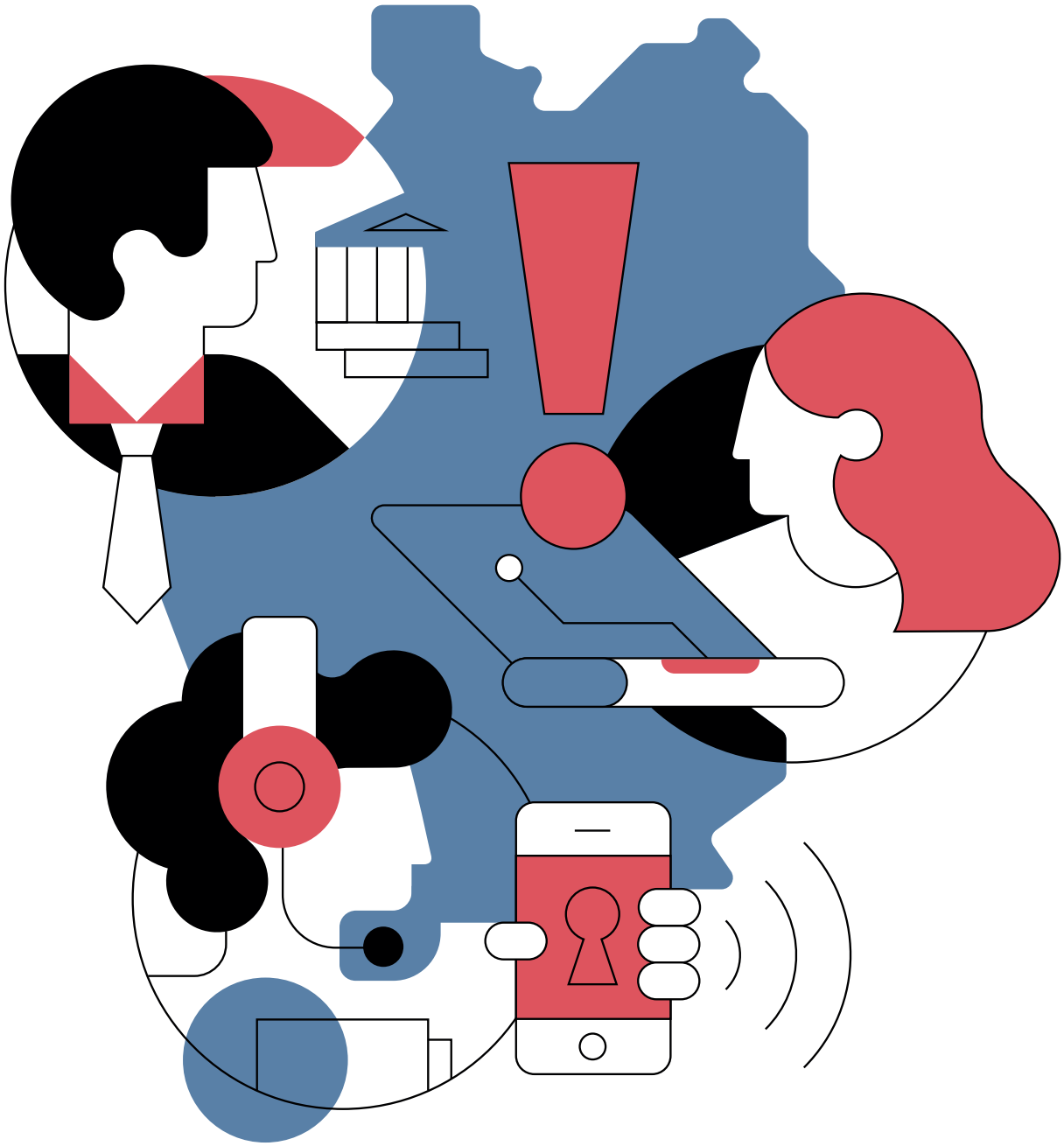
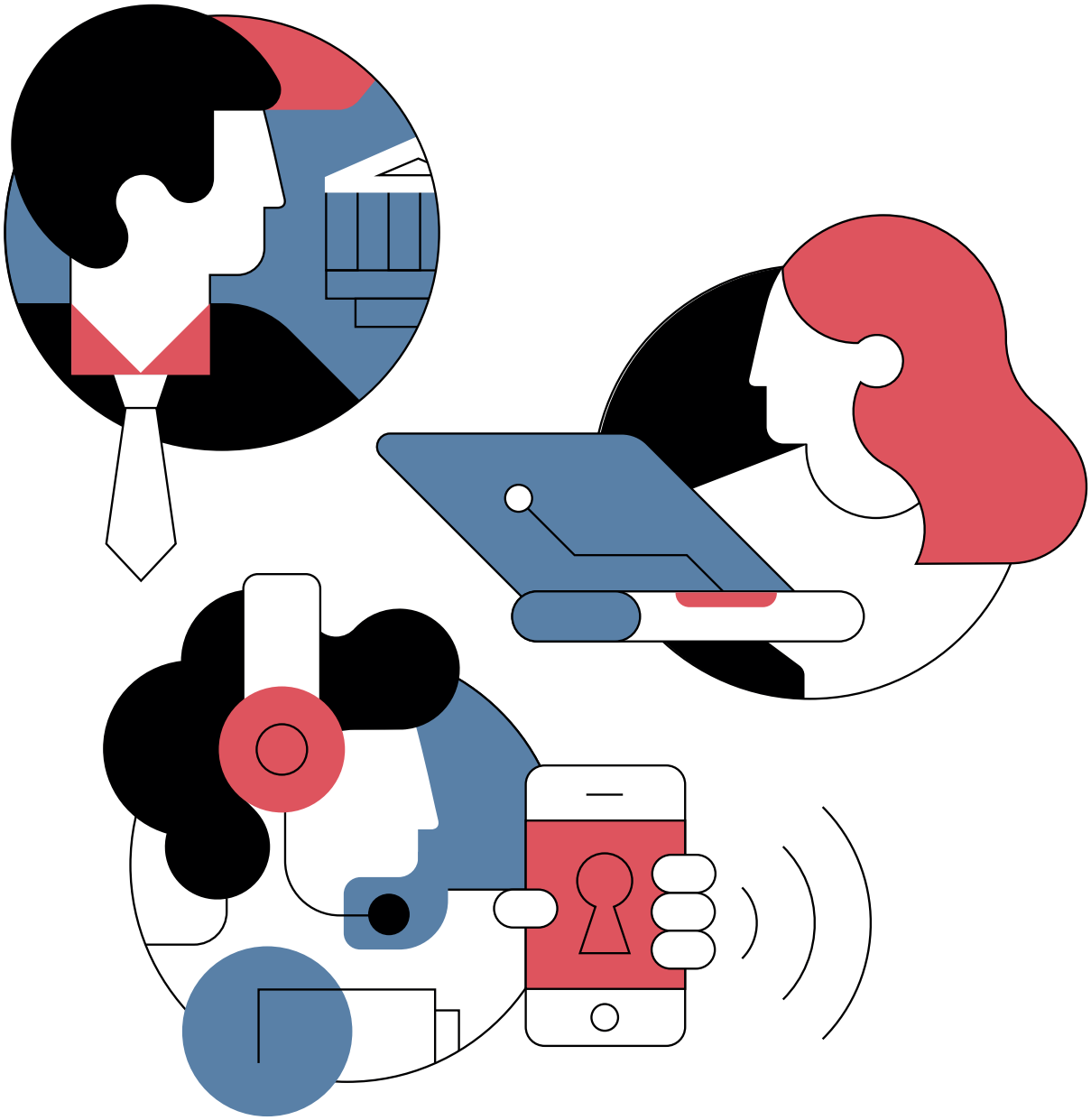
Die Lage der IT-Sicherheit in Deutschland 2022



Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Inhalt



Verzeichnis ausgewählter Vorfälle im Berichtszeitraum:

Abbildungsverzeichnis:

Vorwort

Nancy Faeser, Bundesministerin des Innern und für Heimat

Angesichts des russischen Angriffskrieges gegen die Ukraine sehen wir, wie eng äußere und innere Sicherheit miteinander zusammenhängen. Das gilt gerade für die Cyber-Sicherheit. Bedrohungen aus dem Cyber-Raum machen an keiner Grenze halt.

Cyber- und Informationssicherheit sind für mich wesentliche Schlüsselaspekte der Digitalisierung. Wir sehen, wie wichtig sichere digitale Systeme, Prozesse und Strukturen für eine wehrhafte Demokratie sind. Die Zeitenwende, die wir durch die Bedrohung des Friedens in Europa durchleben, erfordert deutliche Investitionen in unsere Cyber- und Informationssicherheit.

Der Bericht des BSI zur Lage der IT-Sicherheit in Deutschland 2022 bringt es auf den Punkt: Die Gefährdungslage im Cyber-Raum ist so hoch wie nie. Cyber-Kriminelle nutzen modernste Technologien für ihre Angriffe auf Privatpersonen, Unternehmen und staatliche Institutionen. Dem müssen wir entschieden entgegentreten. Die Bürgerinnen und Bürger erwarten von ihrer Regierung zu Recht, dass sie vorausschauend handelt und die Gesellschaft vor Gefahren im digitalen Raum schützt.

Mit der Cyber-Sicherheitsagenda des Bundesministeriums des Innern und für Heimat greifen wir diese Herausforderung auf. Wir streben damit u. a. eine starke Sicherheitsarchitektur und ein höchstmögliches Schutzniveau in der Cyber-Sicherheit an.

Ich bin froh, mit dem BSI und unseren anderen Sicherheitsbehörden starke und zuverlässige Partner an unserer Seite zu haben, die jeden Tag ihr Möglichstes leisten, um uns – Bürgerinnen und Bürger, Wirtschaft und Verwaltung – vor den Gefahren aus dem digitalen Raum zu schützen.

Vorwort

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

Deutschland · Digital · Sicher · BSI

Der vorliegende Bericht zur Lage der IT-Sicherheit in Deutschland betrachtet einen Zeitraum, der nicht nur durch die fortdauernden Auswirkungen der Corona-Pandemie, sondern auch durch die Folgen des russischen Angriffskriegs auf die Ukraine geprägt war.

Die durch die Erfahrungen der vergangenen Monate getroffene Risikoeinschätzung muss nun laufend weiterentwickelt werden. Denn es kam auch in Deutschland zu Kollateralschäden und einzelnen Cyber-Angriffen im Kontext des russischen Angriffskriegs gegen die Ukraine. Mehr als je zuvor haben uns diese Entwicklungen eindrücklich vor Augen geführt, wie zentral Cyber-Sicherheit für den Staat, für Unternehmen, Institutionen und nicht zuletzt auch für Verbraucherinnen und Verbraucher in einer zunehmend digital vernetzten Welt geworden ist.

Dabei war die Bedrohungslage auch vor dem Kriegsbeginn auf einem unverändert sehr hohen Niveau. Beispielsweise Ransomware-Angriffe bei IT-Dienstleistern, in Landkreisen und Kommunen sowie bei großen Unternehmen, Überlast-Angriffe (DDoS) auf Onlineshops an verkaufsstarken Tagen – all diese IT-Sicherheitsvorfälle machen deutlich, wie wichtig Informationssicherheit für unsere sichere Digitalisierung ist. Immer häufiger werden unbeteiligte Dritte durch Cyber-Angriffe beeinträchtigt. Dann zum Beispiel, wenn Bürgerinnen und Bürger kommunale Dienstleistungen nicht mehr in Anspruch nehmen können, weil Verwaltungen von *Ransomware* betroffen sind oder wenn Verbraucherinnen und Verbraucher ihre Einkäufe nicht bezahlen können, weil Anbieter durch Cyber-Angriffe handlungsunfähig sind. Insbesondere die Hersteller und Anbieter digitaler Angebote sind in der Pflicht:

Sie müssen ihrer Verantwortung gerecht werden und sicherstellen, dass die ihnen anvertrauten Daten nicht abhandenkommen oder missbraucht werden können. Des Weiteren müssen sie dafür sorgen, dass ihre digitalen Dienstleistungen sicher und Produkte uneingeschränkt verfügbar sind.

Diese Vorfälle belegen, dass die Gewährleistung von Cyber- und Informationssicherheit unmittelbarer Erfolgsfaktor für das Wohlergehen und den Schutz unserer Gesellschaft ist. Dass wir in Deutschland diesen Bedrohungen aber nicht schutzlos ausgeliefert sein müssen, macht der vorliegende Bericht ebenfalls deutlich. Das BSI als die Cyber-Sicherheitsbehörde des Bundes hat für alle Zielgruppen aus Staat, Wirtschaft und Gesellschaft seine Aktivitäten in Prävention, Detektion und Reaktion weiter gestärkt und ausgebaut. Dies war auch möglich, weil der Gesetzgeber im April 2021 mit dem *IT-Sicherheitsgesetz 2.0* wichtige Voraussetzungen hierfür geschaffen hat.

Doch die weiter zu beobachtende Professionalisierung der Cyber-Erpressungsmethoden, die weiterhin gravierenden Folgen von Ransomware-Angriffen, die weiter steigende Vielfalt von Schadprogramm-Varianten und auch kritische Schwachstellen in weit verbreiteten Software-Produkten wie Log4j legen offen, dass wir die Cyber-Sicherheit kontinuierlich weiter stärken müssen.

Die Herausforderungen im Cyber-Raum bleiben hoch und werden weiter rasant zunehmen. Um mit dieser Entwicklung nicht nur Schritt zu halten, sondern den Schutz vor Cyber-Angriffen in Deutschland und damit auch seine Zukunftsfähigkeit zu stärken, muss Informationssicherheit in Staat, Wirtschaft und Gesellschaft höchste Priorität haben. Ich begrüße deshalb ausdrücklich die von der Bundesregierung geplante weitere Modernisierung der Cyber-Sicherheitsarchitektur und den Ausbau des BSI zur Zentralstelle für Informationssicherheit im Bund-Länder-Verhältnis. Das BSI hat im Berichtszeitraum erneut bewiesen, dass es kompetent und schnell auf neue Herausforderungen reagieren kann. Ich bin mit Blick auf das Engagement und das hoch anerkannte Know-how der BSI-Mitarbeiterinnen und Mitarbeiter sicher, dass dies auch für zukünftige Aufgaben gilt.

Lage

1. Gefährdungen der Cyber-Sicherheit in Deutschland

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beobachtet als nationale Cyber-Sicherheitsbehörde kontinuierlich die Gefährdungslage der IT-Sicherheit in Deutschland. Im Fokus des BSI stehen Cyber-Angriffe auf Unternehmen, staatliche sowie öffentliche Institutionen und Privatpersonen, aber auch Maßnahmen zur Prävention und Bekämpfung dieser Lagen. Der vorliegende Bericht zieht eine Bilanz für die Zeit vom 1. Juni 2021 bis zum 31. Mai 2022 (Berichtszeitraum). Damit greift der Bericht aktuelle und unter Umständen anhaltende Cyber-Bedrohungen auf. Er bewertet auch die IT-Sicherheitslage im Kontext des russischen Angriffskrieges auf die Ukraine.

Anhand zahlreicher konkreter Beispiele aus vielen unterschiedlichen Bereichen zeichnet der Bericht den Weg und die typischen Methoden der Angreifer nach, um zugleich aufzuzeigen, wie sich Menschen und Organisationen schützen können. Die Übersicht beginnt 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 in einer digitalisierten Gesellschaft. Umso wichtiger ist es, jeden einzelnen Bereich mit seinen spezifischen Bedrohungen zu beleuchten und im weiteren Verlauf die Gegenmaßnahmen zielgruppenspezifisch darzustellen.

1.1 – Zusammenfassung und Bewertung

Insgesamt spitzte sich im Berichtszeitraum die bereits zuvor angespannte Lage weiter zu. Die Bedrohung im Cyber-Raum ist damit so hoch wie nie. Im Berichtszeitraum wurde – wie schon im Vorjahr – eine hohe Bedrohung durch Cybercrime beobachtet. *Ransomware* blieb die Hauptbedrohung (siehe Kapitel *Ransomware*, S. 13), besonders für Unternehmen. Hinzu kamen verschiedene Bedrohungen im Zusammenhang mit dem russischen Angriffskrieg auf die Ukraine, zum Beispiel durch Hacktivismus, insbesondere mittels Distributed-Denial-of-Service-Angriffen *(DDoS-Angriffen)*, und Kollateralschäden bei Cyber-Sabotage-Angriffen im Rahmen des Krieges. Sowohl durch Cybercrime als auch durch Cyber-Aktivitäten im Rahmen des Kriegs in der Ukraine hat es darüber hinaus im Berichtszeitraum Störungen von IT-Lieferketten gegeben. Eine Erhöhung der *Resilienz* gegenüber Cyber-Angriffen und technischen Störungen ist daher eine Hauptaufgabe für alle beteiligten Akteure in Staat, Wirtschaft und Gesellschaft.

Russischer Angriffskrieg gegen die Ukraine:

Bislang gab es in Deutschland im Zusammenhang mit dem Angriffskrieg Russlands gegen die Ukraine eine Ansammlung kleinerer Vorfälle und Hacktivismus-Kampagnen (vgl. zum Beispiel *Vorfall Kollateralschäden nach Angriff auf ein Unternehmen der Satellitenkommunikation*, Seite 49 und *Vorfall Cyber-Angriff auf deutschen Mineralölhändler*, Seite 50). Eine übergreifende Angriffskampagne gegen deutsche Ziele war nicht ersichtlich. Die Lage im Cyber-Raum von NATO-Partnern war dagegen teilweise angespannt und in der Ukraine teilweise existenzbedrohend kritisch.

Erpressungsmethoden im Cyber-Raum:

Die im vergangenen Berichtszeitraum beobachtete Ausweitung von Methoden der Erpressungsmethoden im Cyber-Raum hat sich im aktuellen Berichtszeitraum fortgesetzt. Insbesondere das sogenannte Big Game Hunting, also die Erpressung umsatzstarker Unternehmen mit verschlüsselten und exfiltrierten Daten, hat weiter zugenommen. Sowohl die von IT-Sicherheitsdienstleistern berichteten Lösegeld- und Schweigegeld-Zahlungen als auch die Anzahl der Opfer, deren Daten etwa wegen ausbleibender Zahlungen auf Leak-Seiten veröffentlicht wurden, sind weiter gestiegen. Zudem kam es im aktuellen Berichtszeitraum auch immer wieder zu Erpressungen mit erbeuteten Identitätsdaten.

Es ließen sich auch wieder mehrere, teils ungewöhnlich ausgeprägte Sextortion-Kampagnen beobachten. In diesen Spam-Mails behaupten Angreifer, über kompromittierende, intime Geheimnisse des Opfers zu verfügen und drohen, diese zu veröffentlichen. Um die Veröffent-

lichung der vermeintlich vorhandenen kompromittierenden Informationen zu verhindern, solle das Opfer einen bestimmten Betrag in einer Kryptowährung (z. B. *Bitcoin*) überweisen.

Schwachstellen:

Im Jahr 2021 wurden zehn Prozent mehr Schwachstellen bekannt als im Vorjahr. Mehr als die Hälfte von ihnen wiesen hohe oder kritische Scores nach dem Common Vulnerability Scoring System (CVSS) auf. Als besonders kritisch war die Schwachstelle in Log4j zu bewerten, da sich diese in vielen frei verfügbaren Software-Bausteinen befand. IT-Sicherheitsverantwortliche konnten daher in der Regel nur schwer einschätzen, ob die von ihnen eingesetzte Software die Schwachstelle aufwies. Aufgrund der hohen Verbreitung von Log4j war von einer großen Angriffsfläche für Cyber-Angriffe auszugehen.

Advanced Persistent Threats (APT):

Im aktuellen Berichtszeitraum waren vermehrt Angriffe auf *Perimeter-Systeme*, wie zum Beispiel Firewalls oder Router, zu beobachten. Während gezielte APT-Angriffe mittels Schadprogrammen in E-Mails in der Regel hohen Aufwand erfordern, sind *Perimeter-Systeme* direkt aus dem Internet erreichbar, vergleichsweise schlecht geschützt und daher leichter angreifbar. Mehr und mehr scannen APT-Gruppen das Internet nach bekannten Schwachstellen in *Perimeter-Systemen*, für die noch keine Patches verfügbar sind, um diese gezielt angreifen zu können.

Distributed Denial of Service (DDoS):

Nach Berichten verschiedener Mitigationsdienstleister hat die Zahl der *DDoS-Angriffe* weiter zugenommen. So verzeichnete etwa der deutsche Mitigationsdienstleister Link11 für das Jahr 2021 einen Anstieg der *DDoS-Angriffe* um rund 41 Prozent im Vergleich zum Vorjahr. Insbesondere rund um das jährliche Onlineshopping-Event Cyber Week und in der Vorweihnachtszeit waren spürbar mehr Angriffe zu beobachten. Rund um die Cyber Week 2021 hat sich die Zahl der *DDoS-Angriffe* gegenüber der Cyber Week 2020 verdoppelt.

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 von 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, kann sich das Schadprogramm installieren. Neben der E-Mail als Einfallstor zählen gefälschte Links in Webseiten sowie der Missbrauch von legitimen Programmen zu den typischen *Angriffsvektoren*. Für die Infektion angegriffener IT-Systeme nutzen Schadprogramme in der Regel Schwachstellen. Diese treten in Software- oder Hardware-Produkten auf sowie 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 beispielsweise Schadprogramme, die etwa durch Verschlüsselung den Zugang zu Daten oder Systemen einschränken, damit der Angreifer anschließend ein Lösegeld erpressen kann (für weitere Details siehe Kapitel *Ransomware*, Seite 13). Schadprogramme, die sich als gutartige Software tarnen oder in legitimen Dateien verstecken, werden als Trojaner bezeichnet. Bots heißen Schadprogramme, wenn sie sich zum Beispiel mit Hilfe von *Command-and-Control-Servern* fernsteuern lassen (vgl. Kapitel B*otnetze*, Seite 24).

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

1.2.1 — Neue Schadprogramm-Varianten

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

Die Anzahl neuer Schadprogramm-Varianten hat im aktuellen Berichtszeitraum um rund 116,6 Millionen zugenommen (vgl. Abbildung 1; Quelle dieser und der folgenden Daten: Malware-Statistik des BSI auf Basis von Rohdaten des Instituts AV-Test GmbH).

Durchschnittlich nahm die Zahl neuer Schadprogramm-Varianten täglich um knapp 319.000 zu. Das waren 19 Prozent weniger als noch im vergangenen Berichtszeitraum (vgl. Abbildung 2), der mit außergewöhnlich hohen Werten auffiel. Der Indikator hat sich damit wieder normalisiert. Allerdings waren erhebliche Schwankungen zu verzeichnen. Ließen sich im Sommer 2021 noch etwa 300.000 neue Varianten pro Tag zählen, so waren es im Herbst desselben Jahres bis zu 436.000 neue Schadprogramm-Varianten (vgl. Abbildung 3) pro Tag.

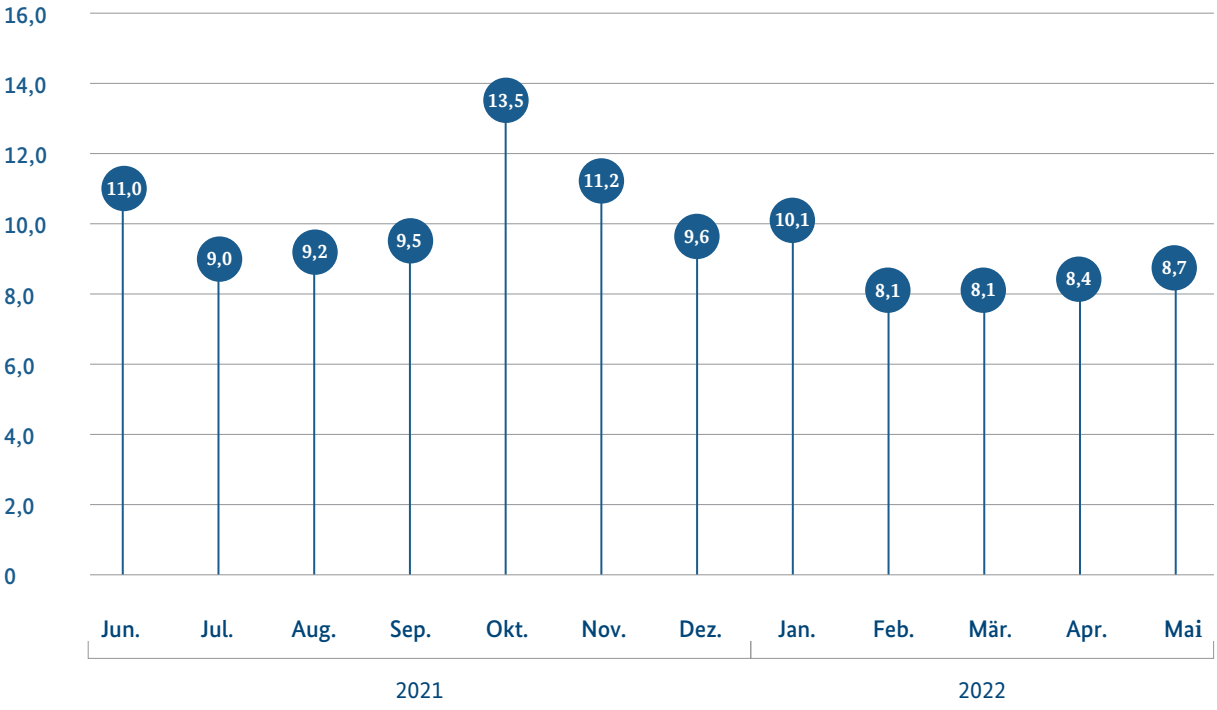
1.2.2 — Ransomware

Ransomware-Angriffe stellen eine der größten Cyber-Bedrohungen für Staat, Wirtschaft und Gesellschaft dar.

Ransomware ist eine Schadsoftware, die den Zugriff auf lokale oder vernetzte Daten und Systeme verhindert. Häufig verschlüsselt sie Nutzerdaten wie Office, Bild- und Videodateien oder ganze Dateninfrastrukturen wie Datenbanken oder Serversysteme. Anschließend hinterlassen die Angreifer eine Erpressernachricht. Die Daten lassen sich dann nur noch mit dem für die eingesetzte *Ransomware* spezifischen Tool entschlüsseln. Die Angreifer drohen bei der Erpressung damit, dieses

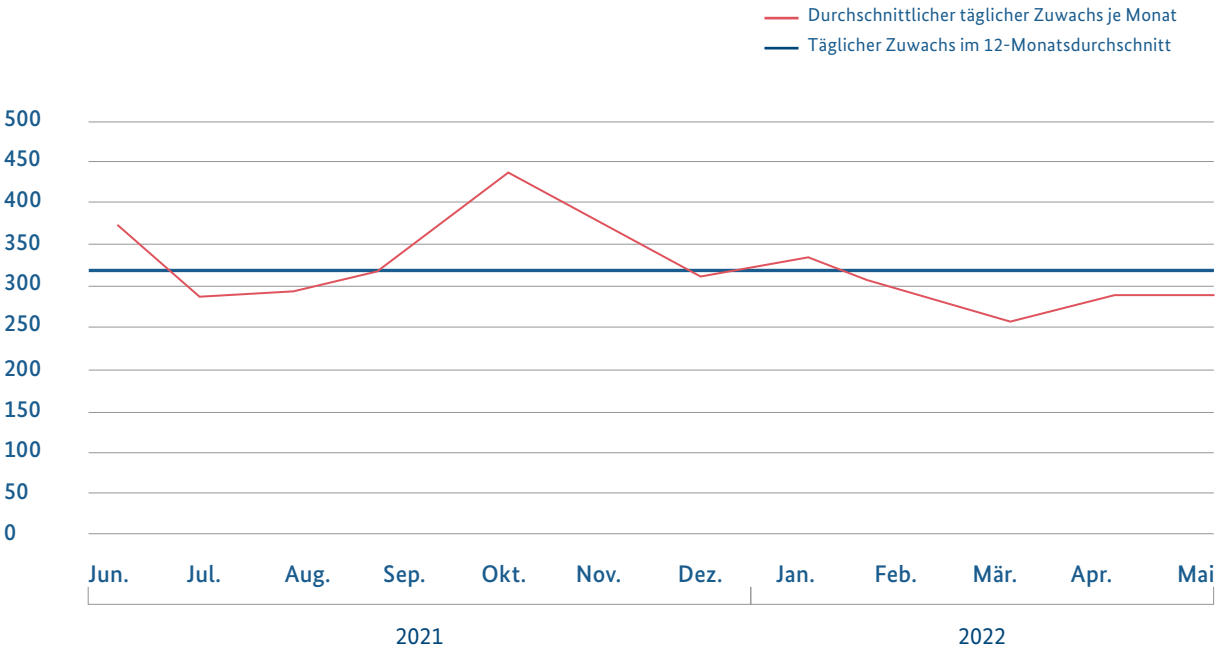
Neue Malware-Varianten von Juni 2021 bis Mai 2022
Anzahl in Millionen

Abbildung 1:
Quelle: Malware-Statistik des BSI auf Basis von Rohdaten des Instituts AV-Test GmbH



Durchschnittlicher täglicher Zuwachs neuer Malware-Varianten von Juni 2021 bis Mai 2022
Anzahl in Tausend

Abbildung 2:
Quelle: Malware-Statistik des BSI auf Basis von Rohdaten des Instituts AV-Test GmbH



Schlüsselmaterial zu vernichten. Zusätzlich stehlen sie vor der Verschlüsselung sensible Daten und drohen mit deren Veröffentlichung, um den Druck ihrer Forderungen zu erhöhen *(Double Extortion)*. Die Kombination dieser beiden Methoden (Lösegeld- und Schweigegelderpressung) ist im Berichtszeitraum zum Regelfall bei Ransomware-Angriffen geworden. Die Lösegeldzahlung wird üblicherweise in digitalen Währungen verlangt. Dies erschwert die Strafverfolgung, da sich solche Zahlungen nicht immer einer Einzelperson zuordnen lassen.

