.bsi.bund.de/ransomware*
b) *https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Unternehmen/Ich-habe-einen-IT-Sicherheitsvorfall-Was-soll-ich-tun/ich-habe-einen-it-sicherheitsvorfall-was-soll-ich-tun_node.html*
c) *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.html*
d) *https://www.bsi.bund.de/ransomware*
e) *https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/netze/Fragen-und-Antworten/fragen-und-antworten_node.html*
f) *https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/spam-phishing-co_node.html*
g) *https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Elektronische-Identitaeten/elektronische-identitaeten_node.html*
h) *https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/...Empfehlungen-nach-Gefaehrdungen/DDoS/ddos_node.html*
i) *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister-DDos-Mitigation-Liste.pdf*
j) *https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/KoViKo_140420.html*
k) *https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Remote/remote_node.html*
l) *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/empfehlung_home_office.html*
m) *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/gesundheitsapps.html*
n) *https://www.bsi.bund.de/VerbraucherInnen*
o) *https://einfachaBSIchern.de*
p) *https://www.bsi.bund.de/viva*
q) *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03162/BSI-TR-03162.pdf*
r) *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Sicher_zahlen_im_E_Commerce.html*
s) *https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0096_0096V2_0096V3.html*
t) *https://upkritis.de*
u) *https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Lageberichte/Cyber-Sicherheitsumfrage/IT-Sicherheit_im_Home-Office/it-sicherheit_im_home-office_node.html*
v) *https://www.bsi.bund.de/DE/Themen/Kampagne-einfach-absichern/Home-Office/home-office_node.html*
w) *https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Netzwerk-Formate/Medien/Cyber-Sicherheits-Podcast/cyber-sicherheits-podcast_node.html*
x) *https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_019.html*
y) *https://www.bsi.bund.de/Zulassung*
z) *https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Zulassung/VS-Anforderungsprofile/vs-anforderungsprofile_node.html*
aa) *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Herausforderungen_und_Massnahmen_KI.html*
bb) *https://www.bsi.bund.de/aic4*
cc) *https://www.bsi.bund.de/Quanten*
dd) *https://www.bsi.bund.de/qcstudie*
ee) *http://www.bsi.bund.de/blockchain*

Ihre Meinung ist uns wichtig!

Mit dem Bericht zur Lage der IT-Sicherheit in Deutschland informieren wir einmal im Jahr über aktuelle Entwicklungen und Gefahren für die Sicherheit in der Informationstechnik. Um den Bericht laufend zu verbessern und auf Ihre Bedürfnisse zuzuschneiden, möchten wir Ihre Meinung erfahren und Ihre Anregungen aufnehmen. Deshalb wären wir Ihnen sehr dankbar, wenn Sie an unserer kurzen Befragung teilnehmen. Ihre Angaben erfolgen anonym und werden selbstverständlich absolut vertraulich behandelt.

Über den folgenden Link gelangen Sie direkt zum Onlinefragebogen: *https://www.bsi.bund.de/leserbefragung*

Natürlich können Sie den Fragebogen auch auf Papier beantworten und an folgende Anschrift zurücksenden:
Bundesamt für Sicherheit in der Informationstechnik, Öffentlichkeitsarbeit, Postfach 200363, 53133 Bonn

1 Was ist für Sie der Hauptgrund, diesen Bericht zu lesen?

_____

_____

2 In welcher Rolle haben Sie diesen Bericht erhalten? *(Mehrfachnennungen möglich)*

- ☐ als Privatperson
- ☐ als Journalistin/Journalist
- ☐ als Mitarbeiterin/Mitarbeiter eines Unternehmens
- ☐ als Mitarbeiterin/Mitarbeiter einer Bundesbehörde
- ☐ als Mitarbeiterin/Mitarbeiter einer Landesbehörde oder kommunalen Behörde
- ☐ als Mitglied des Deutschen Bundestages
- ☐ als Mitarbeiterin/Mitarbeiter des Deutschen Bundestages
- ☐ als Mitglied oder Mitarbeiterin/Mitarbeiter eines Landtages, Kreistages usw.
- ☐ in einer Parteifunktion
- ☐ als Vertreterin/Vertreter von Vereinen oder Verbänden
- ☐ in einer anderen Rolle, und zwar:

  _____

3 In welcher Form liegt Ihnen dieser Bericht vor? *(Mehrfachnennungen möglich)*

- ☐ in gedruckter Form
- ☐ in elektronischer Form

4 Und in welcher Form nutzen Sie den Bericht hauptsächlich?

- ☐ Ich nutze ausschließlich die Print-Version.
- ☐ Ich nutze sowohl die Print-Version als auch die digitale Ausgabe.
- ☐ Ich nutze ausschließlich die digitale Ausgabe.
- ☐ Ich nutze hauptsächlich die Print-Version, aber auch die digitale Ausgabe.
- ☐ Ich nutze vor allem die digitale Ausgabe, aber auch die Print-Version.