Ransomware-Angriffe werden überwiegend von cyber-kriminellen Angreifern verübt. Allerdings könnten APT-Angreifer sie auch nutzen, um andere Angriffe zu verschleiern bzw. von diesen abzulenken, oder sie zur reinen Sabotage einsetzen. Im Falle von Sabotage können die Angreifer ein Interesse am Lösegeld auch nur vorspielen bzw. technisch nie vorsehen, die Daten später wieder zu entschlüsseln. In dem Fall agiert die *Ransomware* als *Wiper* und die verschlüsselten Daten lassen sich technisch nicht wiederherstellen (zum Einsatz von *Wipern* im Rahmen des russischen Angriffskrieges gegen die Ukraine vgl. das Kapitel *Cyber-Sicherheitslage im Kontext des russischen Angriffskrieges gegen die Ukraine*, Seite 45).

Cyber-kriminelle Angreifer werden anhand der eingesetzten Schadsoftware und Vorgehensweise in Gruppen zusammengefasst. Die *Ransomware* Conti wird beispielsweise von einer anderen Gruppierung eingesetzt als die *Ransomware* LockBit 2.0.

Im cyber-kriminellen Raum hat sich in den vergangenen Jahren eine Form der Arbeitsteilung entwickelt: Bestandteile eines Cyber-Angriffs werden an jeweils spezialisierte Angreifergruppen ausgelagert. Dieses Phänomen lässt sich vergleichen mit dem Outsourcing von Dienstleistungen in der Privatwirtschaft. Es wird als *Cybercrime-as-a-Service (CCaaS, Cyber-Straftat als Dienstleistung)* bezeichnet. CCaaS erlaubt es einem Angreifer, nahezu jeden Schritt eines Angriffs als Dienstleistung oder zumindest die dafür notwendige Schadsoftware von anderen Cyber-Kriminellen zu beziehen. Das BSI nimmt an, dass dies ein treibender Faktor für die Zunahme der Bedrohung ist.

1.2.2.1 — Beispielhafter Angriffsablauf

Ein Ransomware-Angriff beginnt häufig mit einer *maliziösen Spam*- oder Phishing-Mail, der Kompromittierung eines Remote-Zugangs wie Remote Desktop Protocol (RDP) oder der Ausnutzung von Schwachstellen. Diese initiale Infektion stellt den Ausgangspunkt für das weitere Vorgehen des Angreifers dar.

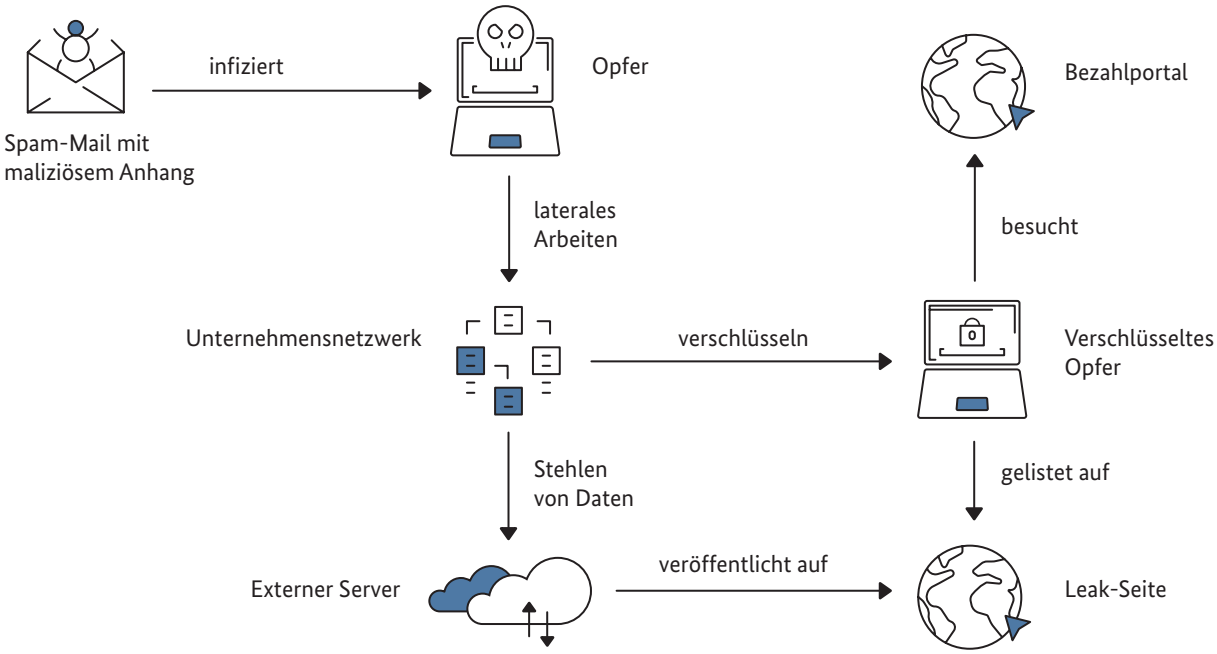
Im nächsten Schritt versucht ein Angreifer, sich lateral im IT-Netz des Betroffenen auszubreiten. Er verfügt dafür über verschiedene Mittel: Weitere Schadprogramme lassen sich einspielen, Zugangsdaten stehlen und Schwachstellen ausnutzen. Teilweise wird legitime Software missbraucht, die eigentlich für die Administration des IT-Systems verwendet wird. Die Aktivitäten des Angreifers wirken so zum Beispiel wie jene eines Administrators und bleiben länger unerkannt.

Hat ein Angreifer sich im IT-Netz ausreichend ausgebreitet, stiehlt er in der Regel sensible Daten. Auch hierfür stehen ihm verschiedene Werkzeuge zur Verfügung: von darauf ausgelegter *Malware* bis hin zu Software, die mit Cloud-Diensten zusammenarbeiten kann. Nach Abschluss des Datendiebstahls verteilt der Angreifer die *Ransomware* im IT-Netz. Alle kompromittierten Systeme werden verschlüsselt.

Der Angreifer hinterlässt abschließend eine Erpressernachricht auf den verschlüsselten Systemen (vgl. Abbildung 4). Darin wird der Betroffene über seine Situation aufgeklärt und zwecks Zahlungsabwicklung oft auch zum Besuch einer oder mehrerer Webseiten des Angreifers aufgefordert. So betreiben Angreifer teilweise gesonderte Seiten für einzelne Betroffene, über die Lösegeldzahlungen verhandelt und abgewickelt werden (vgl. Abschnitt *Lösegeld-Erpressung*, Seite 16). Zudem betreiben Angreifergruppen eigens eingerichtete Leak-Seiten, auf denen die Daten von Betroffenen veröffentlicht werden. Zu den Betroffenen werden teilweise Informationen wie Beschäftigtenzahl, Umsatz oder Branche angegeben. Angreifer veröffentlichen Daten, indem sie diesen Einträgen Links hinzufügen, über die sich die gestohlenen Daten abrufen lassen (vgl. Abschnitt *Schweigegeld-Erpressung*, Seite 16).

Beispielhafter Angriffsablauf

Abbildung 3:
Beispielhafter Ablauf eines Ransomware-Angriffs mit Lösegeld- und Schweigegelderpressung (schematische Darstellung)
Quelle: BSI



Beispiel einer Erpresser-Nachricht

Abbildung 4:
Beispiel einer Erpresser-Nachricht
Quelle: BSI

```
Your network has been breached and all data were encrypted.
Personal data, financial reports and important documents are ready to disclose.
To decrypt all the data and to prevent exfiltrated files to be disclosed at

http://hiveleakxxx.onion/

you will need to purchase our decryption software.

Please contact our sales department at:
   http://hivecustxxx.onion/
      Login:    Jxxx
      Password: gxxx

To get an access to .onion websites download and install Tor Browser at:
   https://www.torproject.org/ (Tor Browser is not related to us)

Follow the guidelines below to avoid losing your data:
 - Do not modify, rename or delete *.key.cggbt files. Your data will be
   undecryptable.
 - Do not modify or rename encrypted files. You will lose them.
 - Do not report to the Police, FBI, etc. They don't care about your business.
   They simply won't allow you to pay. As a result you will lose everything.
 - Do not hire a recovery company. They can't decrypt without the key.
   They also don't care about your business. They believe that they are
   good negotiators, but it is not. They usually fail. So speak for yourself.
 - Do not reject to purchase. Exfiltrated files will be publicly disclosed.
```

1.2.2.2 — Entwicklung der Bedrohungslage

Schweigegeld-Erpressung

Die Zahl der Opfer von Ransomware-Angriffen mit anschließender Schweigegeld-Erpressung nimmt stetig zu. Bekannt werden allerdings oft nur jene Fälle, in denen die Opfer weder Schweigegeld noch Lösegeld zahlten. Eine Statistik der Nachrichtenseite „The Record“ zählt die Opfer, deren Daten auf Leak-Seiten im Internet veröffentlicht wurden[1]. Demnach begannen Ende 2019 und Anfang 2020 die ersten Ransomware-Angreifer damit, Leak-Seiten und Schweigegeld-Erpressung als Druckmittel einzusetzen. In der zweiten Jahreshälfte 2020 entwickelte sich daraus ein Trend, dem mehr und mehr Cyber-Kriminelle folgten. Dies zeigt sich auch in der steten Zunahme der Daten-Leaks im selben Zeitraum (vgl. Abbildung 5).

Mehrere erfolgreiche international koordinierte Strafverfolgungsmaßnahmen wurden Anfang 2021 bekannt. Dabei wurden die Infrastruktur der Schadsoftware Emotet sowie die *Ransomware-as-a-Service (RaaS)*-Angebote von Netwalker und Egregor abgeschaltet. Es ist anzunehmen, dass diese Maßnahmen mitverantwortlich waren für den Rückgang von Daten-Leaks. *RaaS* ist eine Form von CCaaS, bei der der Angreifer die *Ransomware* und oft auch die damit in Verbindung stehende Infrastruktur vom Betreiber der *RaaS* erwirbt. Die Betreiber der *Ransomware* erhalten dafür gleichsam als „Provision“ einen Anteil des erpressten Geldes. Der Angreifer, der diese Dienstleistung bezieht, wird auch als „Affiliate“ bezeichnet.

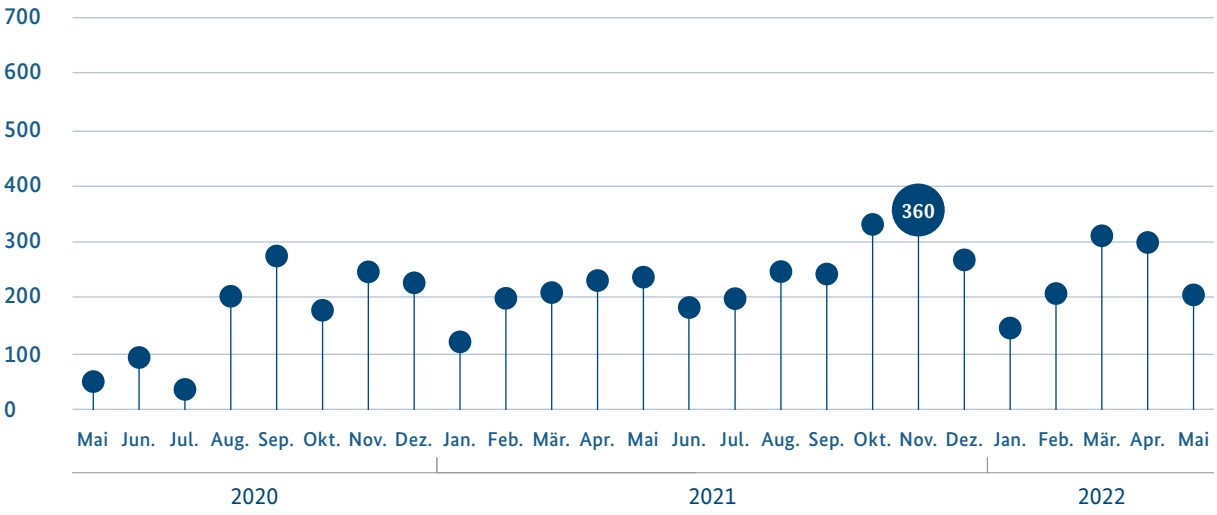
Bemerkenswert ist die Abnahme von Daten-Leaks nach Mai 2021 (vgl. Abbildung 5). Hintergrund ist, dass eine Reihe von RaaS-Angeboten eingestellt wurde. Allerdings versuchten bereits im Sommer 2021 mehrere, teilweise neue *RaaS*, die zuvor entstandene Marktlücke zu schließen. Allen voran ging die *RaaS* LockBit 2.0 gestärkt aus dieser Zeit hervor und stieg in der zweiten Jahreshälfte 2021 unter die drei führenden Ransomware-Familien auf (vgl. Abbildung 6). Weitere sind die *RaaS* Conti und die *Ransomware* Pysa.

Lösegeld-Erpressung

Die dem BSI gemeldeten Ransomware-Angriffe werden von einer mutmaßlich hohen Dunkelziffer an Vorfällen begleitet, die nicht bekannt werden. Statistiken von IT-Sicherheitsdienstleistern beschränken sich in der Regel auf deren jeweilige Kundenkreise, sodass absolute Zahlen über Ransomware-Vorfälle tendenziell untererfasst sind und stets vorsichtig interpretiert werden sollten. Unabhängig davon zeigen die meisten Quellen jedoch einen eindeutigen Trend: Der Betrag der erpressten Lösegelder nimmt zu. Die genaue Höhe unterscheidet sich von Quelle zu Quelle, da eine umfassende Datengrundlage fehlt und Lösegeldstatistiken sich jeweils nur auf die Kundenkreise einzelner

Entwicklung der Bedrohungslage Victim Data Released on Ransomware Extortion Site

Abbildung 5:
Opfer von Daten-Leaks von Jan. 2020 bis Mai 2022
Quelle: The Record



IT-Sicherheitsdienstleister beziehen. Eine Statistik des IT-Sicherheitsdienstleisters Coveware zeigt zum Beispiel die innerhalb eines Quartals gezahlten Lösegelder bei Vorfällen, die Coveware begleitete (vgl. Abbildung 7). Demnach stiegen die durchschnittlichen Lösegeldzahlungen von 84.116 US-Dollar im vierten Quartal 2019 auf 154.108 US-Dollar im vierten Quartal 2020 – ein Anstieg um zirka 183 Prozent. Den Höchstwert der durchschnittlichen Zahlungen beobachtete Coveware im vierten Quartal 2021 mit 322.168 US-Dollar, während zuvor im zweiten und dritten Quartal niedrigere Lösegeldzahlungen zu beobachten waren. Dieses vorübergehende Absinken geht wahrscheinlich hauptsächlich auf verstärkte Maßnahmen der Strafverfolger zurück, nachdem es 2021 mehrere größere Ransomware-Vorfälle gab (vgl. dazu auch Abschnitt *Schweigegeld-Erpressung*, Seite 16).

Erpressung mit erbeuteten Identitätsdaten

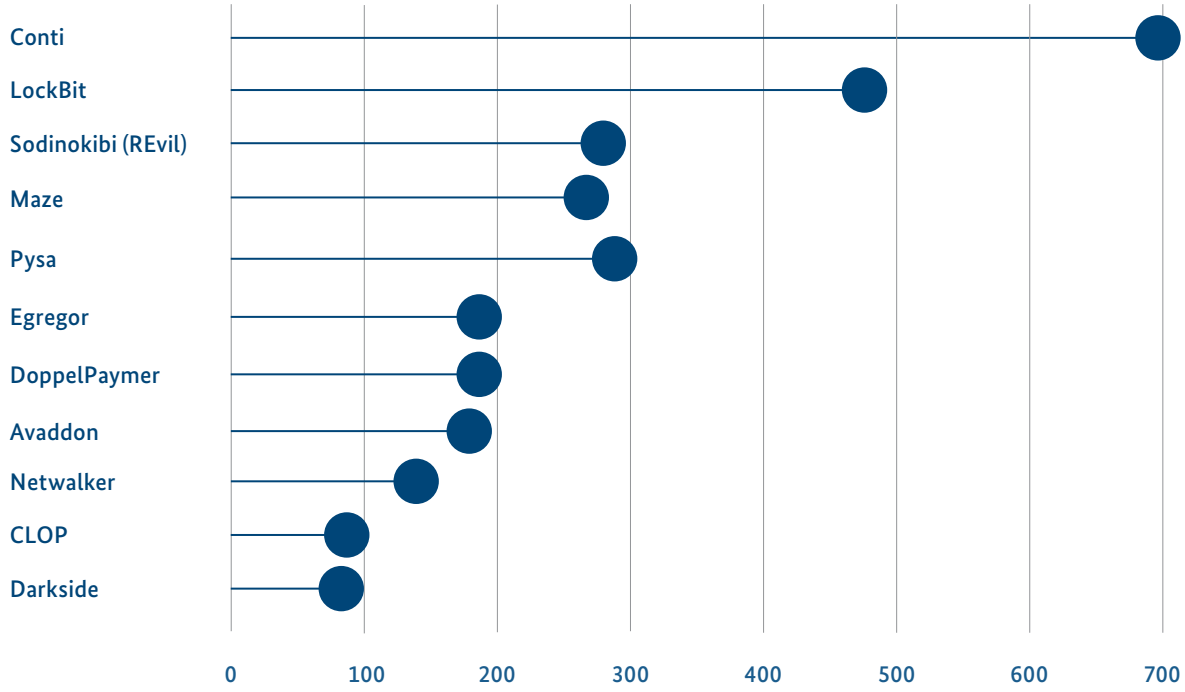
Für die oben beschriebene Schweigegeld-Erpressung (vgl. Abschnitt *Schweigegeld-Erpressung*, Seite 16) leiten Angreifer in der Regel große Datenmengen aus, die häufig auch Identitätsdaten sowie sensible Daten von Personen umfassen und auch auf entsprechenden Leak-Seiten gemeinsam mit den übrigen ausgeleiteten Daten veröffentlicht werden. Weiterhin drohen Angreifer während der Verhandlungsphase beispielsweise mit *DDoS-Angriffen* auf ohnehin schon von einem Ransomware-Angriff betroffene Opfer, um ihren Lösegeld- oder Schweigegeldforderungen weiteren Nachdruck zu verleihen.

Erbeutete Identitätsdaten ermöglichen den Angreifern, einen besonderen Erpressungsdruck auszuüben und das Angriffsopfer noch stärker zum Handeln zu zwingen. Angreifer setzen die Daten besonders für folgende weitere Erpressungsmethoden ein:

1. Erregung öffentlicher Aufmerksamkeit:
Einige Angreifer gehen aktiv auf Kundinnen und Kunden des Opfers oder die Öffentlichkeit zu, um zusätzlichen Druck auszuüben. Dies geht über die Veröffentlichung von Opferinformationen auf dafür eingerichteten Leak-Seiten hinaus. Beispielsweise wenden sich Angreifer per E-Mail an Kundinnen und Kunden oder Mitarbeitende eines Opfers und informieren diese darüber, dass aufgrund eines nicht gezahlten Schweigegelds sensible Daten über sie öffentlich wurden. Insbesondere bei einem intransparenten Umgang des Opfers mit möglicherweise von dem Daten-Leak Betroffenen kann dies den Ruf des Opfers langfristig schädigen. Eine pflichtgemäße Meldung an zuständige Datenschutz- oder Regulierungsbehörden kann die negativen Auswirkungen begrenzen.

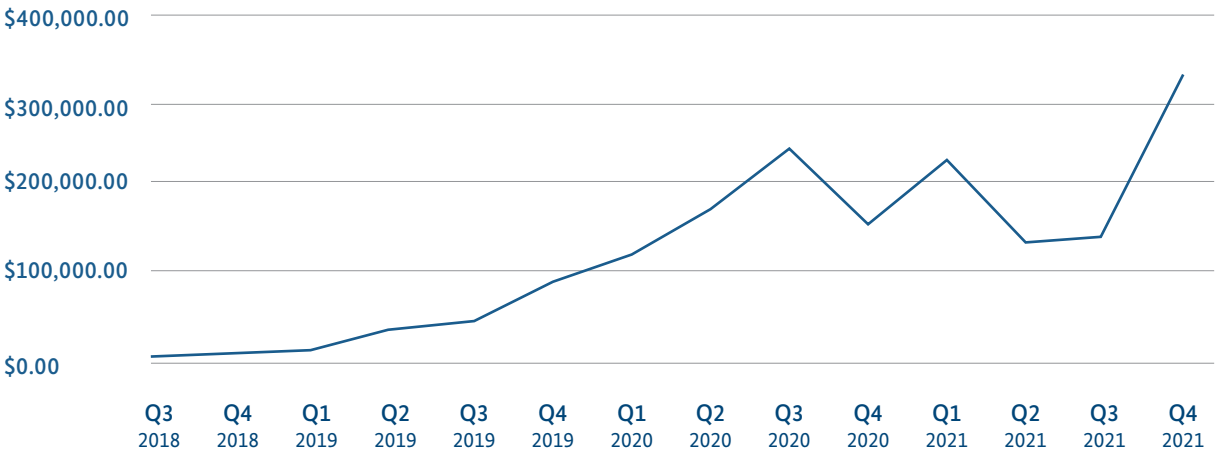
Opfer von Daten-Leaks nach Angreifer-Gruppe
Victims Posted to Extortion Sites

Abbildung 6: Opfer von Daten-Leaks nach Angreifer-Gruppe
Quelle: the Record



Durchschnittliche Lösegeldzahlungen pro Quartal

Abbildung 7:
Lösegeld-Zahlungen 2018 bis 2021
Quelle: Coveware



2. Verkauf sensibler Daten:
Ist der Betroffene nicht bereit zu zahlen, verkaufen oder versteigern einige Angreifer erbeutete Daten an Dritte. Zudem können die Käuferinnen und Käufer der erbeuteten Daten diese ihrerseits erpresserisch gegen das Opfer nutzen. Dies gilt insbesondere dann, wenn es sich um wertvolle Geschäftsgeheimnisse oder kompromittierende Informationen über Einzelpersonen handelt. An wen solche Daten schlussendlich versteigert werden, lässt sich in der Regel nicht mehr feststellen. Daten, die einmal abgeflossen sind, gelten somit im Fall einer erfolgten Schweigegeld- oder Lösegeldzahlung grundsätzlich dauerhaft als kompromittiert.

3. Androhen einer Meldung bei der zuständigen Datenschutz- oder Regulierungsbehörde:
Im Zusammenhang mit einem Cyber-Angriff können Betroffene gegen die Datenschutzgrundverordnung oder andere Regulierungen verstoßen, wenn sie beispielsweise ihren Meldepflichten nicht nachkommen oder nachweisbar ist, dass sensible Daten zum Beispiel auf schlecht abgesicherten Webservern lagen. Solche Sorgfaltspflicht- oder Meldepflichtverletzungen seitens der Opfer nutzen einige Angreifer als weiteres Druckmittel, indem sie drohen, Regulierungsbehörden über den Verstoß zu informieren. Da der Angriff sowie kompromittierte Daten auch über andere Wege öffentlich werden können, sollten Betroffene Gesetzesverstöße durch frühzeitige, pflichtgemäße Meldung vermeiden.

Die Ursachen für Daten-Leaks sind in vielen Fällen jedoch nicht nur Ransomware-Angriffe. Die unfreiwillige Veröffentlichung sensibler Daten durch die eigenen Dienstleister aufgrund fehlender adäquater Schutzmaßnahmen ist weiterhin keine Seltenheit und ließ sich im aktuellen Berichtszeitraum gehäuft beobachten. Das hat immer wieder zur Folge, dass sensible (oft personenbezogene) Daten ohne Beteiligung und in vielen Fällen ohne Kenntnis der Betroffenen an die Öffentlichkeit gelangen. So kam es im Jahr 2021 unter anderem dazu, dass ein fehlkonfiguriertes Gewinnspielportal einer großen deutschen Mediengruppe Dritten den Zugriff auf die Nutzerdaten der Teilnehmenden ermöglichte.

Zudem suchen Angreifer gezielt und häufig automatisiert nach fehlkonfigurierten Systemen sowie nach Schwachstellen, die den Abfluss von Identitätsdaten ermöglichen. Dafür nutzen sie spezielle Scan- und *Scraping*-Methoden. Im Berichtszeitraum ließen sich unter anderem Vorfälle beobachten, bei denen Schwachstellen bei mehreren deutschen Corona-Testzentren den Zugriff auf die Wohn- und E-Mail-Adressen, Telefonnummern, Geburtsdaten sowie die besonders schutzwürdigen Testergebnisse der Getesteten ermöglichten (vgl. Kapitel *Schwachstellen in Software-Produkten*, Seite 32).

Erste Beobachtungen deuten ebenfalls darauf hin, dass sich cyber-kriminelle Gruppen bilden, die vorrangig auf Daten-Leaks als Erpressungsmittel setzen. Solche Gruppen setzen keine *Ransomware* mehr ein, sondern beginnen ihre Erpressung direkt nach dem Datendiebstahl und können damit schneller von einer initialen Infektion in die Erpressung übergehen.

1.2.2.3 — Empfehlungen

Die wichtigste Voraussetzung für die Wiederherstellung der Betriebsfähigkeit nach einem Ransomware-Angriff ist eine klare Backup-Strategie. Diese umfasst die Verfügbarkeit funktionierender und aktueller *Backups*. Die Funktionsfähigkeit dieser *Backups* muss regelmäßig geprüft werden. Es ist inzwischen bei Schadprogramm-Infektionen üblich, dass Angreifende mit zuvor erlangten Administrationsrechten gezielt nach allen *Backups* suchen und diese, ebenso wie Produktivsysteme, verschlüsseln. Daher sollte zumindest je eine Kopie offline gesichert werden. Diese Kopien werden nach dem *Backup* von den anderen Systemen der Einrichtung getrennt und sind daher vor Remote-Angriffen geschützt.

Um der zunehmenden Ausleitung von Daten und der Drohung einer Veröffentlichung wirksam begegnen zu können, ist ein systematisches, regelgeleitetes Monitoring des Datentransfers erforderlich. So lässt sich etwa der Abfluss ungewöhnlich hoher Datenmengen erkennen und unterbinden.

Updates der Betriebssysteme sowie der Server- und Anwendungssoftware sollten regelmäßig und zeitnah durchgeführt werden. Zur Minimierung der Angriffsfläche sollte außerdem die Anzahl der von außen zugänglichen Systeme geringgehalten und deren Nutzung durch Unbefugte erschwert werden (zum Beispiel mittels Mehrfaktor-Authentisierung, Einsatz eines Virtuellen Privaten Netzes *(VPN)*, strengen Passwortvorgaben). Sachgerechte interne Segmentierung der IT-Netze und restriktive Administrationsrechte helfen, das Ausmaß der Schäden bei erfolgreichen Angriffen zu begrenzen. Für alle Institutionen sollten die umfassende und kontinuierliche Schulung aller Mitarbeiterinnen und Mitarbeiter zum Thema Informationssicherheit (Erhöhung der Aufmerksamkeit) und eine Beschränkung des administrativen Zugangs zu den Systemen auf möglichst wenige Personen selbstverständlich sein. Diese und ähnliche Maßnahmen dienen dazu, IT-gestützte geschäftskritische Prozesse möglichst resilient zu gestalten und dadurch widerstandsfähiger gegenüber Cyber-Angriffen zu machen.

Den Auswirkungen eines kurzfristigen Ausfalls von IT-gestützten Prozessen kann zudem mit der Etablierung von alternativen oder auch redundanten digitalen Diensten begegnet werden (zum Beispiel Content Delivery Networks (CDN) für Web-Präsenz, von einem Dienstleister bereitgestellte E-Mail-Services). Die Möglichkeit zur zeitnahen Wiederherstellung solcher Prozesse dient dazu, den gegebenenfalls aus einem Ausfall 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 dokumentiert 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.

Das BSI rät grundsätzlich davon ab, einer Lösegeldforderung nachzukommen, zumal in der Regel keine Garantie besteht, dass die Angreifer den Schlüssel tatsächlich herausgeben.

Weiterführende Informationen finden Sie hier:[a]

Katastrophenfall nach Ransomware-Angriff auf Kreisverwaltung

Sachverhalt
Eine Landkreisverwaltung in Sachsen-Anhalt wurde am 5. Juli 2021 zum Ziel eines Ransomware-Angriffs. Sämtliche IT-Systeme aller Standorte der Kreisverwaltung waren beeinträchtigt. In der Folge des Angriffs konnten keine Dienste für Bürgerinnen und Bürger erbracht werden. Am 9. Juli 2021 stellte der Landkreis den örtlichen Katastrophenfall fest. Am 2. Februar 2022 hob der Landkreis den Katastrophenfall auf. Zu diesem Zeitpunkt waren noch nicht alle Schäden wieder behoben, jedoch eine Funktionsfähigkeit wiederhergestellt.

Als ursächlich für den Vorfall wurde die Ransomware Grief identifiziert. Die Landkreisverwaltung zahlte kein Lösegeld. Die Angreifer veröffentlichten anschließend einige zuvor im Rahmen des Angriffs gestohlene Daten auf der Leak-Seite der Ransomware.

Bewertung
Der Ausfall bzw. die erhebliche Beeinträchtigung der kommunalen Verwaltungsprozesse kann zu vielfältigen Belastungen innerhalb der Bevölkerung führen. Dies gilt besonders für Personengruppen, die möglicherweise durch ausbleibende Zahlungen, etwa von Sozialleistungen oder Elterngeld, unmittelbar vom Ausfall kritischer Dienstleistungen betroffen sind.

Die Ransomware Grief wurde als Nachfolge der Ransomware DoppelPaymer identifiziert. Im cyber-kriminellen Umfeld kommt es wiederholt vor, dass Angreifer länger verwendete Namen ablegen. Im vorliegenden Fall stellten die Angreifer die Verwendung ihrer Ransomware DoppelPaymer ein und wechselten auf die teilweise neu entwickelte Ransomware Grief. Dieser als Rebranding bezeichnete Prozess erschwert die Zuordnung von Angriffen zu einzelnen Angreifern oder Angreifergruppen. Wenn ein Angriff einer bekannten Gruppe zugeordnet werden kann, erleichtert dies die gezielte Reaktion auf einen Vorfall.

Reaktion
Das Landeskriminalamt Sachsen-Anhalt und die zuständige Staatsanwaltschaft nahmen die Ermittlungen auf. Das BSI war mit einem mobilen Einsatzteam (MIRT, vgl. Kapitel Computer Emergency Response Team für Bundesbehörden, Seite 86) auf Anfrage der Landkreisverwaltung bereits am 8. Juli 2021 vor Ort. Das BSI unterstützte den betroffenen Landkreis außerdem bei der weiteren Koordinierung des Krisenmanagements von Bonn aus. Weiterhin analysierte das BSI die bei dem Vorfall eingesetzte Schadsoftware und beriet die Betroffenen hinsichtlich wesentlicher Sicherheitsanforderungen beim Wiederaufbau der IT-Infrastruktur. Die Maßnahmen des BSI wurden in enger Abstimmung mit der ebenfalls vom Landkreis angeforderten Unterstützung der Bundeswehr durchgeführt.

Ransomware-Angriff auf ein Handelsunternehmen

Sachverhalt
Im November 2021 wurde ein Handelsunternehmen aus dem Bereich der Unterhaltungselektronik Opfer eines Ransomware-Angriffs. Zu dem Unternehmen gehören zwei Elektronikmarktketten.

Laut Medienberichten waren offenbar die Warenwirtschaftssysteme und teilweise die Kassen in den Geschäften betroffen. Während der Verkauf von Bestandsware in den Filialen weiterhin funktionierte, seien Warenbestellungen, Rückgaben oder Abholungen nicht möglich gewesen. Es seien alle rund 1.000 Märkte beider Ketten in 13 europäischen Ländern betroffen gewesen, davon allein über 400 in Deutschland.

Ursprünglich seien von den Angreifern 240 Millionen US-Dollar Lösegeld gefordert worden. Die Forderung sei später auf 50 Millionen US-Dollar gesenkt worden. Für den Angriff wurde der RaaS Hive benutzt. Die Gruppe hinter der Ransomware listet auf deren Data-Leak-Seite das Unternehmen als Opfer auf. Möglicherweise ausgeleitete Daten wurden bisher nicht veröffentlicht.

Bewertung
Der Angriff fand unmittelbar vor dem „Black Friday“ und dem jährlichen Vorweihnachtsgeschäft statt – und damit zu einer traditionell umsatzträchtigen Zeit, zu der das Schadenspotenzial für den Einzelhandel besonders hoch ist. Dadurch entsteht ein entsprechend kritischer Handlungsdruck, auf die Lösegeldforderungen der Angreifer einzugehen. Der RaaS Hive war im Sommer 2021 zum ersten Mal in den Schlagzeilen. Das FBI warnte vor Hive, nachdem Ohios Memorial Health System Opfer dieser Ransomware wurde. Der hier beschriebene Vorfall passt in das Bild des Big Game Hunting, bei dem größere Organisationen angegriffen werden, weil von ihnen höhere Summen erpresst werden können.

Reaktion
Sowohl die zuständigen Strafverfolgungs- als auch die Datenschutzbehörden wurden von dem betroffenen Unternehmen informiert. Das BSI unterstützte mit einem MIRT-Team, forensischen Untersuchungen sowie dem Austausch von Indicators of Compromise (IoCs). Dabei handelt es sich um Merkmale eines Systems, kompromittiert zu sein.

Ransomware-Angriff auf Medizintechnologie-Unternehmen

Sachverhalt
Ein japanisches Medizintechnologie-Unternehmen, das auch mehrere Standorte in Deutschland unterhält, ist im September 2021 Opfer eines Ransomware-Angriffes geworden. Medienberichten zufolge waren die Standorte in Afrika, Europa und dem Mittleren Osten von dem Vorfall betroffen. Laut einer Pressemitteilung des Unternehmens wurden die Verkaufs- und Herstellungssektoren zeitweise durch den Angriff beeinträchtigt. Jedoch existieren bisher keine Hinweise darauf, dass Unternehmensdaten abgeflossen sind. Das betroffene Unternehmen gab an, dass nach der initialen Detektion des Vorfalls ein Einsatzteam mobilisiert wurde, um den Angriff zu untersuchen. Im Zuge dessen wurden die Systeme heruntergefahren und vom Netz genommen. Obwohl keine weiteren Informationen mitgeteilt wurden, gehen mehrere Quellen davon aus, dass es sich bei der eingesetzten Schadsoftware um die Ransomware BlackMatter handelte. Der Verdacht basiert auf mehreren Lösegeldforderungen, die auf den infizierten Systemen gefunden worden sind.

Bewertung
Die Ransomware BlackMatter wird als RaaS angeboten und kann somit auch von Affiliates, also weiteren Cyber-Kriminellen, käuflich erworben und für Angriffe genutzt werden. BlackMatter wird derselben Gruppe zugeordnet, die zuvor die RaaS Darkside entwickelt und betrieben hatte. Darkside war als RaaS von November 2020 bis Mai 2021 aktiv und wurde zuletzt im Vorfall gegen den US-Pipeline-Betreiber Colonial Pipeline eingesetzt (vgl. Die Lage der IT-Sicherheit in Deutschland 2021[2]). BlackMatter-Angriffe werden in der Regel von Forderungen nach Methode der Double Extortion, das heißt von Schutzgeld- und Schweigegelderpressungen, begleitet.

Reaktion
BlackMatter wurde vom BSI als ernstzunehmende Bedrohung bewertet. Die RaaS hat im November 2021 aus unbekannten Gründen den Dienst eingestellt.

1.2.3 — Botnetze

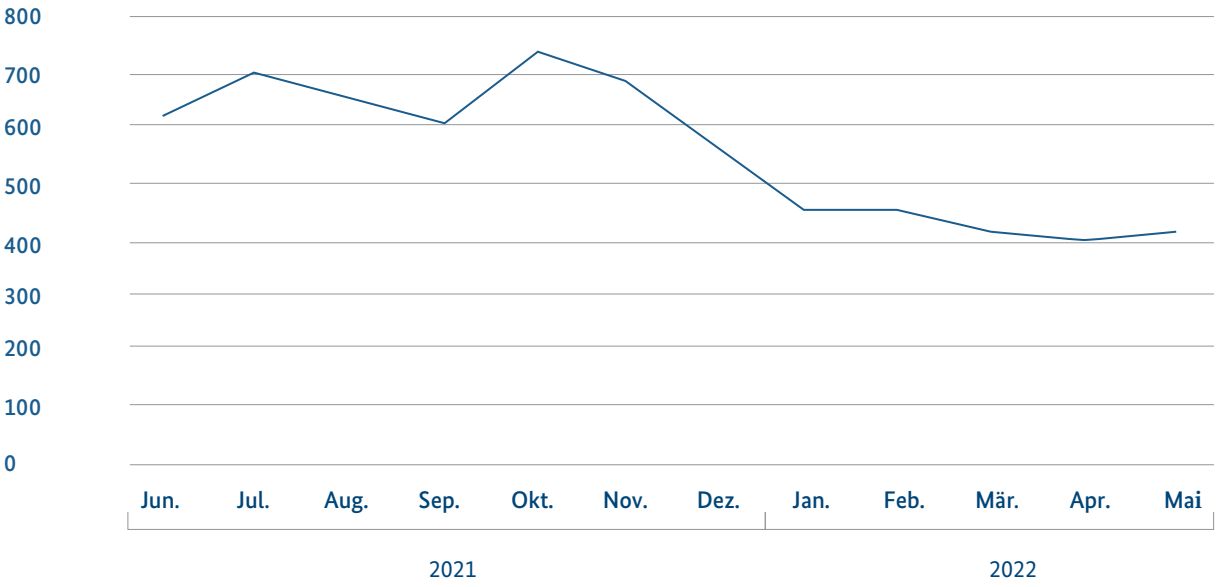
Als *Botnetz* bezeichnet man den Zusammenschluss mehrerer mit einem Schadprogramm infizierter Systeme (Bots), welche über ein zentrales Steuerungssystem, den sogenannten Command-and-Control Server, von einem Bot-Master kontrolliert werden können. Bot-Software existiert heutzutage für nahezu alle internetfähigen Geräte, somit können neben klassischen Computersystemen auch mobile Geräte wie Smartphones oder Tablets, aber auch Internet-of-Things-Geräte (IoT-Geräte) wie Router, Webcams oder Smart-TVs kompromittiert und von Angreifern übernommen werden.

Der modulare Aufbau aktueller Bot-Software ermöglicht den Bot-Mastern, die übernommenen Systeme zielgerichtet für eigene Zwecke zu nutzen, indem benötigte Funktionen durch Updates nachgerüstet werden. Dies umfasst einerseits direkte Schäden auf den infizierten Systemen, beispielsweise durch das Abgreifen persönlicher Daten, Onlinebanking-Betrug, Kryptomining oder auch Verschlüsselung der Gerätedaten. Andererseits können die Geräte auch Schäden auf den Systemen Dritter verursachen, etwa durch den Versand von Spam-E-Mails oder die Ausführung von *DDoS-Angriffen*.

Botnetze beobachtete das BSI in Deutschland im Berichtszeitraum mittels Sinkholing. Der Unique-IP-Index, der das Aufkommen und die Entwicklung der infizierten Systeme in den vom BSI beobachteten *Botnetzen* misst, lag im Durchschnitt des Berichtszeitraums bei 562 Punkten. Die Zahl der beobachteten infizierten Systeme, die täglich in *Botnetzen* aktiv waren, war damit 5,62-mal so groß wie im Jahresdurchschnitt 2019 (vgl. Abbildung 8). Wie auch im vergangenen Berichtszeitraum dienten Bots in erster Linie zum Ausspionieren persönlicher Informationen sowie zur Verbreitung weiterer Schadprogramme. Bei Massenangriffen standen insbesondere mobile Betriebssysteme auf Basis von Android sowie IoT-Geräte im Fokus. So blieb FluBot mit 37 Prozent der Bots die am häufigsten beobachtete Infektion sowohl im Android-Bereich als auch bei Bots allgemein, obwohl die Angreifer Maßnahmen gegen laufende Sinkholing-Verfahren ergriffen, um neue Infektionen unentdeckt zu lassen. Den zweiten Platz im Ranking der beobachteten *Botnetze* belegte ArrkiiSDK mit rund 13 Prozent der Bots. Diese Schadsoftware verfolgt das Benutzerverhalten und installiert unbe-

Unique-IP-Index[1] für Deutschland im Berichtszeitraum
2019 = 100

Abbildung 8:
Unique-IP-Index für Deutschland im Berichtszeitraum
Quelle: BSI

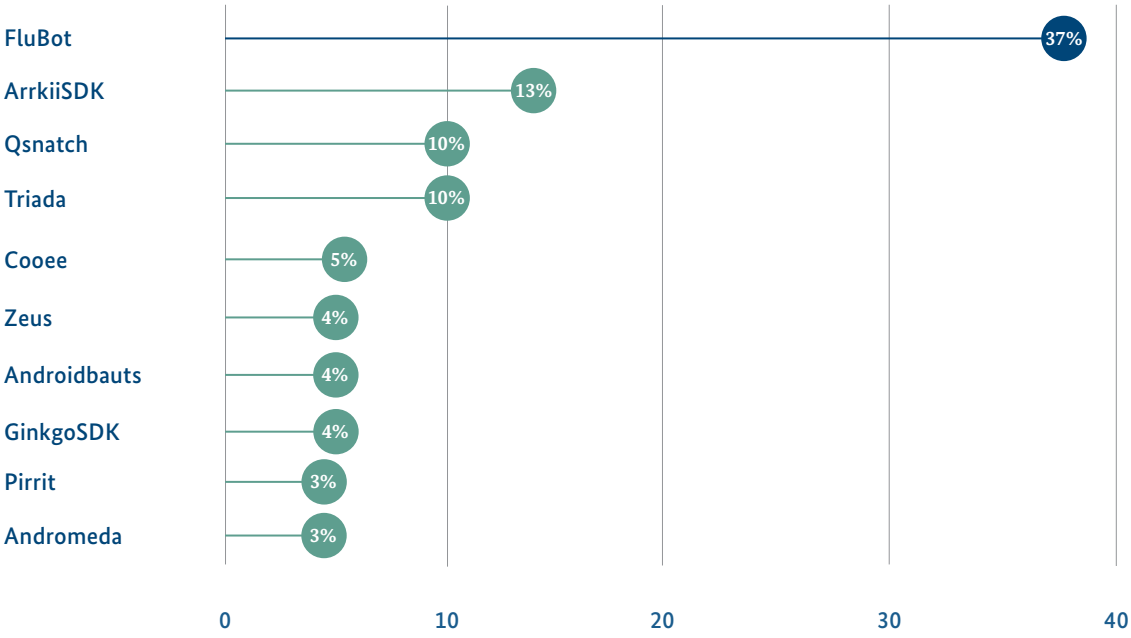


[1] Ohne infizierte IP-Adressen, die nicht im Sinkholding erfasst wurden

Bots (Unique IPs) je beobachtetes Botnetz in Deutschland im Durchschnitt des Berichtzeitraums

Anteil in % in allen Unique IPs

Abbildung 9:
Bots (Unique IPs) je beobachtetes Botnetz in Deutschland im Durchschnitt des Berichtszeitraums
Quelle: BSI



merkt weitere Anwendungen auf dem Mobiltelefon. Die am dritthäufigsten gemeldeten Infektionen betrafen mit rund zehn Prozent QSnatch. Diese Schadsoftware befällt die Netzwerkspeicher des Herstellers QNAP. Im Berichtszeitraum neu beobachtete Botnetz-Varianten zielten größtenteils vornehmlich auf die Android-Plattform.

Bei den gezielteren Angriffen auf finanzstarke Opfer standen primär populäre Server- und Desktop-Betriebssysteme wie Microsoft Windows und Linux im Fokus (vgl. Kapitel *Ransomware*, Seite 13). In diesem Bereich stand die Verbreitung von *Ransomware* an erster Stelle. Hier kam in Deutschland dem *Botnetz* Emotet eine besondere Rolle zu. (vgl. Vorfall *Emotet-Botnetz wieder aktiv*, Seite 26).

Im Berichtszeitraum gab das BSI täglich im Durchschnitt gut 41.100 Meldungen über potenzielle infizierte Systeme in Deutschland an die deutschen Netzbetreiber und Internet-Provider ab, die ihrerseits betroffene Kundinnen und Kunden ermittelten und benachrichtigten. Aufgrund von Mehrfachinfektionen ist von einer deutlich höheren Anzahl an Gesamtinfektionen auszugehen. Die Infektionsdaten stammen überwiegend von BSI-eigenen sowie externen *Sinkhole*-Systemen, die anstelle der regulären *Command-and-Control-Server* die Kontaktanfragen von Bots entgegennehmen und protokollieren. Eine Beschreibung des Sinkholing-Verfahrens sowie Steckbriefe zu den am häufigsten gemeldeten Schadprogrammfamilien finden sich auf der BSI-Webseite[3].

Wie schon in den Vorjahren ist die Bedrohung durch *Botnetze* anhaltend hoch. Die zunehmende Professionalisierung der Cyber-Kriminellen sowie der starke Zuwachs potenzieller Opfersysteme lässt erwarten, dass auch künftig die Zahl und Größe der *Botnetze* zunimmt. Die aus dem Sinkholing ermittelten Infektionszahlen stellen stets eine Untergrenze dar, da sich nur ein Teil der aktuell bekannten *Botnetze* aktiv überwachen lässt. So ergreifen aktuelle Botnetz-Familien wie Emotet, FluBot oder Glupteba Maßnahmen, um dem klassischen domänennamenbasierten Sinkholing zu entgehen, indem sie IP-Adressen, getunnelte DNS-Verbindungen (DNS over HTTPS, DoH) oder Blockchain-Techniken zur Kommunikation zwischen Steuerungsservern und Bots nutzen.

Emotet-Botnetz wieder aktiv

Sachverhalt
Seit Mitte November 2021 sind Anzeichen für einen Wiederaufbau des Emotet-Botnetzes zu beobachten. In einem koordinierten Takedown durch verschiedene internationale Strafverfolgungsbehörden, u. a. das Bundeskriminalamt (BKA), war das Emotet-Botnetz im Januar 2021 vom Netz genommen worden (vgl. Die Lage der IT-Sicherheit in Deutschland 2021[4]). Das BSI hatte zuvor mehrfach über Emotet berichtet und Cyber-Sicherheitswarnungen dazu herausgegeben. Die Schadsoftware Emotet zeichnet sich dadurch aus, dass sie Angriffstechniken massenhaft verwendet, die zuvor nur von aufwändigen APT-Angriffen auf ausgewählte Ziele bekannt waren. Emotet wurde daher auch als die gefährlichste Schadsoftware der Welt bezeichnet.

Der Takedown hatte zu einem monatelangen Stopp des Versands von Emotet-Spam geführt. Seit Mitte November 2021 erfolgte jedoch erneut regelmäßiger Spam-Versand zur Verbreitung der Schadsoftware Emotet über eine neue Infrastruktur der Angreifer.

Bewertung
Bislang hat die Verbreitung von Emotet in Deutschland und Europa noch nicht wieder das Niveau wie vor dem Takedown erreicht. Der Fokus der Angreifer scheint derzeit eher auf dem asiatischen Raum zu liegen.

Ein möglicher Grund hierfür ist, dass Ransomware-Angreifergruppen nach dem Takedown von Emotet auf andere „Türöffner" für den Zugang zu IT-Netzen potenzieller Opfer zurückgegriffen haben. Als ein Beispiel ist hier Qakbot zu nennen, das sich ähnlich wie Emotet über Spam-Mails mit gefälschten vermeintlichen Antworten auf ausgespähte E-Mails verbreitet.

Es ist jedoch jederzeit möglich, dass sich der Fokus der Emotet-Gruppe wieder in Richtung Europa wendet. Es wurden vereinzelte Spam-Wellen diesbezüglich beobachtet. Bei verstärkten Spam-Wellen könnte es erneut zu einem Anstieg der Infektionen und damit verbundenen Schäden kommen.

Reaktion
Das BSI hat im November 2021 eine Cyber-Sicherheitswarnung herausgegeben und vor einer möglichen Wiederaufnahme des Spam-Versands durch das Emotet-Botnetz gewarnt[5]. IT-Sicherheitsverantwortliche wurden gebeten, die Wirksamkeit ihrer Emotet-Schutzmaßnahmen zu überprüfen und sie ggf. zu aktualisieren.

1.2.4 — Spam und Phishing

Allgemein werden unerwünscht zugesandte E-Mails als *Spam* bezeichnet. Der Spam-Versand erfolgt zum Beispiel über kompromittierte oder kommerziell angemietete Server, über von Angreifern gestohlene legitime E-Mail-Accounts, deren Zugangsdaten zuvor ausgespäht worden sind (vgl. Abschnitt *Erpressung mit erbeuteten Identitätsdaten*, Seite 17), oder über infizierte Systeme, die zu Botnetzen zusammengeschlossen und dann für Spam-Dienstleistungen zu Verfügung gestellt werden (vgl. Kapitel *Botnetze*, Seite 24).

Bei Spam-Mails kann es sich sowohl um unerwünschten, aber im Grunde unschädlichen Werbe-*Spam* handeln als auch um Nachrichten mit Angriffshintergrund, wie etwa Erpressungs- oder Betrugs-Mails. Im Berichtszeitraum machte der Werbe-Spam rund 16 Prozent der Spam-Mails aus. Der größte Teil der Spam-Mails waren Cyber-Angriffe wie E-Mail-Erpressung mit 36 Prozent und E-Mail-Betrug mit 33 Prozent. Sonstige Spam-Mails machten 15 Prozent aus. Darunter war auch gefährlicher Malware-Spam, also Spam-Mails, mit denen massenhaft Schadprogramme verteilt werden (vgl. Abbildung 10).

Spam im Berichtszeitraum nach Art des Spam
Anteile in %

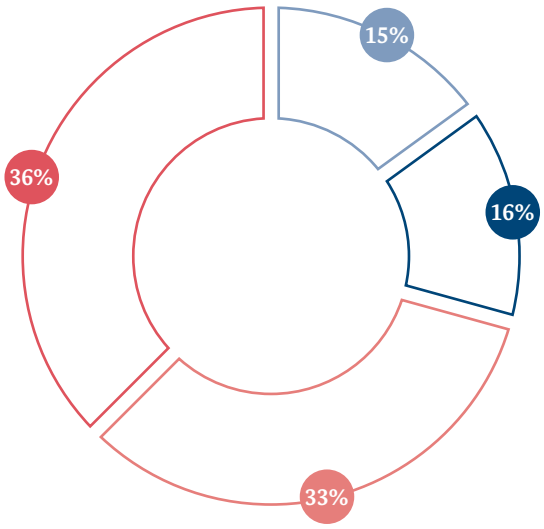


Abbildung 10:
Spam im Berichtszeitraum nach Art des Spam
Quelle: E-Mail-Verkehrsstatistik

Sonstiges
Werbung
Betrug
Erpressung

Die bereits im vergangenen Berichtszeitraum beobachteten Spam-Wellen aus dem Bereich der versuchten Cyber-Erpressung haben sich im aktuellen Berichtszeitraum fortgesetzt. Eine ausgeprägte Erpressungskampagne trieb die Spam-Ratio für die Wirtschaft in Deutschland im Februar 2022 auf 4,5 und damit auf den höchsten Monatsdurchschnitt seit Beginn der Statistik. Die Spam-Ratio gibt an, wie viele Spam-Mails je legitimer E-Mail in einem Berichtszeitraum durchschnittlich eingingen. Ein E-Mail-Postfach, das beispielsweise 100 legitime, erwünschte E-Mails im Februar 2022 erhielt, wurde statistisch gesehen zusätzlich durchschnittlich mit 450 Spam-Mails adressiert.

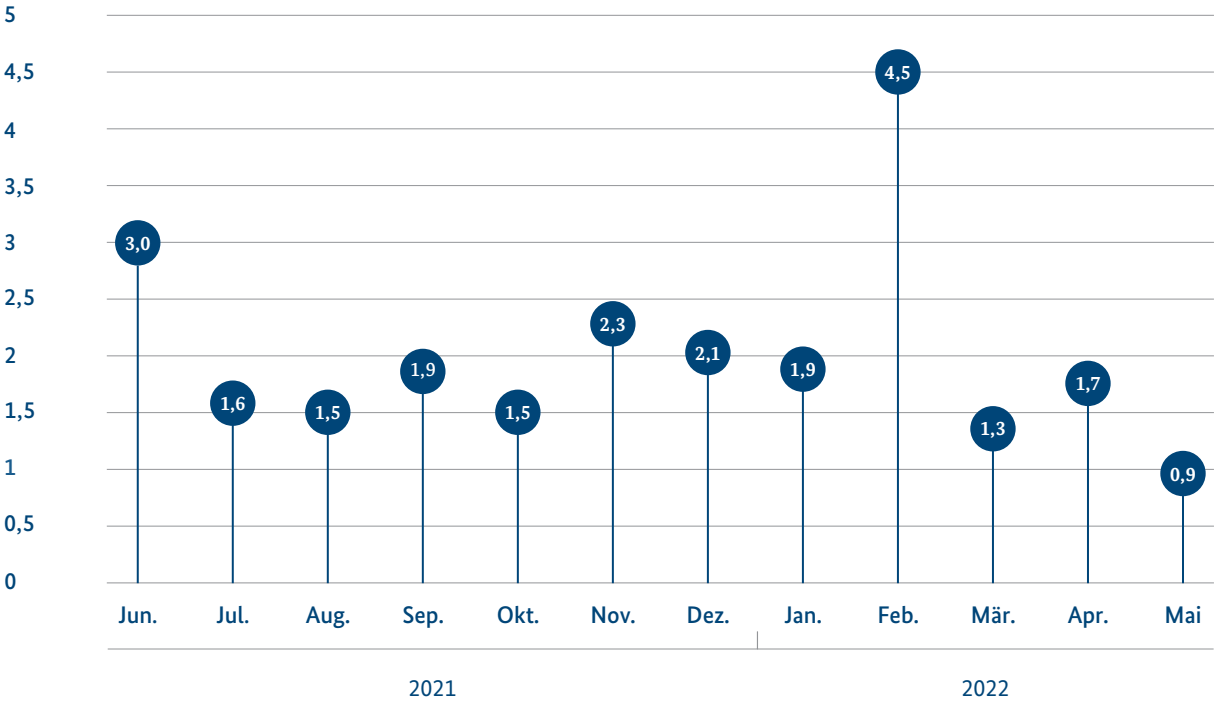
Ursächlich für den spürbaren Anstieg an Spam-Mails im Februar 2022 war eine ausgeprägte, über mehrere Tage andauernde Sextortion-Kampagne. Die Angreifer gaben vor, über kompromittierendes Videomaterial zu verfügen, das das Opfer beim Besuch pornografischer Webseiten zeigen soll. Sie drohten, das vermeintlich vorhandene Material an die Öffentlichkeit zu geben (vgl. Abbildung 12), würde nicht innerhalb von 48 Stunden ein niedriger vierstelliger US-Dollar-Betrag in *Bitcoin* gezahlt. Die Sextortion-Welle machte sich nicht nur in der Wirtschaft in Deutschland und in der Bundesverwaltung bemerkbar, sondern adressierte auch Verbraucherinnen und Verbraucher. Moderne Spam-Filter mit hochwertigen Detektoren auf dem aktuellen Stand der Technik konnten die meisten der Sextortion-Mails abfangen.

Sextortion-Mails machten im Berichtszeitraum mit 76 Prozent den größten Teil der Erpresser-Mails aus. Weitere 12 Prozent der Erpresser-Mails entfielen auf die Kategorie Gesundheit. In den übrigen E-Mails benutzten Angreifer verschiedene Themen, um Schweigegelder zu erpressen. Gemeinsam ist allen Erpresser-Mails, dass die Angreifer vorgeben, über intime Geheimnisse zum Beispiel zum Gesundheitszustand oder sexuellen Vorlieben des Opfers zu verfügen. Zusätzlichen Erpressungsdruck bauen sie auf, indem sie suggerieren, das Opfer Tag und Nacht bei allen Aktivitäten auf all seinen Geräten überwachen zu können.

Im Bereich der Betrugs-Mails nehmen Phishing-Mails mit rund 90 Prozent den größten Anteil ein. Phishing-Mails zielen darauf ab, das Opfer mittels Social-Engineering-Methoden zur Preisgabe von Identitäts- oder Authentifizierungsdaten zu bewegen. Dabei sind Phishing- und Spear-Phishing-Methoden zu unterscheiden. Während Angreifer mit Spear-Phishing aufwendig und gezielt gegen einzelne Personen wie zum Beispiel bedeutende Persönlichkeiten in Staat oder Wirtschaft vorgehen, um deren Identitätsdaten zu erbeuten (vgl. zum Beispiel Vorfall *Spear-Phishing durch APT-Gruppe Ghost-Writer*, Seite 40), richten sich massenhaft und ungezielt

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

Abbildung 11:
Spam-Ratio in der Wirtschaft in Deutschland
Quelle: E-Mail-Verkehrsstatistik



verteilte Phishing-Mails gegen die breite Bevölkerung. Besonders häufig setzten Angreifer im aktuellen Berichtszeitraum auf Finance Phishing. Diese E-Mails sind mittlerweile in der Regel in sehr gutem Deutsch verfasst und so gestaltet, dass sie zum Corporate Design großer Banken in Deutschland passen. Häufig werden Designs verwendet, die denen von Sparkassen, Volksbanken oder der Postbank nachempfunden sind. Die Angreifer suggerieren den Opfern so, eine vermeintlich notwendige Verifizierung durchführen zu müssen, bei der sie ihnen die Zugangsdaten für ihr Online-Banking entlocken. Da Banken in Deutschland ihre Kundinnen und Kunden grundsätzlich nicht per E-Mail zur Eingabe von Zugangsdaten auffordern, sollten Anwenderinnen und Anwender solche E-Mails stets als Phishing-Versuche werten, keinesfalls Zugangsdaten eingeben oder auf enthaltene Links klicken und ihren E-Mail-Provider oder ihr Geldinstitut informieren, damit diese Gegenmaßnahmen ergreifen können.

Darüber hinaus beobachtete das BSI auch im aktuellen Berichtszeitraum wieder sogenannten Vorschussbetrug per E-Mail. Mit solchen Spam-Mails werden die Opfer dazu verleitet, Geld zu überweisen. Die Angreifer geben vor, eine reiche Person zu sein, die ihr Vermögen im Ausland in Sicherheit bringen müsse und dafür Hilfe benötige. Das Opfer soll einen bestimmten Betrag überweisen, um beispielsweise ein Konto eröffnen zu können. Dafür wird ihm eine hohe Entlohnung versprochen, sobald sich das vermeintliche Vermögen der reichen Person sicher im Ausland befindet. Solche *Scam-Mails* machten im aktuellen Berichtszeitraum rund zehn Prozent der betrügerischen Spam-Mails aus.

Im Zusammenhang mit der Flutkatastrophe in Nordrhein-Westfalen und Rheinland-Pfalz sowie mit dem russischen Angriffskrieg gegen die Ukraine war wieder Charity-Scam zu beobachten. Damit verbreiten Angreifer betrügerische „Spendenaufrufe“ über Spam-Mails und Social-Media-Kanäle und versuchen, die Hilfs- und Spendenbereitschaft auszunutzen (vgl. Kapitel *Cyber-Sicherheitslage im Kontext des russischen Angriffskrieges gegen die Ukraine*, Seite 45).

Beispiel einer Sextortion-Mail

Abbildung 12:
Beispiel einer Sextortion-Mail
Quelle: BSI

From: [redacted]
To: [redacted]
Subject: Vergessen Sie nicht, innerhalb von 2 Tagen die Steuer zu zahlen!
Date: 18 Feb 2022 03:03:06 +1000

Hallo, wie geht es Ihnen?
Ich weiß, es ist unangenehm, das Gespräch mit schlechten Nachrichten zu beginnen, aber ich habe keine andere Wahl.
Vor ein paar Monaten habe ich mir Zugang zu Ihren Geräten verschafft, die Sie zum Surfen im Internet benutzen. Danach konnte ich alle Ihre Internetaktivitäten aufspüren.