5 In welcher Form möchten Sie zukünftig den Bericht lesen?

- ☐ in gedruckter Form
- ☐ in elektronischer Form
- ☐ ist mir egal

6 Auf welchem Wege haben Sie diesen Bericht erhalten? *(Mehrfachnennungen möglich)*

- ☐ Ich habe ihn selbst abonniert bzw. bestellt.
- ☐ Er wurde in meinem dienstlichen/geschäftlichen Umfeld abonniert.
- ☐ Ich habe ihn von der Website des BSI heruntergeladen.
- ☐ Ich habe ihn von einer anderen Person erhalten.

7 Wie viele Personen *außer Ihnen* lesen diesen Bericht zur Lage der IT-Sicherheit in Deutschland?
(Sollen sie dies noch nicht abschätzen können, lassen Sie das Feld frei.)

_____ weitere Personen

8 Falls noch weitere Personen diesen Bericht nutzen: Wer nutzt den Bericht außer Ihnen?

- ☐ Menschen, die in meinem Haushalt leben
- ☐ Mitarbeiterinnen/Mitarbeiter in der Abteilung, in der ich selbst arbeite
- ☐ Der Bericht wird allen Kolleginnen/Kollegen in der Behörde/im Unternehmen zugänglich gemacht
- ☐ Sonstiges, und zwar:

  _____

9 Der Bericht zur Lage der IT-Sicherheit in Deutschland erscheint jährlich im Herbst. Haben Sie diesen Bericht jetzt zum ersten Mal erhalten?

☐ ja ☐ nein, auch schon in den Vorjahren erhalten

10 Welche Teile des Berichts zur Lage der IT-Sicherheit in Deutschland lesen Sie? *(Mehrfachnennungen möglich)*

☐ Ich lese den kompletten Bericht durch.
☐ Informationen zur aktuellen Lage der IT-Sicherheit in Deutschland
☐ Informationen zu aktuellen IT-Sicherheitsvorfälle
☐ Informationen zu zielgruppenspezifischen Erkenntnissen und Angeboten für Gesellschaft, Verbraucherinnen und Verbraucher
☐ Informationen zu zielgruppenspezifischen Erkenntnissen und Angeboten für die Wirtschaft
☐ Informationen zu zielgruppenspezifischen Erkenntnissen und Angeboten für Staat und Verwaltung
☐ Informationen zu den gesetzlichen Rahmenbedingungen
☐ Informationen zum BSI allgemein
☐ Ich hebe den Bericht als Nachschlagewerk auf.

11 Bitte geben Sie jeweils an, inwieweit die folgenden Aussagen Ihrer Meinung nach auf den aktuellen Bericht zur Lage der IT-Sicherheit in Deutschland zutreffen oder nicht zutreffen. (*1 bedeutet: „trifft voll und ganz zu" und 6 bedeutet „trifft überhaupt nicht zu".)*

Der Bericht zur Lage der IT-Sicherheit in Deutschland…	1	2	3	4	5	6
a) hat insgesamt eine gute Themenauswahl	☐	☐	☐	☐	☐	☐
b) enthält wichtige/interessante Informationen	☐	☐	☐	☐	☐	☐
c) enthält relevante Themen	☐	☐	☐	☐	☐	☐
d) ist eine gute Unterstützung für meine Arbeit	☐	☐	☐	☐	☐	☐
e) hat eine zeitgemäße Aufmachung,	☐	☐	☐	☐	☐	☐
f) enthält verständlich und hilfreich aufbereitete Grafiken	☐	☐	☐	☐	☐	☐
g) ist verständlich geschrieben	☐	☐	☐	☐	☐	☐
h) ist übersichtlich aufbereitet/gegliedert	☐	☐	☐	☐	☐	☐
i) gefällt mir insgesamt sehr gut	☐	☐	☐	☐	☐	☐
j) würde ich jederzeit weiterempfehlen	☐	☐	☐	☐	☐	☐
k) würde ich sehr vermissen, wenn es ihn nicht gäbe	☐	☐	☐	☐	☐	☐
h) könnte künftig ausschließlich in elektronischer Form erscheinen	☐	☐	☐	☐	☐	☐

12 Was vermissen Sie an diesem Bericht zur Lage der IT-Sicherheit in Deutschland? Über welche Themen möchten Sie gerne mehr lesen?

_____

_____

Zum Abschluss benötigen wir noch einige wenige statistische Angaben:

S1 Welchem Geschlecht ordnen Sie sich zu? ☐ männlich ☐ weiblich ☐ divers

S2 Würden Sie uns Ihr Alter verraten? _____ Jahre

S3 In welchem Bundesland bzw. in welchem Staat wohnen Sie? _____

Vielen Dank für Ihre Unterstützung! Wir wünschen Ihnen noch einen schönen Tag.

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
September 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, S. 8, S. 44-45, S. 46, S. 86: AdobeStock ©Inna;
S. 3: BMI; S. 4: BSI;

Grafiken
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Artikelnummer
BSI-LB21/510

www.bsi.bund.de