Hier ist die Vorgeschichte, wie es dazu kommen konnte:
Zunächst habe ich mir von Hackern den Zugang zu mehreren E-Mail-Konten erkauft (heutzutage ist das online sehr einfach zu bewerkstelligen). So konnte ich mich problemlos in Ihr E-Mail-Konto einloggen ([redacted]).
Eine Woche später habe ich in den Betriebssystemen aller Ihrer Geräte, die Sie zum Öffnen von E-Mails verwenden, einen Trojaner installiert. Ehrlich gesagt, war das ziemlich einfach (da Sie die Links aus Ihren E-Mails im Posteingang geöffnet haben). Das Geniale ist ganz einfach.
Meine Software ermöglicht mir den Zugriff auf alle Steuerungen in Ihren Geräten, wie Mikrofon, Tastatur und Videokamera. Ich kann ganz einfach alle Ihre privaten Daten auf meine Server herunterladen, einschließlich des Verlaufs Ihres Internet-Browsings und Ihrer Fotos. Ich kann mühelos auf alle Ihre Messenger, Konten bei sozialen Netzwerken, E-Mails, Kontaktlisten und Chatverläufe zugreifen. Mein Virus aktualisiert ständig seine Signaturen (weil er treiberbasiert ist) und bleibt daher von Ihrem Antivirusprogramm unbemerkt. Sie können sich also schon denken, warum ich die ganze Zeit unentdeckt geblieben bin.

Als ich Informationen über Sie sammelte, konnte ich nicht umhin festzustellen, dass Sie auch ein echter Fan von Webseiten mit Inhalten für Erwachsene sind. Sie lieben es Pornoseiten zu besuchen und perverse Videos anzuschauen, während Sie sich selbst befriedigen. Ich konnte ein paar schmutzige Aufnahmen mit Ihnen als Hauptdarsteller machen und mehrere Videos montieren, die zeigen, wie Sie beim lustvollen Masturbieren zum Orgasmus kommen. Wenn Sie immer noch unsicher sind, ob meine Absichten ernst gemeint sind, kann ich Ihre Videos mit wenigen Mausklicks an alle Ihre Verwandten, Freunde und Kollegen weiterleiten. Ich kann diese Videos auch für die Öffentlichkeit zugänglich machen. Ich glaube ehrlich gesagt nicht, dass Sie das wirklich wollen, denn in Anbetracht der Besonderheit der Videos, die Sie sich gerne ansehen (Sie wissen natürlich, was ich meine), können all diese perversen Inhalte zu einem Grund für ernsthafte Probleme für Sie werden.

Wir können diese Situation jedoch auf die folgende Weise lösen: Alles, was Sie tun müssen, ist eine einmalige Überweisung von 1850 $ auf mein Konto (oder den entsprechenden Betrag in Bitcoin
je nach Wechselkurs zum Zeitpunkt der Überweisung) und sobald die Transaktion abgeschlossen ist, werde ich alle schmutzigen Inhalte, die Sie entblößen, sofort entfernen. Danach können Sie sogar vergessen, dass Sie mir begegnet sind.
Außerdem schwöre ich Ihnen, dass alle schädlichen Programme auch von allen Ihren Geräten entfernt werden. Zweifeln Sie nicht daran, dass ich meinen Teil erfüllen werde. Das ist wirklich ein großartiges Angebot zu einem vernünftigen Preis, bedenkt man, dass ich ziemlich viel Energie darauf verwendet habe, Ihr Profil und Ihren Datenverkehr über einen längeren Zeitraum zu überprüfen.
Wenn Sie keine Ahnung vom Bitcoin-Kaufprozess haben, können Sie ihn ganz einfach online durchführen, indem Sie sich alle notwendigen Informationen beschaffen.
Hier finden Sie meine Bitcoin-Wallet: [redacted]

Sie sollten die oben genannte Überweisung innerhalb von 48 Stunden
(2 Tagen) nach dem Öffnen dieser E-Mail abschließen. Die folgende Liste enthält Aktionen, die Sie vermeiden sollten:
....

Lassen Sie uns dieses Geschäft auf faire Weise abschließen!
Ach ja, noch etwas... in Zukunft sollten Sie sich besser nicht mehr in ähnliche Situationen verwickeln lassen!
Ein letzter Rat von mir: Ändern Sie regelmäßig alle Ihre Passwörter für alle Konten.

Beispiel einer Finance Phishing Mail

Abbildung 13:
Beispiel einer Finance Phishing Mail
Quelle: BSI

Von: Sparkasse Mitteilung <SparkasseMitteilung@[redacted]>
Gesendet: 5. März 2022 09:31
An: [redacted]
Betreff: Mittteilung Ihrer Sparkasse

[redacted]

Verifizierung benötigt

Sehr geehrte*r Kunde*in,

Durch die neuen Änderungen des Bundes sind wir die Kreditinstitute dazu verpflichtet in regelmäßigen Abständen Informationen unserer Sparkassen-Kunden zu überprüfen.

Wir als Ihr Kreditinstitut haben die neuen Gesetze umgesetzt.

Mit dem Verfahren können unsere Kunden Ihre Informationen für die Legitimation ganz einfach durchführen.

Anschließend werden die von Ihnen eingetragenen Informationen an einen unserer Kundenberater übermittelt und vervollständigt.

Die Überprüfung muss bis zum 31.03.2022 abgeschlossen werden. Wir bitten Sie daher diese Legitimation schnellstmöglich zu vervollständigen. Andernfalls werden wichtige Funktionen Ihres Giro-Kontos für eine bestimmte Zeit eingeschränkt.

Zur Bestätigung

Wir bedanken uns für Ihre Aufmerksamkeit.

Viele Grüße, Ihre Sparkasse

1.2.5 — Social Bots

Bei Social Bots handelt es sich um Computerprogramme, mit deren Hilfe die Kommunikation in sozialen Netzwerken simuliert und automatisiert werden kann. Diese Automatisierung wird als Mittel zur Verbreitung von Inhalten benutzt. Dadurch können Social Bots als schädliches Werkzeug eingesetzt werden, um Falschmeldungen und Propaganda, sowie Schadinhalte (zum Beispiel Phishing-Postings in sozialen Netzwerken) systematisch zu verbreiten.

Das BSI hat 2021 in Zusammenarbeit mit der Westfälischen Wilhelms-Universität Münster eine Analyse zum Thema „Entdeckung, Verbreitung und technologische Entwicklung von Social Bots“ durchgeführt. Ziel der Analyse war neben der Untersuchung aktueller Technologien zur Erkennung von Social Bots auch eine aktuelle Lagebildanalyse vor dem Hintergrund der Bundestagswahl 2021. Die Analyse baute auf einer Studie aus dem Jahr 2017 auf und erweiterte deren Erkenntnisse. Der Fokus der Untersuchung lag unter anderem auf der Verbreitung von *maliziösen* Inhalten (zum Beispiel Phishing-Links) in sozialen Netzwerken. Die Analyse der beiden Untersuchungen hat gezeigt, dass Social Bots zu gebräuchlichen Werkzeugen in sozialen Netzwerken geworden sind. Ein vollständig automatisierter und sicherer Nachweis, dass es sich bei einem konkreten Account um einen Bot handelt, ist jedoch nur in wenigen Fällen möglich. Dies liegt daran, dass die technische Entwicklung von automatisierten Erkennungsmechanismen für Social Bots nach wie vor prototypisch und zugleich wenig zuverlässig ist.

Am vielversprechendsten sind deshalb Verfahren, die aus der vorgelagerten automatischen Erkennung von auffälligem Account-Verhalten und der nachgelagerten Untersuchung von verdächtigen Accounts durch menschliche Analystinnen und Analysten bestehen. Daher wurde im Rahmen der 2021 erstellten Lagebildanalyse diese neue Methodik zur Erkennung mutmaßlicher Automatisierung vor dem Hintergrund der Bundestagswahl 2021 angewendet. Dafür wurde das soziale Netzwerk Twitter ausgewählt, da dieses eine geeignete Schnittstelle für die Datenanalyse bereitstellt. Analysiert wurde der gesamte Twitter-Stream, eingeschränkt auf deutschsprachige Inhalte zur Bundestagswahl.

Eine erkennbare Verbreitung von Schadsoftware oder infizierten Links wurde in dem untersuchten Twitter-Stream während des Wahlkampfs jedoch nicht gefunden.

Daneben ließ sich allgemein feststellen, dass verschiedene Interessengruppen im Wahlkampf zwar Social Bots eingesetzt haben. Diese konnten jedoch aufgrund geringer Reichweite keinen nachweisbaren Einfluss auf die politische Meinungsbildung erzielen. Eine Zuordnung zu Parteien und/oder Organisationen erfolgte nicht, da das BSI kein Mandat für die inhaltliche Auswertung von Social-Media-Accounts hat. Während 2017 hauptsächlich Post-Multiplier zur automatisierten Verbreitung von Inhalten, d. h. das mehrfache Posten von Tweets, genutzt worden sind, waren es 2021 Reply-Multiplier. Sie zielen darauf ab, möglichst subtil Inhalte in Diskussionen zu verbreiten. Post-Multiplier werden von menschlichen Nutzerinnen und Nutzern leicht identifiziert und auch von Twitter schnell erkannt und beseitigt. Reply-Multiplier dagegen reagieren mit ähnlichen oder gleichen Inhalten auf einzelne Posts von Nutzerinnen und Nutzern. Letztere nehmen das als normale Kommunikation wahr. Auch für Twitter ist es schwerer, hier *Spam* bzw. Social Bots zu erkennen.

Inzwischen ist es technisch möglich, mit Hilfe von Sprachmodellen automatisiert realistische Tweets zu erzeugen. Besonders, wenn es sich um so kurze Texte wie auf Twitter handelt, lassen sich diese Inhalte kaum von anderen natürlich-sprachlichen, von Menschen geschriebenen Texten unterscheiden. Damit lässt sich eine bisherige Schwäche von Social Bots, nämlich Texte zu erzeugen, die von Menschen verfassten Texten ähnlich sind, zukünftig umgehen (vgl. Kapitel *Künstliche Intelligenz*, Seite 96). Die bisherigen Methoden zur Erkennung von Social Bots sind nicht in der Lage, diese zuverlässig zu erkennen.

1.3 — Schwachstellen

Die Zahl bekanntgewordener Schwachstellen ist zuletzt gestiegen. Cyber-Kriminelle können die Lücken in Soft- und Hardware-Produkten nutzen, um weitreichenden Schaden anzurichten oder wertvolle Informationen abzugreifen. Dem Aufspüren, Melden und schnellstmöglichen Schließen der entsprechenden Schwachstellen kommt daher eine besonders hohe Bedeutung zu.

Coordinated-Vulnerability-Disclosure-Fälle von 2017 bis 2021
Anzahl

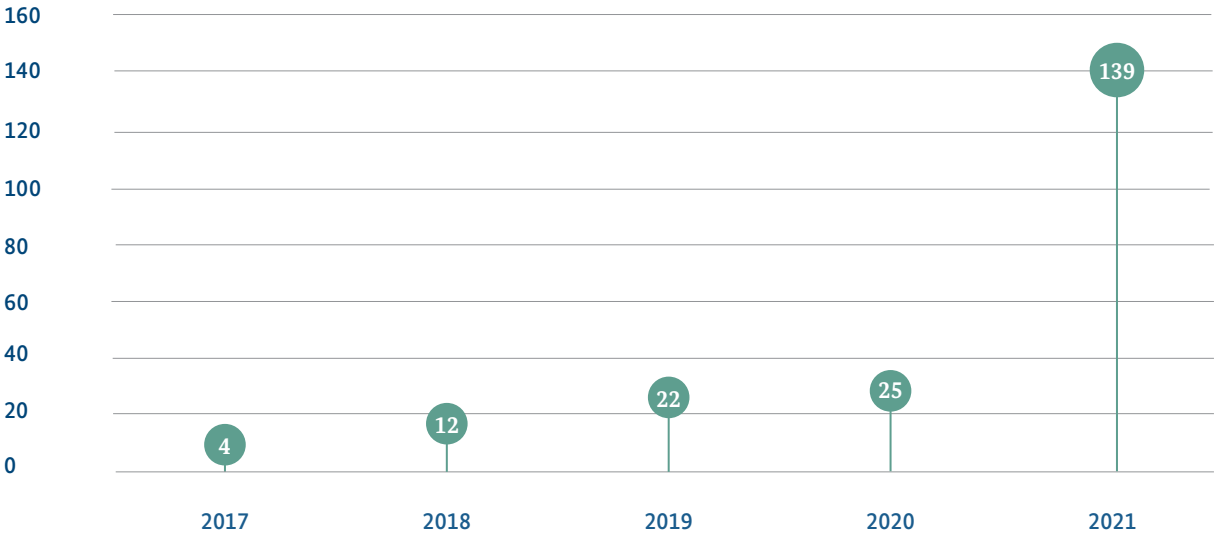


Abbildung 14: Coordinated-Vulnerability-Disclosure-Fälle von 2017-2021
Quelle: BSI

1.3.1 — Schwachstellen in Software-Produkten

Das Prinzip des *Coordinated Vulnerability Disclosure (CVD)* umfasst die koordinierte Veröffentlichung von Informationen zu einer Schwachstelle sowie die Bereitstellung von Patches bzw. Mitigationsmaßnahmen für betroffene Software-Produkte in einer transparenten, systematischen zeitlichen Abfolge. Das CERT-Bund im BSI unterstützt seit mehreren Jahren Sicherheitsforschende bei der Meldung von Schwachstellen an Hersteller und bei der Koordination des Veröffentlichungsprozesses. Damit sich Schwachstellenmeldungen bewerten und besser nachvollziehen lassen, hat das BSI im Berichtszeitraum ein Meldeformular für Schwachstellen online gestellt[6]. Das Formular ermöglicht Sicherheitsforschenden, in Software gefundene Schwachstellen strukturiert an das BSI zu melden. Die darin anzugebenden Informationen dienen der Nachvollziehbarkeit von Schwachstellenmeldung, der Ermittlung der Kritikalität der gefundenen Schwachstelle sowie der Abschätzung möglicher Auswirkungen auf die IT-Sicherheit bei den Zielgruppen des BSI. Im Rahmen eines CVD-Prozesses unterstützt das BSI Sicherheitsforschende anschließend bei der Kommunikation mit dem Hersteller des schwachstellenbehafteten Produkts und der koordinierten Offenlegung der Schwachstelle sowie beispielsweise der Erstellung von Sicherheitshinweisen *(Security Advisories)*. Dabei handelt es sich um Empfehlungen der Hersteller an IT-Sicherheitsverantwortliche in Unternehmen und anderen Organisationen zum Umgang mit aufgefundenen Schwachstellen.

Weiterhin haben viele Software-Hersteller noch nicht die Voraussetzungen geschaffen, einen CVD-Prozess eigenständig durchzuführen. Im ersten Schritt sollten sie dafür generell einen IT-Sicherheitskontakt anbieten, an den sich Sicherheitsforschende wenden können. Das BSI unterstützt Forschende und Hersteller bei der Durchführung des CVD-Prozesses und nimmt als neutrale koordinierende Stelle teil.

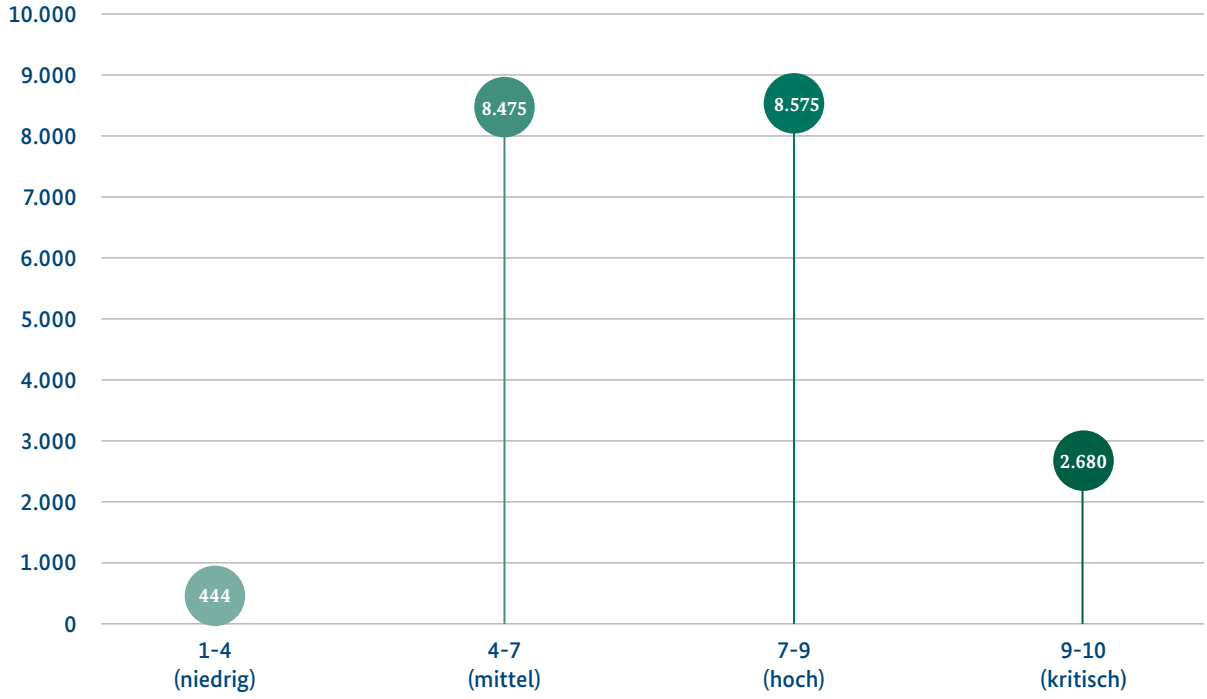
Das BSI hat 2021 insgesamt 139 CVD-Meldungen erhalten (vgl. Abbildung 14). Der Anstieg gegenüber dem Vorjahr dürfte überwiegend auf die Einführung des oben genannten Formulars für Meldungen von Schwachstellen zurückzuführen sein. Im Vorfeld wurde die Community der IT-Sicherheitsforschenden konsultiert. Das Meldeformular war dort daher nicht nur bei dessen Freischaltung auf der BSI-Website bereits bekannt, sondern erfüllt auch die Anforderungen, die Sicherheitsforschende an so eine Meldemöglichkeit stellen.

Bekannt gewordene Schwachstellen 2021 nach dem CVSS-Score[1] für Kritikalität

Anzahl

Abbildung 15:
Bekannt gewordene Schwachstellen 2021 nach dem CVSS-Score für Kritikalität
Quelle: Schwachstellen-Statistik

[1] Risikobewertung nach CVSS-Version 3.1



Bei Schwachstellen, die dem BSI im aktuellen Berichtszeitraum gemeldet wurden, handelte es sich wie schon im vorherigen Berichtszeitraum häufig um solche in der Software von Corona-Testzentren. Ein Grund dafür dürfte sein, dass sich die sicherheitsforschende Gemeinschaft der Sensibilität der dort gespeicherten Daten bewusst ist und daher die jeweiligen Datenbanken und Anwendungen entsprechend in den Fokus genommen hat (vgl. Abschnitt *Digitale Pandemiebekämpfung*, Seite 62, sowie zur Problematik sensibler Daten in IT-Systemen vgl. Abschnitt *Erpressung mit erbeuteten Identitätsdaten*, Seite 17).

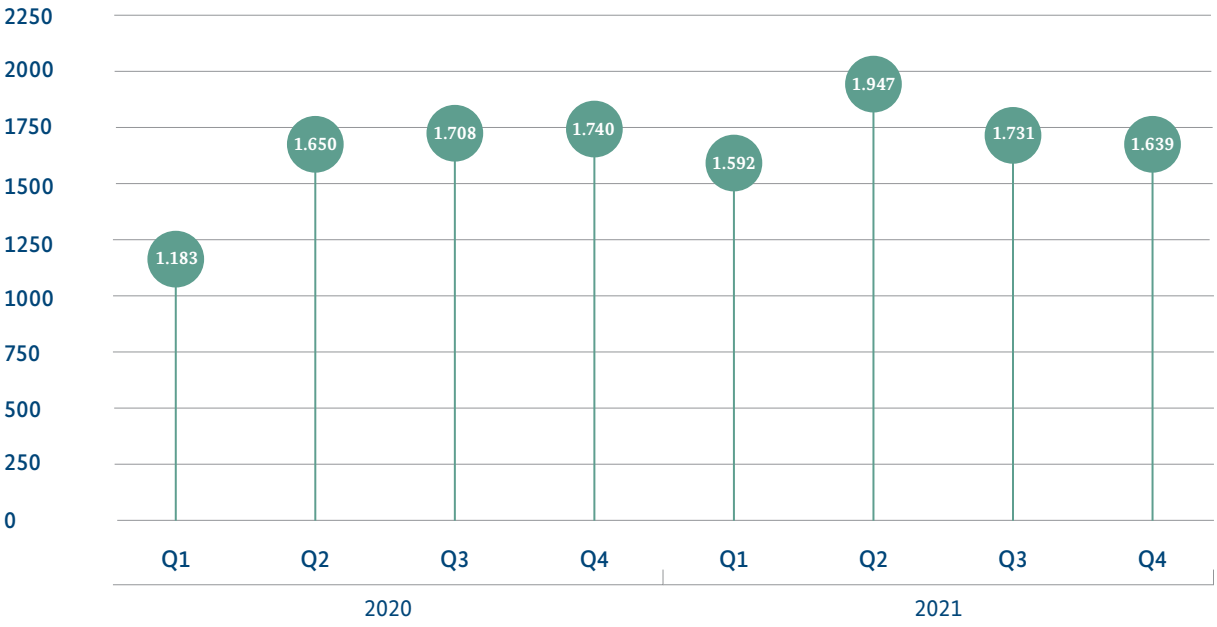
Für die Beurteilung der IT-Sicherheitslage prüft das BSI auch öffentliche Quellen täglich auf neue Informationen zu Schwachstellen. Demnach war die Lage im Berichtszeitraum überdurchschnittlich bedrohlich. Zum einen traten mit Sicherheitslücken in Microsoft Exchange und Log4j wieder besonders kritische Schwachstellen in weitverbreiteten Produkten auf (vgl. *Vorfall Log4j: Schwachstelle in quelloffener Bibliothek*, Seite 37). Zum anderen hat auch die Anzahl der bekannt gewordenen Schwachstellen über alle Kritikalitätsstufen hinweg zugenommen. Im Jahr 2021 verzeichnete das CVSS-Scoring-System, ein Industriestandard, mit dem die Kritikalität von Schwachstellen international vergleichbar bewertet wird, 20.174 Schwachstellen in Software-Produkten – rund zehn Prozent mehr als im Jahr zuvor.

Die Kritikalität der bekannt gewordenen Schwachstellen war gemischt. Gut zwei Prozent (444) wiesen niedrige und 42 Prozent (8.475) mittlere Scoring-Werte auf der zehnstufigen Skala auf (vgl. Abbildung 15). Insgesamt 11.255 – und damit mehr als die Hälfte – wiesen hohe (7-9) oder kritische (9-10) CVSS-Scores auf, wobei 2.680 von ihnen kritische Scoring-Werte erhielten. Der Anteil kritischer Schwachstellen lag 2021 demnach bei rund 13 Prozent.

Diese und weitere Erkenntnisse fließen in den Warn- und Informationsdienst (WID) des BSI ein, der die 150 gängigsten Software-Produkte auf dem deutschen Markt beobachtet und die darin bekannt gewordenen

WID-Meldungen 2020 bis 2021
Anzahl

Abbildung 16:
WID-Meldungen 2020 bis 2021
Quelle: BSI



Schwachstellen bewertet. Der WID ist damit ein wesentliches Instrument, um Nutzerinnen und Nutzer zu informieren. Hinweise auf Schwachstellen werden gesammelt, aufbereitet und auf www.cert-bund.de veröffentlicht. Alle Interessierten haben die Möglichkeit, sich beim WID zu registrieren und Informationen zu den für sie relevanten IT-Produkten als E-Mail zu abonnieren. Sachverhalte, denen eine besondere Relevanz für Privatpersonen unterstellt wird – zum Beispiel Schwachstellen, die gängige Betriebssysteme oder Office-Anwendungen betreffen – werden zudem als Technische Warnungen/Bürger-CERT-Warnungen veröffentlicht.

Weiterführende Informationen finden Sie hier:[b]

Der Mehrwert des WID für die Nutzerinnen und Nutzer besteht somit einerseits darin, dass aktuelle Inhalte aus verschiedenen Quellen gesammelt, bewertet und an einer Stelle zentral angeboten werden. Andererseits unterstützt die Zuordnung der Sachverhalte in unterschiedliche Risikogruppen IT-Sicherheitsverantwortliche bei der Priorisierung von auszurollenden Sicherheitsupdates.

Im Jahr 2021 hat der WID insgesamt 6.910 Meldungen über Schwachstellen in den 150 gängigsten Produkten veröffentlicht – rund zehn Prozent mehr als im Vorjahr.

Hinzu kamen 2.412 *Advisories* für IT-Sicherheitsverantwortliche in Bundesbehörden (plus 13 Prozent gegenüber dem Vorjahr) und 265 Technische Warnungen (plus 17 Prozent gegenüber dem Vorjahr).

Liegen Informationen zu Schwachstellen mit herausragendem Bedrohungspotenzial vor, veröffentlicht das BSI außerdem Cyber-Sicherheitsinformationen, die sich in drei Kategorien aufteilen:

1.) **Cyber-Sicherheitswarnung (Informationen zu Schwachstellen mit technischer Tiefe)**

2.) **Management-Informationen (Hinweise zu aktuellen Bedrohungen für die Entscheidungsebene)**

3.) **Vorfallswarnungen (bei aufgetretenen Vorfällen beobachtete Angriffsindikatoren und Schutzmaßnahmen).**

Dieses Mittel nutzte das Bundesamt im Jahr 2021 insgesamt 68 Mal (darunter 49 Cyber-Sicherheitswar-

nungen, neun Management-Informationen und zehn Vorfallswarnungen). Besonders im Fokus stand dabei die Java-Schwachstelle Log4Shell (vgl. Vorfall *Log4j: Schwachstelle in quelloffener Bibliothek*, Seite 37).

Das Auftreten von Log4Shell illustriert eine Bedrohung, auf die bereits in der Vergangenheit hingewiesen wurde: die zunehmende Modularisierung der Software-Produktion, d. h. die Verwendung von Drittanbieter-Software in eigenen Anwendungen (vgl. *Die Lage der IT-Sicherheit in Deutschland 2021*, Seite 27 f). Oft werden dabei bestimmte Funktionalitäten eines Programms bzw. einer Software mittels externer Komponenten realisiert, die von Drittanbietern bezogen werden, deren Sicherheitsrisiko für die Software-Entwicklung aber schwer zu überblicken sind. Einige Hersteller geben ihrer Software-Entwicklung aus Wirtschaftlichkeitsgründen sogar vor, dass vor einer Eigenentwicklung geprüft werden muss, ob sich die benötigten Funktionen nicht auch extern beziehen lassen. Oft werden solche Komponenten dann verwendet, ohne deren vollständigen Funktionsumfang und Implementierung genau zu kennen. Hinzu kommen neue Risiken, die durch die Art der Einbindung in Anwendungen entstehen, wenn die Nutzungsszenarien der Komponente nicht zu denen der Anwendung passen. In vielen Fällen enthalten Komponenten außerdem Funktionsteile, die für den angedachten Zweck in einer Anwendung gar nicht erforderlich sind. Dadurch erhöht sich nicht nur die Angriffsfläche der Anwendung, sondern es entstehen auch neue Abhängigkeiten. Neben der Verfügbarkeit können Schwachstellen und Angriffe auch die Integrität und Vertraulichkeit von Anwendungen betreffen.

Erschwerend kommt hinzu, dass sich die Sicherheit einer Software-Komponente bzw. deren Einbindung durch Entwickler anhand der Dokumentation nur sehr schwer einschätzen lässt. Oft sind unabhängige Sicherheitsanalysen gefordert, um die Sicherheit solcher Komponenten zu untersuchen. Doch diese können sich nur auf allgemeine Sicherheitsrisiken beziehen, die unter Umständen auch nur für ein bestimmtes Nutzungsszenario gelten. Insbesondere können besondere Risiken, die im Design (und auch der Funktion) der Komponente oder deren spezifischer Nutzung liegen, von Externen nur schwer bewertet werden. Drittanbieter-Komponenten versuchen häufig, ein großes Spektrum an Nutzungsszenarien in ihrer Standard-Konfiguration abzudecken. Komponenten, die mit einem breiten, vorkonfiguriert aktivem Funktionsumfang ausgeliefert werden, stehen daher in einem Zielkonflikt zum Prinzip *Security by Default*[7].

1.3.2 — Schwachstellen in Hardware-Produkten

Schwachstellen in Hardware-Produkten haben gemeinsam, dass diese in der Regel sehr tief in der jeweiligen Architektur oder dem Herstellungsprozess begründet sind. Angriffe setzen etwa bei der Physik von Transistoren in hochintegrierten Schaltungen, der Mikroarchitektur eines Prozessors oder auch den Schritten „Produktion“ und „Lieferkette“ eines IT-Produkts an. Der Aufwand und die Kosten für die Ausnutzung von Hardware-Schwachstellen sind dabei zunächst höher als bei Software-Schwachstellen. Jedoch ist der potenzielle Nutzen aus Sicht eines Angreifers ebenfalls höher, da sich Hardware-Schwachstellen oft nicht durch einfache Software-Patches beheben lassen.

Wie in den Jahren zuvor dominierten im aktuellen Berichtszeitraum bei Schwachstellen in Hardware-Produkten zwei Angriffsklassen. Das sind zum einen Angriffe, die Besonderheiten der transienten Ausführung von Befehlen bei Prozessoren ausnutzen. Seit 2017 die Angriffe Meltdown und Spectre veröffentlicht wurden, existieren nun mehr als 25 Schwachstellen und Variationen dieser Angriffe. Im Jahr 2021 wurden etwa die neuen Schwachstellen „I see dead Micro-Ops“, Blindside und CIPHERLEAKS entdeckt. Transiente Ausführungen bei modernen Prozessoren sind unabdingbar für eine hohe Performance. Eine solche Mikroarchitektur stellt jedoch gleichzeitig eine grundsätzliche Herausforderung für ein schwachstellenfreies Design dar. Daher ist auch weiter mit Schwachstellen aus dieser Angriffsklasse zu rechnen, solange nicht grundlegende Re-Designs der Architektur vorgenommen werden.

Zum anderen dominieren weiterhin Angriffe, die Seiteneffekte bei der Operation von Arbeitsspeicher ausnutzen. Dabei können durch gezielte hochfrequente Zugriffe auf Speicherzellen Datenwerte in benachbarten Speicherzellen verändert werden. Obwohl dieses Phänomen seit 2014 bekannt ist, existieren bis jetzt keine breit verfügbaren Gegenmaßnahmen. Auch fehlerkorrigierender Speicher (ECC Speicher) schafft hier keine Abhilfe. Im Jahr 2021 konnte mit der Angriffsmethode BlackSmith gezeigt werden, dass auch moderner DDR4-Speicher anfällig für solche Seiteneffekte ist.

Aufgrund zahlreicher softwarebasierter Angriffe und verstärkter Wahrnehmung der Bedrohung durch Cyber-Angriffe werden vermehrt hardwarebasierte Lösungen zur Absicherung von IT-Systemen verwendet, zum Bei-

Versorgungsketten-Angriff auf verbreiteten Virtual System Administrator (VSA)

Sachverhalt

Am 2. Juli 2021 wurden Versorgungsketten-Angriffe (Supply-Chain-Angriffe) über die Software Virtual System Administrator (VSA) eines amerikanischen Software-Herstellers bekannt, die auch in Deutschland vielfach verwendet wird. VSA wird von Managed Service Providern (MSP) bzw. IT-Systemhäusern eingesetzt, beispielsweise zur Fernwartung, zum Monitoring sowie zum Management von IT-Systemen ihrer Kundinnen und Kunden. Zum Kundenkreis der MSP gehören auch viele kleine und mittlere Unternehmen (KMU). Unabhängig von MSPs wird VSA auch durch den Software-Hersteller selbst als Software-as-a-Service betrieben. VSA nimmt eine für das IT-Netz einer Organisation empfindliche Rolle ein, weil sich über den Verwaltungsserver von VSA auf jeden verwalteten Client zugreifen und auch Software verteilen lässt. In dem Software-Supply-Chain-Angriff machten sich Angreifer mit der Ransomware REvil (auch bekannt als Sodinokibi) die Verwaltungsfunktionalität von VSA zu Nutze. Über die Zero-Day-Schwachstelle CVE-2021-30116 verteilten die Angreifer innerhalb weniger Tage massenhaft die Ransomware REvil auf mittels VSA verwalteten Clients. Betroffen waren die von MSP eingesetzten VSA. Die über die Software-as-a-Service (SaaS)-Lösung des Software-Herstellers von VSA verwalteten Systeme blieben dagegen von dem Angriff verschont. Trotzdem wurde der SaaS vorsichtshalber abgeschaltet, um eine Ausbreitung des Angriffs zu verhindern, bis entsprechende Patches für die Zero-Day-Schwachstellen vorlagen. Daher stand VSA für einen Zeitraum von neun Tagen nicht zur Verfügung. Von dem Angriff waren möglicherweise 800 bis 1.500 Endkundinnen und Endkunden unmittelbar betroffen sowie wahrscheinlich weitere, denen der SaaS vorübergehend nicht zur Verfügung stand. Am 11. Juli 2021 stellte der Softwarehersteller von VSA Patches für die ausgenutzten Zero-Day-Schwachstellen zur Verfügung. Am 22. Juli 2021 erhielt der Softwarehersteller aus einer vertrauenswürdigen Drittquelle das Schlüsselmaterial für die Angriffskampagne. So konnten die Daten der von der Verschlüsselung betroffenen Endkundinnen und Endkunden wiederhergestellt werden.

Bewertung

Software-Supply-Chain-Angriffe zeichnen sich dadurch aus, dass der Schadcode schon im Verlauf des Herstellungsprozesses in eine legitime Software eingebaut wird. Supply-Chain-Angriffe auf Produkte wie VSA (wie hier über das IT-Netz) können außerordentlich „erfolgreich" sein. Derartige verwaltende Software verfügt oft über Ausnahmen von Zugriffsbeschränkungen oder erweiterte Zugriffsrechte auf Clients, weil sie auch zum Ausspielen von Software in der regulären Administration genutzt werden. Diese Fähigkeit der Software haben die Angreifer hier ausgenutzt. MSPs erbringen oft Software-Dienstleistungen für zahlreiche Unternehmen, und zwar sowohl für große als auch für kleine und mittlere Unternehmen. Derartige Angriffe gegen MSPs skalieren daher unter Umständen schnell und können kurzfristig in weitreichenden Ausfällen über das angegriffene Unternehmen hinaus resultieren. Selbst wenn Angreifern der Netzübergang aus dem angegriffenen MSP-Netz in die Kundennetze nicht gelingen sollte, haben die sich an den Angriff anschließenden Reparaturarbeiten oftmals Ausfälle oder Einschränkungen für die Endkundinnen und Endkunden der MSPs zur Folge. Die REvil-Ransomware-Infrastruktur inklusive Bezahlportal sowie Leak-Seite ist am Morgen des 13. Juli 2021 vollständig offline gegangen. Die Abschaltung geht nach Medienberichten auf Maßnahmen von US-Behörden sowie nicht näher benannten Partnerländern und IT-Sicherheitsdienstleistern zurück. Nach einer kurzen Rückkehr im September 2021 ist die Infrastruktur der RaaS REvil im Oktober 2021 wieder offline gegangen.

Reaktion

Das BSI hat am 4. Juli 2021 eine Cyber-Sicherheitswarnung herausgegeben, die anschließend regelmäßig aktualisiert wurde. Das BSI beobachtete die Betroffenheit deutscher Organisationen intensiv, beriet Betroffene zu IT-forensischen Maßnahmen und übermittelte Erste-Hilfe-Dokumente.

Log4j: Schwachstelle in quelloffener Bibliothek

Sachverhalt
Anfang Dezember 2021 wurde eine Schwachstelle in „Log4j" bekannt, die zunächst in der IT-Sicherheitscommunity und kurz darauf medial breit aufgegriffen wurde. Bei Log4j handelt es sich um eine freie und quelloffene Bibliothek, die in zahlreichen Anwendungen eingebunden ist, um Ereignisse zur späteren Analyse zu protokollieren. Diese Bibliothek wird in Java-Anwendungen sehr häufig verwendet. Durch die Schwachstelle war es möglich, beliebige Schadsoftware auf Systemen mit anfälligen Anwendungen auszuführen.

Bewertung
Die hohe Kritikalität der Schwachstelle ergab sich aus der vergleichsweise einfachen Ausnutzbarkeit in einigen exponierten Anwendungen. Gleichzeitig gibt es insbesondere bei kommerzieller Software häufig keine „Inhaltsangabe", sodass viele IT-Verantwortliche oft nicht wissen konnten, aus welchen Teilkomponenten die von ihnen benutzten Programme bestehen und ob sie von der Schwachstelle in Log4j betroffen waren. Da aus vergangenen Vorfällen bereits bekannt war, dass Angreifergruppen üblicherweise im großen Stil bekannte Schwachstellen ausnutzen und damit die Grundlage für weitere schädliche Aktivitäten wie beispielsweise die Installation von Verschlüsselungstrojanern oder das Stehlen vertraulicher Informationen legen, wurde die Schwachstelle als besonders kritisch bewertet.

Reaktion
Wegen der Gefahr einer möglicherweise breiten Ausnutzung der Schwachstelle für Cyber-Angriffe wurde im BSI eine sogenannte „Besondere Aufbauorganisation (BAO)" im Nationalen IT-Krisenreaktionszentrum aktiviert. Analysiert wurden die Auswirkungen der Schwachstelle auf die Cyber-Sicherheit in Deutschland sowie die Betroffenheit bei den Zielgruppen des BSI.

Weiterhin wurde eine Cyber-Sicherheitswarnung der Stufe Rot (höchste Warnstufe) veröffentlicht sowie ein Leitfaden zur Durchführung von reaktiven und präventiven Maßnahmen an die Öffentlichkeit sowie an die Zielgruppen des BSI verteilt. Durch aktive Medienarbeit des BSI wurden die IT-Verantwortlichen in Deutschland auf das Problem aufmerksam gemacht, um dadurch eine kurzfristige Problemlösung herbeizuführen.

spiel im IoT-Bereich, bei der *Zwei-Faktor-Authentisierung (2FA)* (vgl. Kapitel *Zwei-Faktor-Authentisierung*, S. 63) oder etwa bei Krypto-Wallets. Dabei werden oftmals keine zertifizierten, sondern handelsübliche Sicherheitscontroller verwendet. Solche Mikrocontroller weisen jedoch meist Hardware-Schwachstellen auf, die sich mit relativ moderatem Aufwand ausnutzen lassen. Anfang 2021 etwa wurden Schwachstellen in mehreren handelsüblichen Mikrocontrollern entdeckt, bei denen mittels gezielter Veränderung der Spannungsversorgung der Ausleseschutz umgangen werden konnte. So lassen sich auf dem Controller gespeicherte Geheimnisse, wie zum Beispiel geheime Schlüssel, auslesen.

Ein weiterer Trend ist die herstellerseitige Integration von Sicherheitsfunktionalität in dedizierten Bereichen des Prozessors, einer sogenannten sicheren Ausführungseinheit *(Trusted Execution Environment, TEE)*. Die Integration solcher Sicherheitsfunktionen in ein komplexes Gesamtdesign ist jedoch herausfordernd und fast alle am Markt verfügbaren Implementierungen wiesen im Laufe der Zeit Schwachstellen auf. Im Jahr 2021 kam die Schwachstelle SmashEX hinzu, die ein inkorrektes Verhalten bei vielen TEEs ausnutzt, wenn Programme in einen Fehlerzustand geraten. Dieses Verhalten erlaubt den Zugriff auf geschützte Datenbereiche.

Die Ausnutzung von Schwachstellen in Hardware-Produkten, insbesondere solche, die auf der transienten Ausführung bei Prozessoren basieren, gestaltet sich in der Praxis aufwendig. Da durch zahlreiche Software-Schwachstellen einfachere *Angriffsvektoren* existieren, finden Angriffe auf die genannten Hardware-Schwachstellen aktuell keine breite Anwendung. Zur Vermeidung von ausnutzbaren Hardware-Angriffen sollten kritische Daten und Operationen in dedizierten Sicherheitselementen oder logisch vollständig separierten Prozessorbereichen gespeichert und verarbeitet werden. Ein Vertrauen in die implementierte Sicherheitsfunktionalität schafft dabei nur eine unabhängige Sicherheitsüberprüfung, wie etwa nach dem ISO-Standard 15408: Common Criteria for IT Security Evaluation.

Weiterführende Informationen finden Sie hier:[c]

1.4 — 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, opportunistisch motivierten Angreifern in der Regel massenhaft verteilt werden (vgl. Kapitel *Ransomware*, Seite 13), 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 gegebenenfalls der Sabotage.

Im aktuellen Berichtszeitraum gab es eine Reihe von neuen Entwicklungen, die die APT-Bedrohungslage prägten.

Angriffe auf Perimeter:

Nach wie vor erweitern APT-Gruppen ihr Portfolio an Angriffsarten. Während in den zurückliegenden Jahren vor allem E-Mails mit Schadcode-Anhang oder mit *maliziösen* Links versendet wurden und auch weiterhin versendet werden, ist seit etwa zwei Jahren eine Zunahme an Angriffen auf *Perimeter-Systeme* zu beobachten. Dabei handelt es sich um Server, Firewalls, VPN-Gateways und Router, die direkt aus dem Internet erreichbar sind. Die Angreifer suchen in der Mehrzahl der Fälle nach bekannten Schwachstellen, für die noch kein Sicherheitsupdate eingespielt wurde.

Genutzt werden neben *Exploits* gegen Schwachstellen, zunehmend aber auch *Password-Spraying* und altbekannte, einfache Techniken wie Brute-Forcing. Dieser Trend ist bei unterschiedlichen Angreifer-Gruppen zu beobachten, beispielsweise APT28, APT25/Ke3chang und APT31.

Auf kompromittierten Servern installieren die Angreifer meistens *Webshells*. Dabei handelt es sich um wenige Zeilen Code, die es den Angreifern ermöglichen, sich von außen mit den Servern zu verbinden und Kommandos auszuführen.

Diese Entwicklung hat Auswirkungen auf die Arbeit von IT-Sicherheitsteams. *Perimeter-Systeme* werden in der Regel weniger gut überwacht, es gibt weniger Sicherheitsprodukte als für Endgeräte bzw. Büro-Rechner. *Webshells* können oftmals nicht im Netzwerkverkehr erkannt

werden, sondern müssen gezielt auf den Systemen (also hostbasiert) detektiert werden. Das in der Sicherheitscommunity verbreitete Teilen von Detektions-Indikatoren (Indicators of Compromise, IoCs) wird weniger effektiv, da ein vielgenutzter Typus von IoCs auf der Verwendung von Kontrollservern beruht. Die beschriebenen Angriffsmethoden arbeiten aber oftmals ohne Kontrollserver und der Zugriff erfolgt direkt über Anonymisierungsdienste auf die *Webshells*.

Auch auf absehbare Zeit wird der *Angriffsvektor* „Perimeter" relevant bleiben, und sollte bei allen IT-Sicherheits-Überlegungen (Netzwerk-Architekturen, Incident-Handling, Forensik, Logging, Beratung) mit entsprechender Priorität berücksichtigt werden.

Kompromittierte Heimrouter für Anonymisierung:

Eine Folge der Angriffe auf den Perimeter ist, dass Angreifer nun weniger Kontrollserver benötigen und stattdessen aktiv selbst Verbindungen aus Anonymisierungsnetzen heraus aufbauen können. Mit diesen Verbindungen führen sie *Exploits* aus und steuern nach einer erfolgreichen Kompromittierung via *Webshell* die Weiterverbreitung im IT-Netz des Opfers *(Lateral Movement)*. Dazu werden einerseits kommerzielle VPN-Dienste genutzt. Ein neuer Trend ist andererseits, Heimrouter zu kompromittieren, um über diese Geräte eigene Anonymisierungsnetze aufzubauen. Beispiele für Gruppen, die Router kompromittieren, sind APT31, BlackTech und APT32/OceanLotus. Das BSI geht davon aus, dass weitere Gruppen in Zukunft Router angreifen werden. Zum einen ist wegen des Trends zu Perimeter-Angriffen der entsprechende Bedarf für Infrastruktur zur Verschleierung von Internet-Verbindungen vorhanden, zum anderen sind Router massenhaft in der Fläche verfügbar, werden weltweit von Nutzerinnen und Nutzern eher wenig gewartet und sind nicht mit Sicherheits- und Monitoring-Produkten versehen. Auch für Sicherheitsfirmen ist es schwieriger, Telemetrie über Router zu erhalten und so Angriffe zu detektieren, was für Angreifer ein weiterer Anreiz sein dürfte.

***Cloud* als Einstiegspunkt:**

Ein weiterer Trend ist die Nutzung von Cloud-Diensten als *Angriffsvektor*. Bisher lag das Risiko für Cloud-Nutzung vor allem darin, dass die in der *Cloud* verarbeiteten oder gespeicherten Daten von Angreifern erbeutet werden könnten. Im aktuellen Berichtszeitraum zeigten Berichte über die Gruppe APT29/Nobelium jedoch, dass die *Cloud* auch als Einstiegspunkt in interne IT-Netze der Kundinnen und Kunden missbraucht werden kann. Die Angreifer versuchen beispielsweise zunächst, Passwörter für Cloud-Zugänge zu erraten oder zu stehlen. Sobald sie einen solchen Zugang erlangt haben, nutzen sie Vertrauensbeziehungen zwischen der *Cloud* und dem Kundennetz, um auf Rechner in internen Kundennetzen zugreifen zu können. Es ist davon auszugehen, dass andere Gruppen auf diesen Trend aufsetzen und ggf. neue Techniken entwickeln werden.

Sabotage im Nahen und Mittleren Osten:

Im Nahen und Mittleren Osten beginnen Akteure, Cyber-Sabotage in zwischenstaatlichen Konflikten einzusetzen. Eine der Konfliktseiten setzt dabei auf die Verschleierung solcher Angriffe mittels *Ransomware*. Andere Akteure mit gegensätzlichen Zielen führen unter der Flagge oder dem Deckmantel des Hacktivismus Sabotage-Angriffe aus, die auch Auswirkungen auf die Bevölkerung haben, indem zum Beispiel die Zuglogistik oder die Benzin-Versorgung gestört wird. Es ist nicht auszuschließen, dass sich diese Strategien in zwischenstaatlichen Konflikten, die noch unter der Schwelle einer militärischen Eskalation bleiben, auch außerhalb des Nahen und Mittleren Ostens verbreiten könnten. Cyber-Sabotage kam auch im Angriffskrieg Russlands gegen die Ukraine zum Einsatz (vgl. Kapitel *Cyber-Sicherheitslage im Kontext des russischen Angriffskrieges gegen die Ukraine*, Seite 45).

Hackers-for-Hire:

Besondere Medienaufmerksamkeit haben im Berichtszeitraum öffentlich agierende, sogenannte Hackers-for-Hire erhalten, die Produkte oder Dienstleistungen für offensive Cyber-Operationen verkaufen. Es existiert eine Reihe von Unternehmen, etwa NSO Group Technologies und dessen Produkt Pegasus, die Dienstleistungen und Produkte zu diesem Zweck anbieten. International wurden bereits strategische Maßnahmen diskutiert und teilweise umgesetzt, darunter Sanktionen und neue Regeln für Export-Beschränkungen. Die Existenz spezialisierter Firmen für Exploit-Entwicklung, Malware-Dienstleistungen und die Durchführung von Cyber-Operationen ermöglicht es auch Akteuren, die bisher wenige offensive Fähigkeiten besitzen, Angriffe durchzuführen. Zudem machen es international agierende Firmen schwieriger, Angreifer-Gruppen (bzw. Kunden) voneinander abzugrenzen und deren Beobachtung zu priorisieren. Die Bedrohungslage wird also durch die steigende Anzahl von Angreifern und die hohe Verfügbarkeit von qualitativ ausgereiften *Exploits* und *Malware* kritischer und zugleich schwieriger zu analysieren.

Spear-Phishing durch APT-Gruppe GhostWriter

Sachverhalt
Im Berichtszeitraum wurden in mehreren Wellen Phishing-Mails an deutsche Politikerinnen und Politiker sowie an Aktivistinnen und Aktivisten versendet. Die Phishing-Wellen erstreckten sich über mehrere Monate. Die Kampagne wurde einer Angreifergruppe namens Ghostwriter zugeordnet. Die Gruppe ist bekannt dafür, Zugänge zu E-Mail-Postfächern und zu Webseiten zu sammeln und diese zu nutzen, um Inhalte für Desinformationskampagnen zu verbreiten. Ein besonderes Merkmal der Angriffe war, dass sie sich nicht gegen die dienstlichen Postfächer der Abgeordneten und ihrer Mitarbeitenden in den Landtagen und dem Bundestag richteten. Stattdessen wurden die Phishing-Mails an GMX- und T-Online-Postfächer verschickt. Das Ziel war es, die Empfängerinnen und Empfänger dazu zu verleiten, ihre privaten E-Mail-Zugangsdaten auf den Servern der Angreifer einzugeben. Im März 2022 warnte das Bundesamt für Verfassungsschutz in einem Schreiben an potenziell Betroffene, dass die Gruppe GhostWriter erneut Phishing-Mails gegen deutsche Bürgerinnen und Bürger versende. Die Behörde ging von einem Zusammenhang mit dem Angriffskrieg gegen die Ukraine und den damit verbundenen deutschen Unterstützungsleistungen für die Ukraine aus.[8]

Bewertung
Auffällig war, dass die Gruppe, die normalerweise gegen osteuropäische Ziele aktiv ist, genau im „Superwahljahr" 2021 in Deutschland aktiv wurde. Ein Zusammenhang mit den damals anstehenden Bundestags- und Landtagswahlen war daher nicht auszuschließen. Die Motivation bzw. Zielrichtung der Kampagne konnte jedoch nicht zweifelsfrei identifiziert werden. Desinformationsinhalte, die eindeutig mit dieser Kampagne in Verbindung gebracht werden können, wurden nicht beobachtet. Insbesondere wurden auch Mitglieder von Landtagen in Bundesländern angegriffen, in denen 2021 nicht (und teilweise auch nicht in 2022) gewählt wurde.
Eine BSI-Analyse der Kampagne von 2021 ergab, dass die Angreifer teilweise Postfächer adressierten, die nicht Politikerinnen und Politikern, sondern Personen mit gleichem Namen gehörten. Viele der E-Mail-Adressen ließen sich über Web-Suchen oder in großen Passwort-Leaks finden. Es liegt nahe, dass die Angreifer die E-Mail-Adressen auf diesem Weg gesammelt haben und nicht immer verifizieren konnten, wem die Postfächer gehören.

Reaktion
Der Sachverhalt wurde im Nationalen Cyber-Abwehrzentrum bearbeitet. Die Behörden führten Sensibilisierungsmaßnahmen und IT-Sicherheitsberatungen mit Fraktionen und anderen potenziell Betroffenen durch.
Anfang September 2021, vor der Bundestagswahl, äußerte die Bundesregierung in einer Pressekonferenz die Einschätzung, dass die Gruppe dem russischen Militärgeheimdienst GRU zuzuordnen sei.

1.5 — Distributed Denial of Service

Als Denial-of-Service-Angriffe (DoS-Angriffe) werden Überlastungsangriffe auf Internetdienste bezeichnet. Wird ein solcher Angriff mittels mehrerer Systeme parallel ausgeführt, spricht man von einem verteilten bzw. *Distributed Denial of Service (DDoS). DDoS-Angriffe* existieren seit nunmehr über zwanzig Jahren. *DDoS* zählt weiterhin zu den Hauptbedrohungen für die Cyber-Sicherheit. Dies wird u. a. auch von einer repräsentativen Studie des Bitkom e.V. bestätigt, bei der mehr als 1.000 Unternehmen aller Branchen zu ihrer Betroffenheit durch Cyber-Angriffe in den Jahren 2020 und 2021 befragt wurden. Rund 27 Prozent gaben an, dass *DDoS-Angriffe* innerhalb der letzten zwölf Monate zu einem Schaden im Unternehmen geführt hätten. Das war hinter *Malware* mit 31 Prozent der 2. Platz unter den Angriffsarten und entsprach einer Zunahme der schadenverursachenden *DDoS-Angriffe* um rund acht Prozentpunkte gegenüber dem vorigen Berichtszeitraum[9].

Das BSI beobachtet im Berichtszeitraum die Entwicklung von *DDoS-Angriffen* im Netz eines großen deutschen Internetproviders. Die durchschnittliche Bandbreite im Berichtszeitraum lag dabei bei rund 684 Mbps (Megabit per second). Allerdings erreichten einzelne Angriffe immer wieder auch maximale Bandbreiten von über 200.000 Mbits. Die maximal gemessene Bandbreite eines DDoS-Angriffs lag in diesen Daten im Berichtszeitraum bei über 290.000 Mbits. Der Angriff fand am 2. Dezember 2021 statt und dauerte 228 Minuten. Die durchschnittliche Bandbreite dieses Angriffs lag bei 50.000 Mbits.

Über alle Angriffe hinweg gemittelt haben die durchschnittlichen Bandbreiten beobachteter *DDoS-Angriffe* im Berichtszeitraum tendenziell abgenommen (vgl. Abbildung 17).

Grund dafür dürfte unter anderem sein, dass sich eine seit Jahren beobachtbare Strukturveränderung innerhalb der DDoS-Angriffsarten fortsetzt: Die Angreifer setzen nicht mehr so sehr auf hohe Bandbreiten, sondern greifen verstärkt auf Netzwerk- und Transportebene an, was mit geringeren Bandbreiten einhergeht. Bei diesen Angriffen gehen die Angreifer präzise vor, um mit effizientem Mitteleinsatz Überlastungen im Angriffsziel auszulösen.

Technische Lage

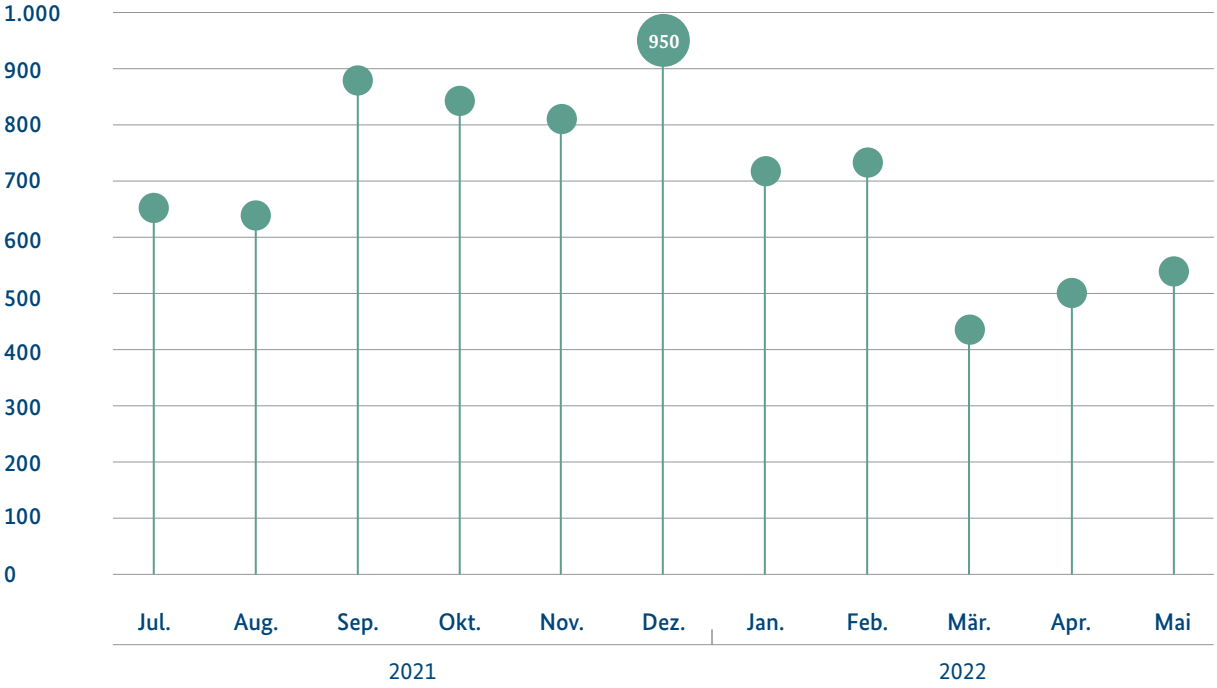
Im internationalen Umfeld verzeichnete der Security-Anbieter Radware Inc. im Jahr 2021 innerhalb der ersten neun Monate 75 Prozent mehr *DDoS-Angriffe* als in den ersten neun Monaten des Vorjahres[10]. In Deutschland verzeichnete der deutsche Mitigationsdienstleister Link11 für das Gesamtjahr 2021 einen Anstieg der Angriffe von 41 Prozent im Vergleich zum Vorjahr[11].

Trotz des Trends zu Angriffen auf Netzwerk und Protokollebene wurden im dritten Quartal 2021 auf drei Kontinenten die Rekordwerte von volumetrischen *DDoS-Angriffen* gebrochen. Sowohl die Bandbreiten als auch die Anfrageraten erreichten bis dahin nicht beobachtete Werte. Microsoft berichtete über einen abgewehrten DDoS-Angriff mit einer Bandbreite von 2,4 Tbps (Terabit per second), der in der letzten Augustwoche 2021 auf einen Azure-Kunden in Europa abzielte[12]. Dies liegt deutlich über der maximalen Bandbreite, die vom BSI im deutschen Providernetz beobachtet wurde (siehe oben). Microsoft zufolge stammte der Angriffsverkehr aus etwa 70.000 Quellen und mehreren Ländern im asiatisch-pazifischen Raum sowie aus den Vereinigten Staaten. Der *Angriffsvektor* war UDP-Reflection, die sich über mehr als zehn Minuten mit kurzen Stößen erstreckte, die jeweils innerhalb von Sekunden auf Terabit-Volumen anstiegen. Aufgrund seiner hohen Angriffsbandbreite verfügte der Angriff über sehr hohes technisches Potenzial. Da die Anbindungsbandbreite im Ziel höher war als die Angriffsbandbreite, hatte der Vorfall keine nennenswerten Auswirkungen.

Mitte August berichtete Cloudflare über einen DDoS-Angriff, bei dem der Anfrageraten-Rekordwert von 17,2 Mrps (Million requests per second / Millionen Anfragen pro Sekunde) erreicht wurde. Ausgeführt wurde der Angriff mit dem Mirai-Botnetz, bei dem mehr als 20.000 infizierte Geräte aus 125 Ländern zum Einsatz kamen. Ziel des Angriffs war ein Unternehmen im Finanzsektor[13]. Nur wenig später meldete der russische DDoS-Mitigationsdienstleister Qrator einen DDoS-Rekordwert mit 21,8 Mrps beim DDoS-Parameter Anfrageraten[14]. Erreicht wurde dieser Wert unter Anwendung des neu entdeckten Meris-Botnetzes mit weltweit etwa 250.000 infizierten Geräten, von denen die meisten von einem einzigen Hersteller stammen. Ziel des Angriffs war die Infrastruktur einer russischen Bank, die auf Yandex-Servern gehostet wurde. Inoffiziellen Quellen zufolge soll sich das Botnet ab zirka 80 US-Dollar pro Stunde mieten lassen. Bei Angriffen gegen „Voice over Internet Protocol"-Provider (VoIP-Provider) wurden Angriffe auf

Durchschnittliche Brandbreite aller bekannt gewordenen DDoS-Angriffe je Monat
Megabits pro Sekunde

Abbildung 17:
Durchschnittliche Bandbreite bekannt gewordener DDoS-Angriffe je Monat
Quelle: BSI



unterschiedlichen OSI-Layern kombiniert. Während Angriffe auf Anwendungsebene auf HTTP-Webseiten und APIs zielten, richteten sich Angriffe auf Netzwerk- und Transportebene gegen VoIP-Server-Infrastrukturen. Hierbei wurden TCP und UDP Flooding eingesetzt. VoIP-Services sind besonders anfällig für UDP-basierte Angriffe.

DDoS-Schutzgelderpressungen als Modus Operandi von *DDoS-Angriffen*

Wie schon im vergangenen Berichtszeitraum wurden Anfang Juni 2021 erneut umfangreiche DDoS-Erpressungen beobachtet. Betroffen waren zu diesem Zeitpunkt bereits verschiedene Länder in Europa. Bestätigt wurden Erpressungsversuche u. a. in Irland, Belgien, Portugal, Finnland, Österreich, Dänemark und der Schweiz. Die Erpresser-Welle traf viele Unternehmen zu einem Zeitpunkt, in dem sich ein Großteil der Belegschaft noch über Remote-Working organisiert hatte und auf uneingeschränkten Zugang zum Unternehmensnetz angewiesen war. Das Vorgehen der Cyber-Kriminellen, die sich „Fancy Lazarus“ nennen, ist bei den jeweiligen Angriffen ähnlich: In einer Erpressungs-E-Mail an ein Unternehmen kündigen sie einen Demo-Angriff an und fordern zur Zahlung von *Bitcoins* auf. Der angekündigte Demo-Angriff erfolgt meistens mit Spitzenbandbreiten von zirka 30 bis 250 Gbps unter Anwendung des *Angriffsvektors* DNS-Reflection. Falls das Unternehmen nicht fristgerecht zahlen sollte, wird ein bandbreitenstarker großer DDoS-Angriff mit mehr als zwei Tbps angedroht.

Über das tatsächliche Auslösen dieser Angriffe im Falle des Verstreichens der Frist gibt es unterschiedliche Meldungen. Das FBI berichtet von vielen betroffenen Unternehmen, die nach Ablauf der Frist keine weiteren Aktivitäten beobachteten oder die Angriffe erfolgreich mitigieren konnten[15]. Link11 berichtet zudem über Unternehmen, bei denen es zu beträchtlichen Störungen kam. Die dabei erreichten Spitzenbandbreiten lagen aber regelmäßig weit unter der angedrohten Angriffsbandbreite von zwei Tbps[16].

Die Erpressungskampagnen richteten sich zwischen August und Oktober 2021 auch gegen mehrere VoIP-Provider in Nordamerika und Europa. Auch im Jahr 2021 beobachtete das BSI vor den anstehenden umsatzstarken Online-Aktivitäten im E-Commerce-Bereich

(Black Friday, Cyber Monday, Vorweihnachtsgeschäft, Weihnachtsgeschäft) einen Anstieg der Aktivitäten im DDoS-Bereich. Das Aufstellen von rekordverdächtigen Spitzenwerten für die Angriffsbandbreite (*DDoS* gegen MS Azure) und für die Anfrageraten (*DDoS* gegen Yandex mit Meris-Botnetz) durch neu entwickelte DDoS-Angriffstechnologien sind Belege dafür.

Das BSI hat aufgrund der verschiedenen Beobachtungen der technischen DDoS-Entwicklungen und der Entwicklung bei der DDoS-Schutzgelderpressungen im Vorfeld des Vorweihnachtsgeschäfts öffentlich gewarnt. Organisationen wurde empfohlen, ihre DDoS-Schutzmaßnahmen zu evaluieren, um der aktuellen Bedrohungslage begegnen zu können. Hierbei sollte besonderes Augenmerk auf UDP-Reflection-Angriffe und Angriffe mit hohen Anfrageraten gelegt werden. Tatsächlich legten die DDoS-Aktivitäten um 100 Prozent im Vergleich zum Vorjahr zu[17]. Mit 1,1 Tbps wurde der höchste bislang in Deutschland gemessene Volumenangriff detektiert, der doppelt so hoch ausfiel wie der bisherige Rekordwert aus Mai 2021 mit 550 Mbps.

Neben den geschilderten kriminell motivierten DDoS-Schutzgelderpressungen hat das BSI auch Fälle von politisch motivierten DDoS-Aktivitäten beobachtet. So kam es im Umfeld der Bundestagswahl 2021 in mehreren Fällen zu DDoS-Vorfällen. Auch Überlastsituationen von Webseiten aufgrund legitimer Anfragen wurden beispielsweise im Umfeld von Parteitagen beobachtet.

Auch im Rahmen des russischen Angriffskriegs gegen die Ukraine kam es darüber hinaus international zu politisch motivierten DDoS-Angriffen, die überwiegend dem Phänomen des Hacktivismus zugeordnet wurden (vgl. Kapitel *Cyber-Sicherheitslage im Kontext des russischen Angriffskrieges gegen die Ukraine*, Seite 45).

1.6 – 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.

Dagegen können folgende Aspekte dazu führen, dass das theoretische Sicherheitsniveau in der Praxis reduziert ist:

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

Durch die Auswahl ungeeigneter Algorithmen bzw. fehlerhafte Implementierungen kann die Wirksamkeit im schlimmsten Fall vollständig aufgehoben werden (Beispiel siehe Kasten *Schwache RSA-Schlüsselerzeugung – falsche Methoden und schlechter Zufal*l, Seite 44).

Bei der Absicherung von Kryptosystemen, die selbst Angreifern in räumlicher Nähe standhalten sollen, sind zusätzlich Seitenkanäle (z. B. Stromverbrauch oder elektromagnetische Abstrahlung der Geräte) zu berücksichtigen, über die ebenfalls Daten abfließen können. Die Seitenkanalanalyse, also die Analyse auf Anfälligkeit für *Seitenkanalangriffe*, ist ein Forschungszweig, der neue Gegenmaßnahmen und 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 in der Kryptografie*, Seite 98).

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

Die Sicherheitsgarantien vieler heute eingesetzter Kryptoalgorithmen gelten allerdings nicht mehr, sobald ein hinreichend leistungsstarker Quantencomputer zur Verfügung steht. Die Kapitel 2.5.2 Kryptografie (Seite 99) und 2.5.3 Quantum Key Distribution (Seite 99) zeigen Möglichkeiten auf, dieser Bedrohung zu begegnen, und stellen die Aktivitäten des BSI in diesem Bereich dar.

Schwache RSA-Schlüsselerzeugung – falsche Methoden und schlechter Zufall

Die Sicherheit kryptografischer Verfahren, die auf RSA basieren, beruht insbesondere auf der Schwierigkeit, RSA-Module zu faktorisieren. Dieser ist Teil des öffentlichen RSA-Schlüssels und das Produkt zweier nicht öffentlicher Primzahlen p und q. Sind p und q einem Angreifer bekannt, kann das kryptografische Verfahren leicht gebrochen werden. Das BSI macht in der Technischen Richtlinie TR-02102 Vorgaben zur Länge des RSA-Moduls und zu dessen Erzeugung. Werden diese Bedingungen bei der Erzeugung von n beachtet, ist es nach derzeitigem Kenntnisstand praktisch nicht möglich, nur aus der Kenntnis von n die beiden Primfaktoren p und q zu ermitteln. Auf RSA basierende Verfahren sind nicht mehr sicher, sobald ein hinreichend starker Quantencomputer zur Verfügung steht (siehe Kapitel Kryptografie, Seite 99).

Im Februar 2022 wurde ein Angriff veröffentlicht (CVE-2022-26320)[18], in welchem die Faktorisierungsmethode von Fermat auf eine Vielzahl publizierter RSA-Moduli angewendet wurde und so für eine kleine Anzahl dieser Moduli die Primfaktoren bestimmt werden konnten. Die betreffenden RSA-Moduli gehörten zu den öffentlichen Schlüsseln von TLS-Zertifikaten verschiedener Druckermodelle, die alle ein bestimmtes Kryptomodul verwendeten. Der mehr als 300 Jahre alte Algorithmus von Fermat ist immer dann effizient anwendbar, wenn die beiden Primzahlen p und q relativ nah beieinanderliegen. Das kann zum Beispiel passieren, wenn der Algorithmus für die Schlüsselerzeugung zunächst p zufällig wählt und anschließend von p ausgehend hochzählt, bis die nächste Primzahl q gefunden wurde. Im Wesentlichen sucht der Algorithmus von Fermat in einer relativ kleinen Umgebung der Wurzel von n nach Kandidaten für die Primfaktoren p und q. Liegen p und q genügend nah beieinander, ist die Suche schnell erfolgreich – und n ist faktorisiert. So ist zum Beispiel im Extremfall, wenn p und q übereinstimmen, der Primfaktor p bereits durch die Wurzel von n gegeben.

Eine weitere im September 2021 veröffentlichte Schwachstelle betrifft die Erzeugung identischer RSA-Schlüssel durch die Javascript-Bibliothek Keypair (CVE-2021-41117)[19]. Keypair wurde dabei von dem GitHub-Client GitKraken und eventuell weiteren Clients verwendet, um Schlüssel für das SSH-Protokoll zu erzeugen. Eine Analyse des Quellcodes von Keypair hat dabei eine Reihe von kritischen Schwachstellen in der Implementierung der Zufallszahlenerzeugung identifiziert: Keypair verwendet einen eigenen deterministischen Zufallszahlengenerator. Diesem muss initial ein sogenannter Seed, der idealerweise aus echtem Zufall besteht, übergeben werden. Ab da erfolgt die Weiterverarbeitung dann vollständig deterministisch: Gleiche Seeds führen auch stets zur Ausgabe gleicher Zufallszahlen. Ein Fehler im Quellcode von Keypair verhindert dabei die Ausführung eines RNGs der Javascript-Bibliothek der eigentlich für die Berechnung des Seeds eingesetzt werden sollte. Als alternative Seed-Quelle verbleibt dann nur noch ein für kryptografische Einsatzzwecke ungeeigneter RNG. Ein zusätzlicher Implementierungsfehler resultiert letztlich darin, dass dieser RNG fast nur Nullen ausgibt. Die vom Keypair-RNG ausgegebenen Werte wiederholen sich damit regelmäßig und resultieren in der Erzeugung identischer RSA-Schlüssel.

1.7 – Hybride Bedrohungen

Illegitime Einflussaktivitäten fremder Staaten, sogenannte *hybride Bedrohungen*, stellen eine Gefahr für Staat, Wirtschaft und Gesellschaft dar und sollen das jeweilige Zielland destabilisieren. Zu hybriden Bedrohungen können unterschiedliche Maßnahmen zählen, die orchestriert eingesetzt werden, wobei eine Urheberschaft möglichst verschleiert werden soll. Die Maßnahmen und *Angriffsvektoren* bleiben dabei – im Vergleich zu einem offenen militärischen Konflikt – meist bewusst unterschwellig und besitzen häufig eine ambivalente Wirkung, die es dem Zielland erschwert, auf diese Art von Bedrohungen zu reagieren. Insbesondere Cyber-Angriffe, aber auch wirtschaftliche Maßnahmen, die gezielte Steuerung von Migration oder Desinformation, stellen mögliche Mittel dar. Maßnahmen lassen sich zudem in ihrer Intensität steigern und können in einen offenen bewaffneten Konflikt mit hybrider Kriegsführung münden, wie es der Angriffskrieg Russlands auf die Ukraine verdeutlicht (vgl. Kapitel *Cyber-*

Sicherheitslage im Kontext des russischen Angriffskrieges gegen die Ukraine, Seite 45).

Der Dimension „Cyber“ kommt in Bezug auf *hybride Bedrohungen* eine herausgehobene Stellung zu. Cyber-Angriffe sind für hybrid agierende Angreifer besonders aufgrund ihrer Schnelligkeit, schwierigeren Zuordnung, Ort- und Grenzenlosigkeit sowie infolge geringer Kosten ein attraktiver *Angriffsvektor*, der sich auch als Multiplikator zur Unterstützung anderer Methoden einsetzen lässt.

Angriffe in der Dimension „Cyber“ können darüber hinaus in anderen Dimensionen wirken, wie etwa den Dimensionen Information oder Medien. Ein Beispiel hierfür sind sogenannte Hack-and-Act-Operationen, in denen zunächst mittels Cyber-Angriffen Daten erbeutet werden, die zu einem späteren, vermeintlich günstigen Zeitpunkt, durch einen Angreifer veröffentlicht werden.

Zu den Aufgaben des BSI in der Abwehr von hybriden Bedrohungen in der Dimension „Cyber“ zählen unter anderem die Etablierung und Koordinierung von Maßnahmen zur Absicherung von Wahlen, der Dialog mit Betreibern sozialer Medien, die Sensibilisierung von Staat, Wirtschaft und Gesellschaft für Themen der IT-Sicherheit, sowie die Unterstützung von Betreibern Kritischer Infrastruktur (vgl. Vorfall *Cyber-Angriff auf deutschen Mineralölhändler*, Seite 50).

Der Berichtszeitraum war durch das „Superwahljahr 2021“ und mögliche Bedrohungsszenarien für die Bundestagswahl geprägt. Im Vorfeld der Wahl kam es zu Phishing-Mail-Wellen gegen deutsche Mandatsträgerinnen und -träger in Bund und Ländern, die sich als Vorbereitungshandlungen für weiterführende Angriffe, gegebenenfalls auch im Zusammenhang mit der Verbreitung von Desinformation, werten lassen. Das Bundesamt für Verfassungsschutz und das BSI warnten daher gemeinsam und ergriffen geeignete Maßnahmen zur Absicherung der Mandatsträgerinnen und -träger.

1.8 — Cyber-Sicherheitslage im Kontext des russischen Angriffskrieges gegen die Ukraine

Der russische Angriffskrieg gegen die Ukraine wird von anhaltenden Aktivitäten im Cyber-Raum begleitet. Dies macht eine dauerhafte Lagebeobachtung und -bewertung erforderlich. Das BSI steht hierzu fortwährend in engem Austausch mit nationalen und internationalen Partnerbehörden und berichtet regelmäßig an die Bundesregierung und die Bundesverwaltung. Die Zusammenarbeit mit nationalen Behörden erfolgt dabei insbesondere im Nationalen Cyber-Abwehrzentrum.

Die Cyber-Aktivitäten im Umfeld des Krieges waren vielfältig ausgeprägt. In den ersten Tagen kamen besonders gegen ukrainische Stellen sogenannte *Wiper* zum Einsatz. *Wiper* sind Programme, die zum unwiederbringlichen Löschen von Daten verwendet werden. Sie wurden beispielsweise gegen ukrainische Banken eingesetzt. Seit Kriegsbeginn wurden auch verstärkt Aktivitäten bestimmter APT-Gruppen beobachtet, die zum Beispiel Spear-Phishing-Mails an westliche politische, administrative oder militärische Stellen richteten.

In Deutschland wurden zu Kriegsbeginn Troll-Aktivitäten in den sozialen Medien beobachtet. Dabei wurde eine Vielzahl pro-russischer Kommentare auf Social-Media-Auftritten westlicher Medien hinterlassen.

Im Verlauf des Krieges traten Hacktivisten-Gruppen in Erscheinung. Dabei handelte es sich um Aktivisten, die für eine der beiden Seiten Partei ergriffen und durch öffentlichkeitswirksame Aktionen auffielen. Prominentes Beispiel ist die pro-russische Gruppe Killnet, welche u. a. durch DDoS-Angriffe auf Ziele in europäischen Ländern durchführte. Das BSI schätzte die Bedrohungslage für Deutschland durch DDoS-Angriffe von Killnet als eher gering ein. Es gab mehrere Angriffswellen gegen deutsche Ziele, die Killnet zugeordnet wurden. Die hier verwendeten Angriffsbandbreiten waren jedoch vergleichsweise gering und nach Erkenntnissen des BSI hatten die Angriffe wenig Auswirkungen auf die Verfügbarkeit. Sie ließen sich spätestens mit der Aktivierung von DDoS-Schutzmechanismen wirksam mitigieren.

Prominente Beispiele für pro-ukrainische Hacktivisten-Gruppen wiederum sind hier die Kollektive Anonymous und IT-Army. Dabei hat es auch Angriffe gegen Unternehmen außerhalb Russlands gegeben, die entweder Geschäftsbeziehungen zu Russland haben oder einem russischen Konzern angehören. Ein Beispiel dafür ist ein Angriff von Anonymous gegen einen deutschen KRITIS-Betreiber, der Teil eines russischen Ölkonzerns ist. Durch den Angriff kam es zur Einschränkung einer kritischen Dienstleistung.

Die in der Ukraine beobachteten Cyber-Angriffe zeigten meist keine substanziellen technischen Neuerungen. Ausnahme ist eine neue Variante von Industroyer. Die Schadsoftware richtet sich speziell gegen Prozesssteuerungssysteme und wurde 2016 eingesetzt, um Stromausfälle in der Ukraine hervorzurufen. Industroyer2 ist im April 2022 erneut in ukrainischen Umspannwerken gefunden worden, ließ sich aber deaktivieren, bevor es zur Sabotage kommen konnte.

Die Sanktionen gegen russische Unternehmen führten auch zu Einschränkungen bei IT-Dienstleistungen für russische Firmen. So zeigte sich bei einem IT-Sicherheitsvorfall gegen ein russisches Unternehmen in Deutschland, dass eine schnelle Wiederherstellung durch IT-Dienstleister nur eingeschränkt möglich war. Auch die Verfügbarkeit von Software-Updates kann für sanktionierte Unternehmen eingeschränkt sein.

Die Angreifer hinter dem *RaaS* Conti positionierten sich zu Beginn des Ukraine-Krieges pro-russisch und drohten westlichen Staaten mit Vergeltungsschlägen, sollten sie russische Einrichtungen oder kritische Infrastruktur angreifen. In der Folge dieser Positionierung wurden eine Vielzahl interner Daten der Gruppe geleakt, die zeigen, dass die pro-russische Positionierung der Hacker-Gruppe intern durchaus umstritten gewesen sein muss. Im April 2022 wurden dann mehrere Conti-Vorfälle in Costa Rica bekannt, welche die Angreifer als Demonstration eines Cyber-Angriffs gegen ein gesamtes Land bezeichneten. Am 8. Mai 2022, dem Tag seines Amtsantritts, musste der Präsident Costa Ricas infolgedessen den Notstand ausrufen. Zumindest 27 staatliche Einrichtungen waren betroffen, neun davon schwer. Erstmals überhaupt war damit ein gesamter Staat von einem Cyber-Angriff betroffen. Neben der Darstellung der Angreifer, es habe sich um einen gezielten Angriff zu Demonstrationszwecken gehandelt, kann das BSI jedoch auch einen finanziell motivierten, opportunistischen Angriff nicht ausschließen, den die Angreifer erst im Nachhinein umdeuteten. Dem IT-Sicherheitsdienstleister AdvIntel zufolge schalteten die Angreifer hinter der *RaaS* Conti ihre Server am 19. Mai 2022 ab. Das BSI kann dies weder bestätigen noch widerlegen. Im Falle einer Beendigung der *RaaS* Conti geht das BSI von einer Wanderung der *Affiliates* zu anderen aktiven RaaS-Gruppen aus.

Im Rahmen seiner Analyse-Kompetenz hat das BSI zu Beginn des Krieges vor Kollateralschäden in Deutschland gewarnt. Ein derartiger Fall ist im Kriegsverlauf aufgetreten, als ein Angriff auf einen Satelliten-Dienstleister zum Ausfall von Modems in deutschen Windkraftanlagen führte. Dieser Fall ist der erste bekannte Cyber-Kollateralschaden, den das BSI im Zuge des Konflikts beobachtet hat (vgl. Vorfall *Kollateralschäden nach Angriff auf ein Unternehmen der Satellitenkommunikation*, Seite 49).

Durch den russischen Angriffskrieg gegen die Ukraine hat sich die Bedrohungslage in Deutschland insgesamt weiter erhöht. Es ließen sich zahlreiche Cyber-Aktivitäten gegen verschiedene westliche Staaten beobachten, die vereinzelt auch Kritische Infrastrukturen in Deutschland betrafen (vgl. Vorfall *Kollateralschäden nach Angriff auf ein Unternehmen der Satellitenkommunikation*, Seite 49, *Vorfall Cyber-Angriff auf deutschen Mineralölhändler*, Seite 50). Eine zentral gesteuerte Kampagne gegen Deutschland mit einer breiten Wirkung war bis Redaktionsschluss aber nicht erkennbar. Gleichzeitig besteht weiterhin eine große Bedrohung durch Angriffe, die nicht im Zusammenhang mit dem Krieg gegen die Ukraine stehen, insbesondere durch *Ransomware*. Weiterhin beobachtet das BSI, dass der Krieg gegen die Ukraine auch als Betrugsmasche im Rahmen von *Spam* genutzt wurde. Bereits kurz nach Kriegsbeginn gab es erste Spam-Mails, die sich gegen die breite Masse der Bevölkerung richteten. Sogenannter Charity-Scam, der bereits im Zusammenhang mit der Flutkatastrophe vom Sommer 2021 zu beobachten gewesen war, nutzte auch den Krieg gegen die Ukraine aus, um vermeintlich Spendengelder zu sammeln (vgl. Abbildung 18).

Um vertrauenswürdig zu wirken, fälschen die Angreifer dafür auch das Corporate Design seriöser Hilfsorganisationen. Das Opfer soll hierbei zum Klicken verleitet werden, um dann vermeintliche Spendengelder und persönliche Daten preiszugeben (vgl. Abbildung 19). Bei Vorschussbetrügereien im Zusammenhang mit dem Krieg gaben sich Angreifer zum Beispiel als ukrainische Flüchtlinge aus und versprachen Spam-Opfern eine fürstliche Entlohnung für deren finanzielle Hilfe bei einer vermeintlichen Flucht.

Auch in der Kategorie des Finance Phishing waren die Auswirkungen des Krieges zu beobachten. Angreifer fälschten dafür das Corporate Design von verbreiteten Banken und Sparkassen und verschickten Spam-Mails, um angeblich die Einhaltung von Sanktionen zu überprüfen. Ziel dieser Phishing-Mails ist es aber lediglich, das Opfer zum Klicken zu verleiten und persönliche Daten wie Zugangsdaten zum Online-Banking abzugreifen.

Beispiel einer Charitiy-Scam-Mail

Abbildung 18:
Charitiy-Scam-Mail
Quelle: Phishing-Radar des BSI in Zusammenarbeit mit der Verbraucherzentrale NRW

Von: Ukraine Crisis Relief Fund <ukrarelief@unations.com>
Gesendet: Dienstag, 1. März 2022 11:39
An: [redacted]
Betreff: [redacted], Donate To Ukraine and save a life, Please read

Hello,

We are urging you to please donate to Ukrainians as many people have fled their homes to seek refuge. Help us provide a safe solution for Ukrainian families who have already suffered too much, Shelter, water for those who need it the most in this time of crisis.

You can give any amount, since the banks are not working, kindly save a life, and donate to us through our UCRF (Ukraine Crisis Relief Fund) wallet.

Bitcoin Wallet: [redacted]

We Sincerely appreciate your help.

Thank You,
Amin Awad
Ukraine Crisis Relief Fund

Beispiel einer Charitiy-Scam-Mail

Abbildung 19:
Charitiy-Scam-Mail
Quelle: Phishing-Radar des BSI in Zusammenarbeit mit der Verbraucherzentrale NRW

Von: Für Menschen mit Herz <mail@world-of-shopping-mail.de>
Gesendet: 27. Februar 2022 14:37
An: [redacted]
Betreff: +++ Ukraine: Hilfe dringend benötigt +++

Sollte der Newsletter nicht richtig dargestellt werden, klicken Sie bitte hier

Malteser International
Order of Malta Worldwide Relief

Malteser
...weil Nähe zählt.

Eskalation im Ukraine-Konflikt

Erste Hilfslieferung unterwegs

Bild: Malteser Ukraine

♡ Jetzt spenden!

Liebe Leserin, lieber Leser,

wir alle hatten die Hoffnung, dass die Ukraine und Russland ihren Konflikt ohne weitere kriegerische Handlungen lösen. Heute kamen dann die unfassbaren Nachrichten: Russland hat die Ukraine angegriffen.

Kollateralschäden nach Angriff auf ein Unternehmen der Satellitenkommunikation

Sachverhalt

Am 24. Februar 2022 fiel um etwa 3 Uhr Weltzeit im europäischen Raum ein Satellitendienst aus. Über diesen werden u. a. Prozesse zur Entstörung von Windenergieanlagen in der Strombranche mittels Satellitenkommunikationslösungen unterhalten. Infolge der Störung konnten rund 5.800 Windenergieanlagen nicht mehr mittels Fernwartung gewartet werden[20]. Weiterhin kam es auch bei deutschen Kundinnen und Kunden zu Störungen bei der Implementierung der Satellitenkommunikationslösungen und darüber hinaus waren auch Geräte der Gefahrenabwehr eines Landkreises betroffen. Der Betreiber räumte ein, Störungen aufgrund eines Firmware-Updates zu haben und mutmaßte über eine Manipulation (d. h. einen Cyber-Angriff). Ein Dienstleister wurde mit der Untersuchung des Vorfalls beauftragt. Die betroffenen Modems mussten auf Werkseinstellungen zurückgesetzt werden, um ihre Funktionsfähigkeit wieder herzustellen[21]. Von der Störung waren auch weitere Staaten betroffen, darunter Frankreich[22] und Irland.

Bewertung

Am 30. März 2022 veröffentlichte der Betreiber weitere Informationen und bestätigte, dass es sich am 24. Februar 2022 um einen Angriff gehandelt hat. Eine Attribution wurde allerdings nicht vorgenommen. Ziel des Angriffs sei die Nicht-Verfügbarkeit des Dienstes gewesen. Der Angriff soll sich nur auf einen von privaten Nutzerinnen und Nutzern verwendeten Bereich des Satellitennetzes gerichtet haben. Das Unternehmen entdeckte demnach zuerst einen gezielten Denial-of-Service-Angriff mit einem sehr hohen Volumen an Datenverkehr, bei dem viele Modems offline gingen. Absender des Datenverkehrs waren laut Analyse mehrere Modems und weitere zugehörige Geräte von Kundinnen und Kunden aus der Ukraine. Laut Angaben des Betreibers sei ein Zugriff auf Kundendaten oder ein unrechtmäßiger Zugriff auf persönliche Kundengeräte nicht feststellbar gewesen. Die forensische Analyse ergab, dass sich die Angreifer durch eine fehlkonfigurierte VPN-Verbindung Zugang zu einem Management-Netz verschafft hatten. Über dieses sollen die Angreifer Befehle auf zehntausenden Modems zeitgleich ausgeführt haben. Dabei wurde der Flashspeicher überschrieben und die Modems unbrauchbar gemacht. Bei mehreren zehntausend Kundeninnen und Kunden soll der zuständige Dienstleister neue Modems verbaut haben bzw. die Modems sollen über ein Over-the-Air-Update gepatcht worden sein[23].

Der IT-Sicherheitsvorfall mit Störung der Verfügbarkeit der Satellitenkommunikation im Konfliktgebiet hatte in der Folge auch Auswirkungen u. a. auf die Wartungsfähigkeit von Windkraftanlagen in Deutschland.

Auswirkungen auf die Versorgungssicherheit in den mittelbar betroffenen Sektoren deutscher Kritischer Infrastrukturen, beispielsweise Energie, waren jedoch nicht zu beobachten. Die Stromversorgung und die Netzstabilität waren durch den Vorfall wahrscheinlich nicht beeinflusst. Die Windkraftanlagen arbeiteten im Regelbetrieb ohne Eingriffe von außen autark.

Reaktion

Beim BSI gingen im Zusammenhang mit dem Vorfall verschiedene Störungs- und Vorfallsmeldungen ein. Der Betreiber nahm eine forensische Analyse vor und bestätigte den Angriff. Die betroffenen Modems wurden durch den zuständigen Dienstleister ausgetauscht.

Cyber-Angriff auf deutschen Mineralölhändler

Sachverhalt
Am 11. März 2022 fielen bei einem deutschen Unternehmen zur Distribution und zum Handel von Mineralöl, einem Unternehmen mit russischem Mutterkonzern, mehrere virtualisierte Serversysteme aus. Daraufhin informierte der Betreiber umgehend seinen IT-Dienstleister und meldete den Vorfall gemäß den KRITIS-Meldepflichten nach §8b Abs. 4 BSIG an das BSI.

Zu dem Angriff bekannte sich die Gruppe Anonymous Deutschland. Ihr war es gelungen, tief in die Systeme des Unternehmens einzudringen und Daten in größerem Umfang von verschiedenen Speichersystemen, Mailservern und Festplattenimages auszuleiten. Die Daten wurden jedoch nicht veröffentlicht. Trotzdem musste der Betreiber seine gesamten Systeme als kompromittiert betrachten und diese abschalten. Für die Wiederherstellung der Systeme in einen Notbetrieb wurden Dienstleister benötigt, welche die Unterstützung wegen juristischer Unklarheiten bzgl. der Auslegung der EU-Sanktionsliste zunächst verweigerten. Nach Klärung der Situation mit Hilfe verschiedener Behörden konnten die benötigten Systeme in einen Notbetrieb überführt werden. Es kam zu keinen spürbaren Versorgungsengpässen.

Bis Redaktionsschluss befand sich das Unternehmen noch immer im Notbetrieb in einer abgeschotteten Umgebung. Daneben wurde versucht eine neue, sichere Systemumgebung unter Beachtung von Security-by-Design aufzubauen. Jedoch wurden auch hierfür Dienstleister benötigt, welche die Zusammenarbeit mit der deutschen Tochter eines russischen Mutterkonzerns mit Verweis auf die Sanktionen verweigerten. Eine Lösung hierfür konnte bis Redaktionsschluss noch nicht gefunden werden.

Bewertung
Der Erdölbevorratungsverband hat jederzeit Rohöl und Mineralölprodukte in Höhe der in Deutschland in einem Zeitraum von 90 Tagen netto eingeführten Mengen zu halten. Die Vorräte an Mineralölprodukten sind über ganz Deutschland verteilt, um schnell und flächendeckend die Nachfrage decken sowie wirksam auf regionale Versorgungsstörungen reagieren zu können. Der Mineralölhandel wird in Deutschland über ein großflächig verteiltes Netz an Distributionsstellen abgewickelt. Bei anhaltender Störung wäre ein volkswirtschaftlicher Schaden und Versorgungsverknappung (bei hohen Öl-Preisen) nicht auszuschließen gewesen.

Reaktion
Das BSI begleitete die Vorfallsanalyse und -bereinigung zusammen mit einem externen BSI-qualifizierten APT-Dienstleister und stand in regelmäßigem Austausch mit dem Betreiber, dem APT-Dienstleister und weiteren Behörden.

Industroyer2-Angriff auf ukrainischen Energiesektor

Sachverhalt

Am 12. April 2022 berichtete das CERT der Ukraine über einen Angriff auf eine ukrainische Organisation aus dem Energiesektor. Die Angreifergruppe Sandworm sollte einen Blackout für den 8. April 2022 vorbereitet haben. Die Vorbereitungen wurden jedoch entdeckt und der Blackout konnte verhindert werden[23]. Bei dem Vorfall soll eine neue Schadsoftware-Variante mit dem Namen Industroyer2 verwendet worden sein. Dabei scheint es sich um eine neue Version der Schadsoftware Industroyer – auch als Crashoverride bezeichnet – zu handeln, die bereits seit 2016 bekannt ist. Beide Versionen haben Steuerbefehle eines Standard-Kommunikationsprotokolls der International Electrotechnical Commission (IEC) implementiert und zielen damit auf Industrial Control Systems (ICS) ab. Der Code der neuen Variante ähnelt stark einem Modul aus der damaligen Industroyer-Variante. Daher gehen IT-Sicherheitsforscher davon aus, dass es sich um dieselbe Codebasis handelt. Ziel des Angriffs soll es gewesen sein, mit Hilfe von Industroyer2 Schäden an Umspannwerken zu erzeugen, um dadurch den Stromtransport zu beeinträchtigen oder zu verhindern.

Neben Industroyer2 soll außerdem u. a. folgende Schadsoftware eingesetzt worden sein:

- *CaddyWiper sollte die Wiederherstellung der auf Windows basierenden Systeme verlangsamen und die Betreiber des Energieunternehmens davon abhalten, die Kontrolle über die ICS-Systeme zurückzuerlangen. Die Malware CaddyWiper war zuvor bereits gegen eine ukrainische Bank und eine ukrainische Regierungsorganisation eingesetzt worden.*
- *Schäden an Linux-Servern sollten durch den Einsatz der Wiper Orcshred, Soloshred und Awfulshred erreicht werden.*

Bis zum Redaktionsschluss war weder der initiale Angriffsvektor bekannt noch, wie die Angreifer in das ICS-Netz gelangen konnten. Die Gruppe Sandworm wird oftmals einem russischen Nachrichtendienst zugeordnet und war mutmaßlich bereits 2015 für einen Cyber-Angriff auf das ukrainische Stromnetz verantwortlich.

Bewertung

Das ukrainische Stromnetz ist seit Mitte März 2022 an das europäische Verbundnetz angeschlossen. Daher könnte ein großflächiger Stromausfall in der Ukraine auch dazu führen, dass ein geringer Teil der vorgehaltenen Regelenergie des europäischen Verbundnetzes zur Stabilisierung des ukrainischen Stromnetzes herangezogen wird. Im Jahr 2016 wurde durch Industroyer ein großflächiger Stromausfall in der Ukraine herbeigeführt. Es kann daher davon ausgegangen werden, dass Industroyer2 ein vergleichbares Schadenspotenzial aufweist. Industroyer2 zeichnet sich – im Gegensatz zu Industroyer – durch eine hart-codierte Konfiguration aus. Daher müssen die Angreifer die Malware für jeden Einsatzzweck bzw. jedes Ziel modifizieren. Die Verwendung dieser Version von Industroyer2 gegen andere Ziele ist daher eher unwahrscheinlich. Gleichzeitig erschwert diese Änderung die Detektion, da Hashes für Industroyer2 als Indicators of Compromise (IoCs) jeweils für ein bestimmtes Ziel spezifisch sind.

Der geschilderte Vorfall könnte in ähnlicher Art auch Kritische Infrastrukturen in Deutschland treffen. Eine Beeinträchtigung von Energienetzkomponenten als Folge eines erfolgreichen Angriffs mit einer entsprechend modifizierten Version von Industroyer2 kann nicht ausgeschlossen werden.

Reaktion

Das BSI hat am 12. April 2022 eine Cyber-Sicherheitswarnung an die entsprechenden Zielgruppen versendet.

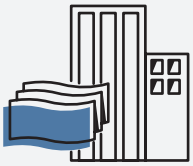
Die Lage der IT-Sicherheit in Deutschland 2022 im Überblick

Top 3-Bedrohungen je Zielgruppe:

Gesellschaft

Identitätsdiebstahl
Sextortion
Fake-Shops im Internet

Wirtschaft



Ransomware
Schwachstellen, offene oder falsch konfigurierte Online-Server
IT-Supply-Chain: Abhängigkeiten und Sicherheit

Staat und Verwaltung

Ransomware
APT
Schwachstellen, offene oder falsch konfigurierte Online-Server

Erster digitaler Katastrophenfall in Deutschland

207 Tage Katastrophenfall

Nach Ransomware-Angriff konnten Elterngeld, Arbeitslosen- und Sozialgeld, KfZ-Zulassungen und andere bürgernahe Dienstleistungen nicht erbracht werden.

Die Anzahl der Schadprogramme steigt stetig.

Die Anzahl neuer Schadprogramm-Varianten hat im aktuellen Berichtszeitraum um rund

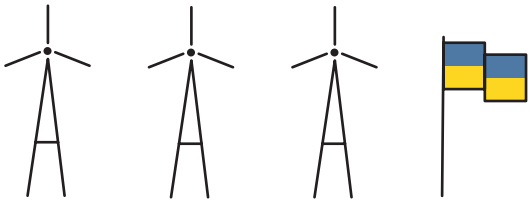
116,6 Millionen zugenommen.

Hacktivismus im Kontext des russischen Krieges:

Mineralöl-Unternehmen in Deutschland muss kritische Dienstleistung einschränken.

Kollateralschaden

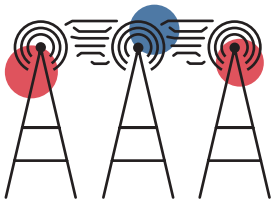
nach Angriff auf Satelliten-kommunikation



20.174

Schwachstellen in Software-Produkten (13 % davon kritisch) wurden im Jahr 2021 bekannt. Das entspricht einem **Zuwachs von 10 %** gegenüber dem Vorjahr.

15 Millionen Meldungen zu Schadprogramm-Infektionen in Deutschland übermittelte das BSI im Berichtszeitraum an deutsche Netzbetreiber.



34.000

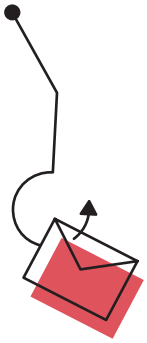
Mails mit Schadprogrammen wurden monatlich durchschnittlich in deutschen Regierungsnetzen abgefangen.

78.000

neue Webseiten wurden wegen enthaltener Schadprogramme für den Zugriff aus den Regierungsnetzen gesperrt.

69%

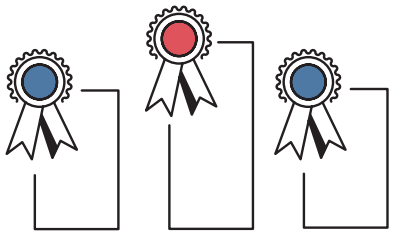
aller Spam-Mails im Berichtszeitraum waren Cyber-Angriffe wie z. B. Phishing-Mails und Mail-Erpressung.



90%

des Mail-Betrugs im Berichtszeitraum war Finance Phishing, d. h. die Mails erweckten betrügerisch den Eindruck, von Banken oder Sparkassen geschickt worden zu sein.

BSI ist weltweit der führende Dienstleister im Bereich Common-Criteria-Zertifikate.



5.100
2021

4.400
2020

Zehn Jahre Allianz für Cyber-Sicherheit:
2022 sind wir bereits

6.220
Teilnehmer.

Deutschland
Digital•Sicher•BSI•

---

12 Monate Cyber-Sicherheit im Überblick

Juni 21

- Neuer Beirat Digitaler Verbraucherschutz in Deutschland tagt erstmalig
- BSI erteilt erstes Zertifikat nach dem Schema „Beschleunigte Sicherheitszertifizierung“
- BSI eröffnet neuen Stützpunkt mit KI-Schwerpunkt in Saarbrücken
- BSI veröffentlicht „IT-Sicherheitsleitfaden für Kandidierende bei Bundes- und Landeswahlen“

Juli 21

- Ransomware-Angriff mit weltweiten Auswirkungen
- Katastrophenfall nach Ransomware-Angriff auf Kreisverwaltung
- Aktualisierung der Mindeststandards „Schnittstellenkontrolle“ und „Nutzung externer Cloud-Dienste“
- Kampagne #einfachaBSIchern beleuchtet Schwerpunktthema sicheres Online-Shopping

August 21

- BMBF und BSI kommunizieren erstmals über quantengesicherte Videokonferenz

September 21

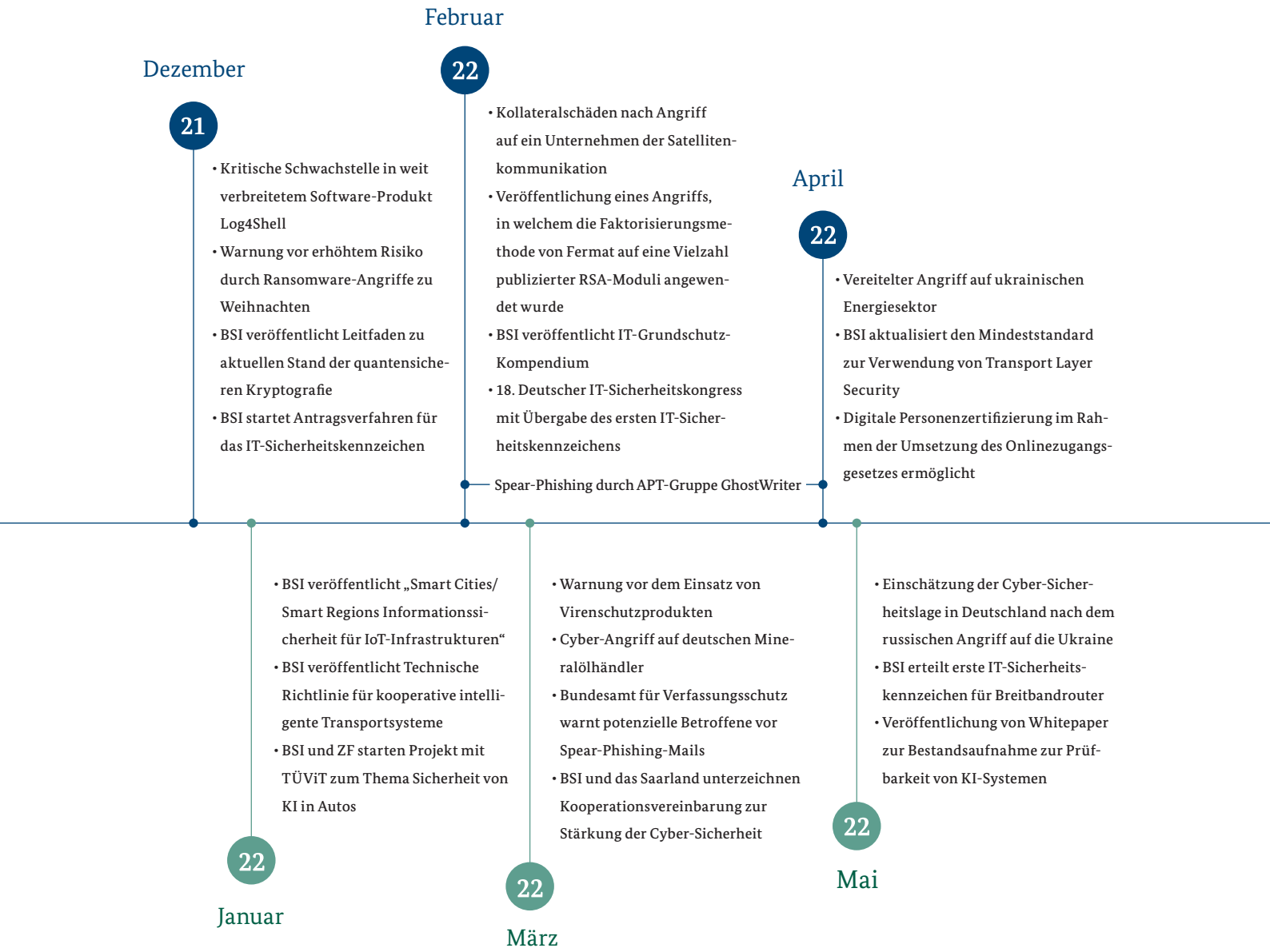
- Ransomware-Angriff auf Medizintechnologie-Unternehmen mit mehreren Standorten in Deutschland
- Veröffentlichung einer Schwachstelle betreffend die Erzeugung identischer RSA-Schlüssel durch die Javascript-Bibliothek Keypair
- Veröffentlichung des europäischen Standards der Testspezifikation für Sicherheit im Smart Home
- BSI unterzeichnet Verwaltungsvereinbarung für mehr Cyber-Sicherheit in der Schifffahrt

Oktober 21

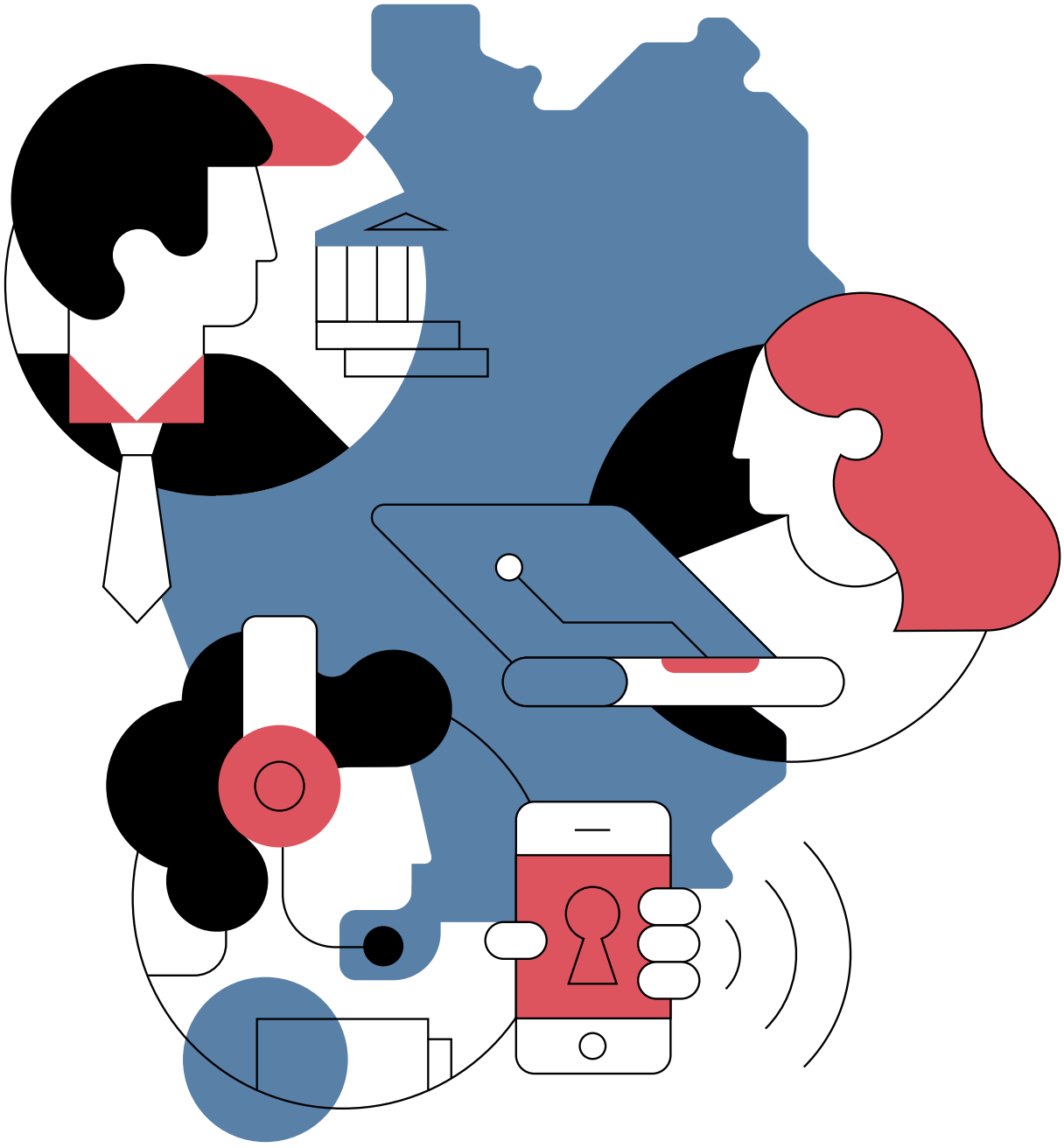
- „Smishing“ mit neuer Betrugsmasche
- Das Nationale Koordinierungszentrum für Cybersicherheit nimmt Arbeit auf
- BSI startet neues, beschleunigtes Zertifizierungsprogramm
- BSI veröffentlicht Mindeststandard für Videokonferenzdienste

November 21

- Ransomeware-Angriff aus Handelsunternehmen im Bereich der Unterhaltungselektronik
- Emotet-Botnetze wieder aktiv, Cyber-Sicherheitswarnung durch BSI veröffentlicht
- Warnung vor *DDoS-Angriffe* zum Black Friday
- Unterzeichnung der bundesweit ersten Kooperationsvereinbarung zwischen BSI und Niedersachsen


Dezember
21
• Kritische Schwachstelle in weit verbreitetem Software-Produkt Log4Shell
• Warnung vor erhöhtem Risiko durch Ransomware-Angriffe zu Weihnachten
• BSI veröffentlicht Leitfaden zu aktuellen Stand der quantensicheren Kryptografie
• BSI startet Antragsverfahren für das IT-Sicherheitskennzeichen
Januar
22
• BSI veröffentlicht „Smart Cities/ Smart Regions Informationssicherheit für IoT-Infrastrukturen“
• BSI veröffentlicht Technische Richtlinie für kooperative intelligente Transportsysteme
• BSI und ZF starten Projekt mit TÜViT zum Thema Sicherheit von KI in Autos
Februar
22
• Kollateralschäden nach Angriff auf ein Unternehmen der Satellitenkommunikation
• Veröffentlichung eines Angriffs, in welchem die Faktorisierungsmethode von Fermat auf eine Vielzahl publizierter RSA-Moduli angewendet wurde
• BSI veröffentlicht IT-Grundschutz-Kompendium
• 18. Deutscher IT-Sicherheitskongress mit Übergabe des ersten IT-Sicherheitskennzeichens
Spear-Phishing durch APT-Gruppe GhostWriter
März
22
• Warnung vor dem Einsatz von Virenschutzprodukten
• Cyber-Angriff auf deutschen Mineralölhändler
• Bundesamt für Verfassungsschutz warnt potenzielle Betroffene vor Spear-Phishing-Mails
• BSI und das Saarland unterzeichnen Kooperationsvereinbarung zur Stärkung der Cyber-Sicherheit
April
22
• Vereitelter Angriff auf ukrainischen Energiesektor
• BSI aktualisiert den Mindeststandard zur Verwendung von Transport Layer Security
• Digitale Personenzertifizierung im Rahmen der Umsetzung des Onlinezugangsgesetzes ermöglicht
Mai
22
• Einschätzung der Cyber-Sicherheitslage in Deutschland nach dem russischen Angriff auf die Ukraine
• BSI erteilt erste IT-Sicherheitskennzeichen für Breitbandrouter
• Veröffentlichung von Whitepaper zur Bestandsaufnahme zur Prüfbarkeit von KI-Systemen

Erkenntnisse & Maßnahmen



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, der Wirtschaft sowie mit Staat und Verwaltung und internationalen Gremien. Mit Inkrafttreten des IT-Sicherheitsgesetzes 2.0 wurde der Auftrag des BSI 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

Die Digitalisierung spielt heutzutage in eine Vielzahl von Bereichen unserer Gesellschaft mit hinein – von der Nutzung verschiedenster Online-Dienste über das Gesundheitswesen bis hin zu Abstimmungen und Wahlen. Informationssicherheit ist für all das eine notwendige Voraussetzung. Das BSI arbeitet kontinuierlich daran, die Informationssicherheit in allen Bereichen unseres Lebens zu verbessern, damit die Bürgerinnen und Bürger ihre persönlichen Daten gut aufgehoben sehen, IT sicher anwenden und sich vertrauensvoll in der vernetzten Welt bewegen können. Dafür bündelt das BSI sein umfangreiches Know-how in den Bereichen Prävention, Detektion und Reaktion und leitet daraus konkrete Informationsangebote für gesellschaftliche Gruppen, aber auch für die einzelnen Bürgerinnen und Bürger ab. Im Berichtszeitraum hat sich das BSI dafür unter anderem mit Fragen rund um die Sicherheit vernetzter medizinischer Produkte, elektronischer Identitätsverfahren und den Möglichkeiten virtueller Versammlungen und Abstimmungen auseinandergesetzt.

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 und seit 2019 jährlich durchgeführte Online-Befragung. Es 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.

Kriminalität im Internet leicht gestiegen – mehr als jeder Vierte ist Opfer

Die generelle Betroffenheit von Verbraucherinnen und Verbrauchern ist im Vergleich zu den vergangenen drei Jahren zuletzt leicht angestiegen: 29 Prozent der Befragten gaben an, bereits Opfer von Kriminalität im Internet gewesen zu sein. In den vergangenen Jahren waren es noch 25 Prozent. Dabei ist jeweils einem Viertel der Befragten vor allem Betrug beim Onlineshopping (25 %), ein Fremdzugriff auf ein Online-Konto (25 %) und/oder eine Infektion mit Schadsoftware (24 %) widerfahren. Im Gegensatz zum Betrug beim Onlineshopping (2021: 19 %) sind die Zahlen zur Betroffenheit vom Fremdzugriff auf ein Online-Konto (2021: 31 %) oder einer Infektion mit Schadsoftware (2021: 29 %) im Vergleich zum Vorjahr rückläufig. Von *Phishing* waren nur noch 19 Prozent der Befragten betroffen – im Vorjahr galt das noch für ein Viertel (25 %).

Die Anwendung von Schutzmaßnahmen durch Verbraucherinnen und Verbraucher bleibt weiterhin ausbaufähig. Die Nutzung von Antivirenprogrammen (53 %), sicheren Passwörtern (52 %) und einer aktuellen Firewall (44 %) ist in der Bevölkerung verbreitet. Lediglich ein Drittel (34 %) der Befragten gab an, automatische Updates zu nutzen. Die Aktivierung einer 2FA nutzten nur 38 Prozent der Befragten.

Umgang mit Sicherheitsempfehlungen

Zwei von fünf Befragten kennen Sicherheitsempfehlungen zum Schutz vor Kriminalität im Internet (45 %). Von diesen gab wiederum über die Hälfte (58 %) an, diese Empfehlungen zum Teil umzusetzen. 22 Prozent setzen sie vollständig um, nur vier Prozent gar nicht. Über die Hälfte der Befragten (51 %) informiert sich über Internetsicherheit, gut ein Fünftel (23 %) nie. Besonders wichtig ist den Befragten die Sicherheit beim Onlinebanking (83 %), beim Installieren von Software (70 %) und beim Onlineshopping (62 %).

Wunsch nach Orientierung für den Notfall

Die Opfer von Kriminalität im Internet gaben meist an, sich selbst geholfen zu haben. Das entspricht ihrem Bedarf nach Informationen: Die meisten wünschen sich eine Checkliste für den Notfall als Hilfestellung, gefolgt von einer Webseite mit Erklärvideos und einem Berater oder einer Beraterin bei der Polizei. Insgesamt wünschte sich über die Hälfte mehr Informationen zu Themen rund um Sicherheit im Internet, insbesondere Hinweise, wie sich Kriminalität im Internet erkennen lässt, und Informationen, wie sich Online-Konten schützen lassen.

2.1.2 — Digitaler Verbraucherschutz

Phishing und Leaks sind nur zwei Begriffe, die im Verbraucheralltag leider eine große Rolle spielen (vgl. Kapitel *Spam und Phishing*, Seite 26, und Abschnitt *Erpressung mit erbeuteten Identitätsdaten*, Seite 17). Das BSI empfiehlt Verbraucherinnen und Verbrauchern daher Online-Dienste mittels 2FA zu sichern. Es liegt in der Verantwortung der Anbieter von Online-Diensten, sichere und leicht nutzbare 2FA- und Wiederherstellungsverfahren anzubieten[25]. Einer Marktuntersuchung des Verbraucherzentrale Bundesverbands (vzbv) zufolge kommen nur wenige Anbieter dieser Verantwortung nach. Gestützt durch eine Verbraucherbefragung des vzbv ist zudem festzustellen, dass Verbraucherinnen und Verbraucher wenig Kenntnis zu Stärken und Schwächen einzelner 2FA-Verfahren und deren sicherer Verwendung haben.

Das BSI hat für den Digitalen Verbraucherschutz eine Gegenüberstellung gängiger 2FA-Verfahren samt Bewertungstabellen erstellt, die versierten und technisch affinen Verbraucherinnen und Verbrauchern bestimmte Verfahrenseigenschaften darlegen. Betrachtet wurden Aspekte der IT-Sicherheit, der Usable Security (einfach nutzbare IT-Sicherheit) sowie der Vertraulichkeit der Daten. Bei der Bewertung der IT-Sicherheit wurden – eine sichere Nutzungsumgebung vorausgesetzt – Angriffsszenarien betrachtet, die eine Gefahr darstellen können. Diese bezogen sich auf Phishing-Angriffe, Leaks und Angriffe aus der Ferne auf den zweiten Faktor. Festgestellt wurde, dass die hardwarebasierten Verfahren Chip-TAN und Personalausweis resistent gegen diese Angriffsszenarien sind. Zukünftig wird die Identifikation über das Smart-eID-Verfahren möglich sein und damit im Vergleich zur betrachteten Nutzung des Personalausweises zusätzliche Vorteile bei der Usable Security mit sich bringen.

Weiterführende Informationen finden Sie hier:[d]

Corporate Digital Responsibility – Verantwortung übernehmen für mehr Sicherheit

Worum sorgen sich Verbraucherinnen und Verbraucher beim Onlineshopping am meisten? Datendiebstahl und finanzielle Schäden durch Betrug sind laut einer repräsentativen Befragung des Bundesministeriums der Justiz (BMJ) die Top-Antworten. Anbieter werden in der Verantwortung gesehen, für Datenschutz und Cyber-Sicherheit zu sorgen. Der überwiegenden Mehrheit der Befragten zufolge werden Unternehmen dieser Forderung aktuell jedoch nicht gerecht[26]. Die Corporate Digital Responsibility (CDR) soll daher einen Orientierungs- und Anforderungsrahmen für einen verantwortungsvollen Einsatz digitaler Technologien schaffen.

In Anlehnung an Corporate Social Responsibility (CSR) basiert das 2015 erstmals beschriebene Konzept auf einem freiwilligen und ganzheitlichen Ansatz. Ein Von-Anfang-an-Mitdenken stellt den Aufbau und Erhalt von Vertrauen in den Mittelpunkt[27]. Das bedeutet auch, dass sich Maßnahmen direkt positiv auf Produkte und Dienstleistungen für Verbraucherinnen und Verbraucher auswirken können. Der Bekanntheitsgrad von CDR ist noch gering, die Anzahl der aktiven Akteure überschaubar. Referenzrahmen, Handlungsfelder und Maßnahmen befinden sich aktuell in einer umfassenden Diskussion. Mit dem CDR-Kodex wurde erstmals ein übergreifender Ansatz gemeinsam mit Unternehmen entwickelt. Inhaltlich wird sich unter anderem zur konsequenten Weiterentwicklung der Informations-

sicherheit und deren Berücksichtigung bereits bei der Produktentwicklung verpflichtet[28]. Für Unternehmen bietet sich damit eine Chance, Informationssicherheit positiv als Mehrwert und Wettbewerbsvorteil umzusetzen und zu kommunizieren. Im Handlungsfeld Informationssicherheit unterstützt das BSI mit seinen zahlreichen Angeboten das gemeinsame Ziel, ein höheres Sicherheitsniveau für Verbraucherinnen und Verbraucher zu erreichen.

2.1.3 — IT-Sicherheitskennzeichen

Im Dezember 2021 hat das BSI das Verfahren zur Erteilung des IT-Sicherheitskennzeichens eröffnet und damit eine wichtige neue Aufgabe aus dem novellierten BSI-Gesetz (BSIG) erfolgreich umgesetzt. Seitdem sind beim BSI bereits Anträge für eine Vielzahl von Produkten und Diensten aus den Bereichen Breitbandrouter und E-Mail-Services eingegangen.

Am 1. Februar 2022 wurden die ersten vier IT-Sicherheitskennzeichen erteilt und auf dem 18. Deutschen IT-Sicherheitskongress durch BSI-Präsident Arne Schönbohm an einen E-Mail-Provider übergeben.

Um das Bewusstsein für den Mehrwert des neuen IT-Sicherheitskennzeichens zu erhöhen, führt das BSI den kontinuierlichen Dialog mit Stakeholdern aus dem Bereich Verbraucherschutz und Wirtschaft. Ein umfangreiches Informationsangebot auf der Webseite des BSI erklärt Verbraucherinnen und Verbrauchern sowie interessierten Unternehmen die Funktionsweise des IT-Sicherheitskennzeichens und gibt einen umfassenden Überblick zum Thema.

Abbildung 20: BSI-Präsident Arne Schönbohm und Fabian Bock, Geschäftsführer der mail.de GmbH, bei der Übergabe des ersten IT-Sicherheitskennzeichens. Quelle: BSI

Das BSI arbeitet daran, den Geltungsbereich des IT-Sicherheitskennzeichens zu erweitern, indem es fortlaufend neue Produktkategorien entwickelt und veröffentlicht, zum Beispiel Produkte aus dem Bereich Consumer-IoT. Grundlage für diese neuen Produktkategorien soll die europäische Norm ETSI EN 303 645 sein, die grundlegende Regelungen zur Sicherheit von Consumer-IoT beinhaltet.

Mit dem neuen Kennzeichen macht das BSI die Sicherheit von Produkten und Diensten auf dem Deutschen Verbrauchermarkt transparenter. Hersteller und Dienstanbieter können das Versprechen in die Sicherheit ihrer Produkte besonders auszeichnen und gegenüber den Kundinnen und Kunden leicht erkennbar machen.

Weiterführende Informationen finden Sie hier:[e]

2.1.4 — Information und Sensibilisierung von Verbraucherinnen und Verbrauchern

Das BSI verfolgt beim Digitalen Verbraucherschutz unter anderem das Ziel, das Risikobewusstsein von Verbraucherinnen und Verbrauchern zu erhöhen. Es soll deutlich werden, was im Falle eines Cyber-Vorfalls auf dem Spiel steht. Darüber hinaus will das BSI die Lösungskompetenz von Verbraucherinnen und Verbrauchern steigern und ihnen vermitteln, wie sie auf einen IT-Notfall reagieren können. Deswegen informiert das BSI regelmäßig zu aktuellen Entwicklungen, gibt Empfehlungen, wie ein digitaler Basisschutz aussieht, und weist auf Gefahren und gängige Angriffsmethoden hin. Durch diese Angebote will das BSI Verbraucherinnen und Verbraucher dabei unterstützen, sich sicher und selbstbestimmt im Netz zu bewegen.

Webseite als zentraler Anlaufpunkt

Auf den BSI-Webseiten finden Interessierte konkrete Handlungsempfehlungen zu Fragen des digitalen Alltags und Hintergrundinformationen aus dem Bereich Cyber-Sicherheit.

Zudem sprach das BSI im Berichtszeitraum gezielt neue Zielgruppen an: beispielsweise die Gaming-Com-

munity mit einer umfangreichen virtuellen Präsenz bei der Gamescom im August 2021. Eine andere Zielgruppe erreichte das BSI zum Deutschen Seniorentag im November 2021. In vier virtuellen Vorträgen erfuhren hunderte Privatanwenderinnen und -anwender sowie Ehrenamtliche, wie sie sicher durch den digitalen Alltag kommen.

Wachsende Community

Das BSI gewann auf seinen Social-Media-Kanälen, die sich vor allen an Verbraucherinnen und Verbraucher richten, viele neue Abonnentinnen und Abonnenten. Besonders beliebt sind Erklärungen rund um Technik- und Internetphänomene sowie Warnungen zu aktuellen Sicherheitsvorfällen. Auch Storytelling-Formate sorgten für eine erhöhte Aufmerksamkeit. Zudem erhielt der Newsletter „Sicher • Informiert“ Zuwachs und hält inzwischen über 121.000 Abonnentinnen und Abonnenten auf dem Laufenden zu aktuellen Entwicklungen der digitalen Welt. Nicht zuletzt gehört der Podcast „Update verfügbar“ nach über einem Jahr zu den Top 10-Prozent der am häufigsten gestreamten Podcasts auf dem deutschen Markt. Die monatlich aktive Community beläuft sich auf 4.500 bis 7.000 Hörerinnen und Hörer bei mehr als 3.000 Abonnements.

Onlineshopping im Fokus der Kampagne #einfachabsichern

Onlineshopping ist zu einem festen Bestandteil des Einkaufsverhaltens im privaten Alltag geworden. Deshalb wurde der Fokus der Informations- und Sensibilisierungskampagne zur IT-Sicherheit vom BSI und dem Bundesministerium des Innern und für Heimat (BMI) zwischen Juli und Anfang September 2021 auf den sicheren Online-Einkauf im Netz gelegt. Interessierte erhielten Tipps und Informationen zu drei zentralen Aspekten: sichere Onlineshops, sichere Nutzerkonten und sicheres Bezahlen. Die Hinweise wurden zudem Ende des Jahres noch einmal während der Cyber Week und des Weihnachtsgeschäfts gezielt bekannt gemacht.

Weiterführende Informationen finden Sie hier:[f]

2.1.5 — Projekt „Dialog für Cyber-Sicherheit"

Das BSI verfolgt das Ziel, Cyber-Sicherheit für, mit und in der gesamten Gesellschaft zu gestalten. Dazu führt es seit Frühjahr 2021 im Projekt „Dialog für Cyber-Sicherheit“ den gesamtgesellschaftlichen Austausch im Bereich Cyber-Sicherheit auf der Grundlage eines partizipativ ausgerichteten Multi-Stakeholder-Ansatzes mit allen gesellschaftlichen Gruppen fort. In einem Pilotprozess wird ein Dialogmodell umgesetzt, das im Vorgängerprojekt „Institutionalisierung des Gesellschaftlichen Dialogs“[26] von den Dialogteilnehmerinnen und -teilnehmern entwickelt wurde.

Mit dem Dialog möchte sich das BSI im Sinne eines Open-Government-Ansatzes öffnen, Vertrauen aufbauen, die bidirektionale Kommunikation ausbauen, Partizipation ermöglichen und eine Plattform für einen dauerhaften Dialog zur Cyber-Sicherheit mit allen gesellschaftlichen Gruppen schaffen.

Im Anschluss an die Denkwerkstatt 2021, auf der die Dialogpartnerinnen und -partner ein Dialogkomitee und Themen für die weitere Arbeit gewählt haben, startete im Juli 2021 die gemeinsame Arbeit in fünf Arbeitsgruppen (Workstreams). Vier davon wurden bis März 2022 umgesetzt, einer konnte nicht zu Ende geführt werden. Zu folgenden Themen sind Produkte entstanden, die auf der Projekt-Website abrufbar sind:

1. **Digitales Mindesthaltbarkeitsdatum**
2. **Dos and Don'ts für nachhaltig sichere Produkte**
3. **Effektive IT-Security Awareness**
4. **Update4Schule – Datenerhebung zur digitalen Bildung**

Mit der Präsentation der Workstream-Ergebnisse endete der erste Projektzyklus. Das Dialogprojekt läuft noch bis Ende 2024.

Weiterführende Informationen finden Sie hier:[g]

2.1.6 — Sicherheit im Internet der Dinge, im Smart Home und in Smart Cities

Vernetzte Geräte im *Internet der Dinge* bieten eine breite Angriffsfläche für Cyber-Angriffe. Insbesondere die Kaperung solcher Systeme mit Hilfe von Schadsoftware und die Integration in Botnetze birgt Schadenspotenzial. Denn gekaperte vernetzte Geräte können zum Werkzeug für weitere Angriffe werden – gegen die betroffenen Verbraucherinnen und Verbraucher einerseits, aber auch gegen dritte Ziele, wenn Angreifer die Rechenkapazität zum Beispiel für DDoS-Angriffe nutzen (vgl. Kapitel *Botnetze*, Seite 24).

Die europäische Norm ETSI EN 303 645 definiert Basisanforderungen an die IT-Sicherheit von vernetzten Geräten für Verbraucherinnen und Verbraucher zum Beispiel im Smart Home. Darunter fallen beispielsweise sichere Mechanismen (z. B. Passwörter), die das Produkt vor einem Zugriff unberechtigter Personen schützen. Im August 2021 wurde die zugehörige Prüfspezifikation ETSI TS 103 701 veröffentlicht, die unter maßgeblicher Beteiligung des BSI entstanden ist. Ihre Anwendung ermöglicht es, zu prüfen, ob ein vernetztes Gerät die Anforderungen der europäischen Norm erfüllt. Beide Dokumente bilden seit Mai 2022 die zugrundeliegenden Standards für die Erteilung des IT-Sicherheitskennzeichens an verschiedenste Produktkategorien, wie zum Beispiel smarte Kameras oder Lautsprecher.

Mit den Technischen Richtlinien für E-Mail-Dienste (BSI TR-03108) und Breitband-Router (BSI TR-03148) konnte zur Einführung des IT-Sicherheitskennzeichens im Dezember 2021 für die ersten beiden Produktkategorien auf bereits existierende Standards des BSI zurückgegriffen werden. Die Nachfrage von Herstellern und Dienstanbietern ist groß, es konnten bereits eine Reihe von IT-Sicherheitskennzeichen erteilt werden.

Nicht zuletzt durch die Auswahl von 28 weiteren „Modellprojekte Smart Cities“ im Rahmen der dritten Staffel des entsprechenden Förderprogramms vom BMI nimmt die Digitalisierung von Regionen, Kreisen, Städten und Gemeinden auch im Kontext der öffentlichen Daseinsvorsorge weiter an Fahrt auf. Damit sind nun insgesamt 73 Projekte seit 2019 in der Förderung. Das BSI hat hierzu zielgruppenorientierte Handlungsempfehlungen veröffentlicht.

Weiterführende Informationen finden Sie hier:[h]

2.1.7 — Sicherheit im Gesundheitswesen

Digitale Gesundheitsfürsorge kann das Leben der Menschen erleichtern, lange Wege und Wartezeiten minimieren und im Krankheits- oder Notfall schnell helfen. Doch alle Vorteile von eHealth sind ohne Informationssicherheit nicht denkbar. Denn die Digitalisierung erhöht auch im Gesundheitswesen das Risiko von IT-Sicherheitsvorfällen und Cyber-Angriffen (vgl. zum Beispiel den Vorfall *Ransomware-Angriff auf Medizintechnologie-Unternehmen*, Seite 23).

Sicherheit von Medizinprodukten

Seit dem vergangenen Berichtszeitraum gab es zwei Ereignisse, die besonderen Einfluss auf die IT-Sicherheit von vernetzten Medizinprodukten hatten: Die im August 2021 veröffentlichte Sammlung kritischer Schwachstellen „BadAlloc“ stellt durch den Einsatz des Echtzeitbetriebssystems Blackberry QNX auch eine Bedrohung für viele Komponenten im medizinischen Bereich dar und kann je nach Einsatz die Ausführung von fremdem Code erlauben. Darüber hinaus wurden im März 2022 die Schwachstellen „Access:7“ in Fernverwaltungsprodukten der Marke Axeda bekannt. Diese Produkte werden insbesondere zur Fernwartung vernetzter medizinischer Systeme in Krankenhäusern und Laboren eingesetzt und können Unbefugten einen Zugriff ermöglichen. Durch die veröffentlichten Patches und Maßnahmen für beide Schwachstellensammlungen lässt sich die Sicherheit im medizinischen Bereich weiterhin gewährleisten, Beeinträchtigungen der Patientensicherheit sind nach dem aktuellen Stand nicht bekannt.

Sicherheit der Telematikinfrastruktur

Im Berichtszeitraum hat die Digitalisierung im Gesundheitswesen, auch im Bereich der Telematikinfrastruktur (TI) erneut deutlich zugenommen. Nach Einführung der ersten Fachanwendungen zum Notfalldatenmanagement (NFDM), des eMedikationsplans im Rahmen der Arzneimitteltherapiesicherheit (AMTS) und der elektronischen Patientenakte (ePA), die es allen gesetzlich Versicherten erlaubt, ihre medizinischen

Befunde und Informationen aus vorhergehenden Untersuchungen zentral und sicher zu hinterlegen und im Bedarfsfall auch über Praxis- und Krankenhausgrenzen hinweg weiteren behandelnden Ärztinnen und Ärzten zur Verfügung zu stellen, wurden weitere Ausbaustufen der TI hinsichtlich ihrer Spezifikation konkretisiert und getestet. Sie stehen nun vor der direkten Umsetzung. Ein Beispiel hierfür ist das eRezept, das seit Ende 2021 unter Koordination der Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) in einer Testphase erprobt wird und einen Meilenstein in der Digitalisierung des Gesundheitswesens darstellt.

Gerade unter den momentanen Covid-19-Pandemiebedingungen wurde das Gesundheitssystem stark gefordert. Im Vorfeld geplante Tests zur funktionalen Erweiterung der TI liefen aufgrund der nun zum Teil verknappten oder anderweitig gebundenen personellen Ressourcen unter erschwerten Voraussetzungen.

Digitale Pandemiebekämpfung

Seit Beginn der Arbeiten an der Corona-Warn-App führt das BSI, ergänzend zum Entwicklungsprozess, Sicherheitsanalysen durch. Das BSI unterstützt die Weiterentwicklung der App durch siebentägige Penetrationstests und Code-Reviews in einem zweiwöchigen Rhythmus. Die Entwicklung der Corona-Warn-App findet transparent in einem öffentlich zugänglichen Quellcode-Verwaltungssystem (GitHub) statt. Dort meldet das BSI die identifizierten Schwachstellen an die Entwicklerinnen und Entwickler (vgl. auch das Kapitel *Schwachstellen in Software-Produkten*, Seite 32). Seit der Veröffentlichung der Corona-Warn-App wurden in enger Zusammenarbeit zwischen BSI, Robert-Koch-Institut (RKI), Deutscher Telekom AG und SAP diverse Erweiterungen entwickelt.

Im Jahr 2021 wurde die Corona-Warn-App unter anderem um die Funktion einer Event-Registrierung und die Anbindung an das digitale COVID-Zertifikat sowie Corona-Testzentren erweitert. Durch die IT-Sicherheitsanalysen des BSI im Rahmen der Erweiterungen wurden seit Juni 2021 insgesamt neun Schwachstellen in der Corona-Warn-App identifiziert. Diese ließen sich im Rahmen der engen Zusammenarbeit zwischen BSI und Konsortium beheben. Unter anderem ließ sich im Rahmen der Tests nachweisen, dass das Konsortium auf die als „Log4Shell“ bekannte Schwachstelle schnell und angemessen reagiert hat, sodass die Corona-Warn-App für diese Schwachstelle nicht anfällig ist.

Digitaler Impfnachweis

Seit Beginn der Entwicklung des digitalen Impfnachweises unterstützt das BSI das Bundesministerium für Gesundheit (BMG) sowie das RKI sowohl in der Bewertung von Sicherheitskonzepten als auch durch Penetrationstests und Code-Reviews. Jegliche Weiterentwicklungen der Apps und der Hintergrundsysteme wurden durch das BSI begleitet. Technische Schwachstellen ließen sich so zeitnah an die Entwicklerinnen und Entwickler kommunizieren. Durch diese Kooperation konnte ein Gesamtsystem bestehend aus Hintergrundsystemen, der Cov-Pass-App und der Cov-Pass-Check-App geschaffen werden, das seit seiner Veröffentlichung ein hohes Niveau von IT-Sicherheit vorweisen kann. Insgesamt ließen sich so seit dem Beginn der Entwicklung der App ungefähr 40 Schwachstellen identifizieren und beheben.

2.1.8 — Sichere Gestaltung virtueller Versammlungen und Abstimmungen

Im Berichtszeitraum waren viele Unternehmen und öffentliche Einrichtungen weiterhin gezwungen, ihren Mitarbeitenden die Arbeit von zu Hause zu ermöglichen und mussten Geschäftsprozesse daher weiter digitalisieren. Daraus ergibt sich ein verstärkter Bedarf für die Digitalisierung von Verwaltungsprozessen, wie Wahlen von Betriebsräten, Gleichstellungsbeauftragten oder Vorständen. Viele Unternehmen steigen daher aktuell mit neuen Produkten in den Markt für Online-Wahlen ein. Das BSI erstellt im Projekt „Markt- und Schwachstellenanalyse von Online-Wahlprodukten“ eine umfassende Markt- und Sicherheitsanalyse von einer Auswahl aktuell verfügbarer Produkte. Das Ziel dieser Analyse ist die Erstellung eines detaillierten Lagebilds über den Stand der IT-Sicherheit in diesem Bereich. Die Ergebnisse werden in die Technischen Richtlinien und Schutzprofile für nicht-politische Wahlen und Abstimmungen einfließen.

Das Thema Online-Wahlen fand 2022 auch den Weg in den Bundestag. Am 6. April fand im Ausschuss für Bildung, Forschung und Technikfolgenabschätzung (ABFT) ein öffentliches Fachgespräch zum Thema „E-Voting“ statt. Das Büro für Technikfolgenabschätzung führt aktuell zu diesem Thema eine Kurzstudie durch; die Zwischenergebnisse wurden im Fach-

gespräch in Form eines Thesenpapiers vorgetragen und mit Sachverständigen, unter anderem aus dem BSI, diskutiert. Zu den Leitfragen gehörten: „Inwiefern erfüllt E-Voting die Wahlrechtsgrundsätze?“ und „Können Online-Wahlen sicher umgesetzt werden?“ Zudem wurde über die Frage diskutiert: „Sollte E-Voting bei Bundestagswahlen in Deutschland eingesetzt werden?“ Der Konsens unter den Expertinnen und Experten lautete: „Das E-Voting wird in den nächsten Jahren keine Option bei Bundestags- oder Landtagswahlen werden.“ Die Sachverständigen sprachen sich übereinstimmend dafür aus, die Möglichkeit der Online-Stimmabgabe vorerst bei Wahlen zu Selbstverwaltungskörperschaften – Sozialwahlen oder Gremienwahlen – zu testen und daraus gewonnene Erkenntnisse mit einem interdisziplinären Ansatz wissenschaftlich auszuwerten.

Weiterführende Informationen finden Sie hier:[i]

2.1.9 — Sicherheit von Bezahlverfahren

Beim smsTAN-Verfahren (auch mTAN genannt) sendet die Bank der Kundin oder dem Kunden eine Transaktionsnummer (TAN) per SMS an die im Bankingportal hinterlegte Mobilfunknummer. Diese TAN wird zur Freigabe der durch die Kundin oder den Kunden initiierten Transaktion, beispielsweise der Freigabe einer Überweisung, benötigt. Die SMS enthält neben der TAN Details zu der durchzuführenden Transaktion, wie zum Beispiel Empfängerin oder Empfänger und Betrag einer Überweisung, sodass hier eine Überprüfung stattfinden kann.

Das Problem: SMS werden unverschlüsselt übermittelt, sodass sich Daten abfangen lassen. Außerdem ist das Bankkonto nicht an ein konkretes Gerät der Nutzerin oder des Nutzers gebunden, sondern in der Regel nur mit einer Mobilfunknummer verknüpft. So besteht die Gefahr des sogenannten *SIM-Swappings*. Hier wird im Namen der Nutzerin oder des Nutzers eine weitere SIM-Karte zur Mobilrufnummer bestellt, sodass mTANs an mehrere Geräte gesendet werden. Gleichermaßen besteht bei Diebstahl oder Verlust des mobilen Gerätes die Gefahr des Missbrauchs, wenn Kriminelle im Besitz der Login-Daten zum Onlinebanking sind. Allein durch Missbrauch des smsTAN-Verfahrens ist in der Vergangenheit jährlich ein Schaden von mehreren Millionen Euro entstanden.

Das BSI weist schon lange auf dieses Problem hin, so dass mittlerweile immer mehr Banken vom mTAN-Verfahren Abstand genommen haben. Durch die Verbreitung von Smartphones setzen die Kreditinstitute PushTAN oder PhotoTAN ein. Durch kryptografische Verfahren wird zunächst eine Gerätebindung zwischen dem Smartphone und dem Onlinebanking-Zugriff der Kundin oder des Kunden erzeugt. Sobald das Smartphone eindeutig an das Bankkonto gebunden ist, wird die TAN nur an das registrierte Gerät gesendet. Die Übermittlung der TAN erfolgt durch eine Push-Nachricht aufs Smartphone oder das Auslesen eines 2D-Barcodes mit der Smartphone-Kamera. Für das ChipTAN-Verfahren wird die eigene Bankkarte zusammen mit einem separaten TAN-Generator verwendet, der nicht mit dem Internet verbunden ist. Aus den Transaktionsdaten wird ein graphischer Code erstellt, der mit dem ChipTAN-Generator ausgelesen wird. Das macht dieses Verfahren besonders sicher, da auf der Karte gespeicherte Merkmale für die Erzeugung der TAN erforderlich sind.

Aktuelle Umfragen lassen erahnen, dass die Schadensentwicklung durch TAN-Betrug auf Basis des Einsatzes der neuen Verfahren abnimmt.

Weiterführende Informationen finden Sie hier:[j]

2.1.10 — Zwei-Faktor-Authentisierung

Mittlerweile bieten viele Online-Dienstleister Verfahren an, mit denen sich Nutzerinnen oder Nutzer zusätzlich bzw. alternativ zur Passworteingabe identifizieren können, wenn sie sich in ein Konto einloggen. Diese sogenannte Zwei-Faktor-*Authentifizierung* oder kurz 2FA gibt es in zahlreichen Varianten. Dabei bieten vor allem hardwaregestützte Verfahren ein hohes Maß an Sicherheit.

Der übliche Weg zur *Authentisierung* basiert nach wie vor auf der Eingabe eines Passworts. Ein einzelner Faktor – das „Wissen“ des Passworts – wird vom Dienst abgefragt, um die Nutzerin oder den Nutzer zu authentifizieren. Passwörter als Authentisierungsmechanismus sind

einfach umzusetzen, haben aber mehrere Nachteile: Zum Beispiel reicht die Kenntnis des einen Faktors „Wissen“, um den Authentisierungsmechanismus zu überwinden.

Mehr und mehr Dienste fragen daher neben dem Passwort einen zweiten Faktor ab, um die Nutzerin oder den Nutzer sicherer zu authentifizieren, zum Beispiel mit einer weiteren Abfrage von „Wissen“ in Form eines Authentisierungscodes, der auf das Smartphone gesendet wird, um zum Beispiel Identitätsdiebstahl entgegenzuwirken. Eine höhere Sicherheit ist hier aber nur dann gegeben, wenn eine echte Trennung der Geräte stattfindet und sich die Faktoren damit nicht durch einen Angriff gesammelt gewinnen lassen. Das BSI hat zur Orientierung die Technische Richtlinie TR-03168 Authentisierungsverfahren und -systeme erarbeitet, um einen genaueren Überblick und Empfehlungen zur sinnvollen Kombination von verschiedenen Faktoren zu geben. Eine Betrachtung verschiedener Faktoren aus Verbrauchersicht wurde im Rahmen einer Bewertungstabelle dargestellt (vgl. Kapitel *Digitaler Verbraucherschutz*, S. 58).

Eine Möglichkeit, mehrere Faktoren darzustellen, folgt den Standards der 2013 mit vielen verschiedenen Vertretern aus Staat und Industrie gegründeten Fast-IDentity-Online-Allianz, um offene und lizenzfreie Industriestandards für die weltweite *Authentisierung* im Internet zu entwickeln. Ein Nachweis über die Sicherheit des verwendeten FIDO-Authentikators ist notwendig, um eine sichere Umsetzung der Protokolle in Produkten zu gewährleisten. Als Mitglied der FIDO-Allianz ist das BSI an der Definition nachweisbar sicherer Authentikatoren beteiligt.

Das BSI hat zwei handelsübliche, nicht extern zertifizierte FIDO-Token mit der Fragestellung untersucht, ob diese ein „substantielles“ Vertrauensniveau nach BSI TR-03107-1 erfüllen. Exemplarisch wurden Angriffsszenarien betrachtet, bei denen die Angreifer für eine begrenzte Zeit physischen Zugriff auf einen FIDO-Token hatten. Hier fanden sich bei beiden Token relevante Manipulationsmöglichkeiten, womit sie sich als ungeeignet für das Vertrauensniveau „substantiell“ erwiesen haben.

Weiterführende Informationen finden Sie hier:[k]

2.1.11 — Bewertung von elektronischen Identifizierungsverfahren

Das BSI untersucht bei elektronischen Identifizierungsverfahren sowohl grundlegende Technologien als auch konkrete Verfahren, um für Staat, Wirtschaft und Gesellschaft die Risiken zu bewerten und zu minimieren.

Konkrete privatwirtschaftliche Verfahren bewertet das BSI im Kontext des Onlinezugangsgesetzes. Diese technischen Bewertungen bilden die Grundlage für das BMI, um innerhalb des IT-Planungsrats über die Nutzung des jeweiligen Verfahrens im E-Government, speziell für Nutzerkonten von Bund und Ländern, zu entscheiden. Im Berichtszeitraum hat das BSI die Bewertung von einem weiteren Verfahren erfolgreich abgeschlossen. Zur Untersuchung der Möglichkeiten und Risiken bei foto- und videobasierten Prüfungen von Ausweisdokumenten kooperiert das BSI weiterhin mit dem BKA.

2.1.12 — Sichere elektronische Identitäten auf dem Smartphone

Ungesicherte, offene oder falsch konfigurierte Online-Server und -Dienste stellen eine breite Angriffsfläche für Cyber-Angriffe dar (vgl. zum Beispiel Kapitel *Ransomware*, bzw. konkret Kapitel *Beispielhafter Angriffsverlauf*, Seite 15). Erbeutete Identitätsdaten können für vielfältige weitere Angriffe missbraucht werden (vgl. zum Beispiel der Abschnitt E*rpressung mit erbeuteten Identitätsdaten*, Seite 17). Die Verbesserung der Cyber-Sicherheit ist eine gemeinsame Aufgabe sowohl von Herstellern und Anbietern von Produkten und Online-Diensten als auch von Nutzerinnen und Nutzern.

Eine Grundvoraussetzung für die erfolgreiche Umsetzung von Digitalisierungsvorhaben ist die breite Verfügbarkeit von eID-Verfahren, welche eine Identifizierung auf einem geeigneten Vertrauensniveau ermöglichen. Das aktuelle Großprojekt Digitale Identitäten der Bundesregierung sieht hierfür die Einführung einer mobilen Identitätslösung vor, die durch die Smart-eID realisiert wird. Diese basiert auf der Technologie des Personalausweises und ermöglicht es, Identitätsdaten sicher abzuspeichern und datensensible Dienste auch auf dem Smartphone nutzbar zu machen.

Da Smartphones, wie jedes vernetzte Gerät, ständig der Gefahr eines Cyber-Angriffs ausgesetzt sind, müssen besondere Voraussetzungen erfüllt sein, damit sich die sichere Speicherung einer eID auf dem Smartphone gewährleisten lässt. Grundlage für die Smart-eID ist daher ein eID-Applet, das ausschließlich innerhalb eines Sicherheitselementes des Mobilgerätes ausgeführt werden darf. Hierfür kommt entweder ein Secure Element („SE“) oder ein eUICC („eSIM“) in Frage. Das Applet selbst basiert auf den etablierten kryptografischen Protokollen des Personalausweises. Das hat den Vorteil, dass die Smart-eID kompatibel zu bestehenden Diensten ist, welche bereits die Online-Ausweisfunktion angebunden haben.

Bei der Realisierung der Smart-eID agiert das BSI als technische Projektleitung für die mit der Durchführung beauftragten Unternehmen und erstellt technische Konzepte, Sicherheitsvorgaben und Schnittstellen mit dem Ziel, eine hochsichere und gleichsam benutzerfreundliche Lösung für die Bürgerinnen und Bürger bereitzustellen. Parallel dazu führt das BSI Gespräche mit Herstellern von mobilen Endgeräten und bringt entsprechende Expertise in internationale Standardisierungsgremien ein.

2.1.13 — Mediale Identitäten

Eine mediale Identität beschreibt die Repräsentation eines Individuums in digitalen Medien wie Videos oder Audiosignalen. Durch Methoden aus dem Bereich der künstlichen Intelligenz wird es zunehmend einfacher, auch ohne spezielles Expertenwissen, eine solche Identität zu manipulieren. Aufgrund der Nutzung von tiefen neuronalen Netzen (engl. „deep neural networks”) spricht man hierbei umgangssprachlich von *„Deepfakes”*.

Die Bedrohungslage durch die Manipulation von medialen Identitäten hat im Berichtszeitraum zugenommen. Denn bisher wurden mediale Identitäten häufig zu Unterhaltungszwecken oder lediglich in der Theorie betrachtet. Hohe Medienaufmerksamkeit hat im Oktober 2021 ein sogenannter *CEO-Fraud* erhalten, bei dem ein Bankdirektor aus Hongkong über einen Anruf mit gefälschter Stimme dazu gebracht wurde, Überweisungen in der Gesamthöhe von 35 Million US-Dollar an Cyber-Kriminelle zu autorisieren. Ebenso wurde die Nutzung von *Deepfakes* zu Propagandazwecken, beispielsweise in Konfliktsituationen, zur realistischen Bedrohung. Im März 2022 erschien eine vermeintliche Kapitulationsansprache vom ukrainischen Präsidenten Selenskyj in sozialen Medien und auf infiltrierten ukrainischen Nachrichtenportalen. Dieses Video, bei dem der künstlich generierte Kopf des Präsidenten auf einen Schauspieler gesetzt und die Stimme künstlich angepasst wurde, war jedoch von niedriger Qualität, weshalb die Fälschung relativ schnell als solche erkannt wurde und damit keinen größeren Schaden anrichten konnte.

Es zeigt sich also, dass automatisierte Manipulationen von medialen Identitäten immer mehr Einsatz in verschiedensten Bedrohungsszenarien gegen Staat, Wirtschaft und Gesellschaft finden. Weiter wurde im Berichtszeitraum sowohl im Audio- wie auch im Videobereich beobachtet, dass die Echtzeitfähigkeit der Manipulationsmethoden zunimmt und das bei zunehmender Qualität. Das konnte auch exemplarisch durch das BSI nachgestellt werden (siehe Abbildung 21). Ebenso wird eine wachsende öffentliche Verfügbarkeit von Werkzeugen zur Erstellung von Fälschungen beobachtet, wodurch es für Fälscher einfacher wird hochqualitative Manipulationen durchzuführen.

Da eine zentrale präventive Gegenmaßnahme gegen die Gefahren von *Deepfakes* in der Aufklärung über diese Technologie liegt, hat das BSI Anfang 2022 eine Themenseite zu der Deepfake-Technologie veröffentlicht.

Abbildung 21: Ergebnis eines Face-Swap (rechts) von Arne Schönbohm (Mitte) als Zielperson auf einen BSI-Mitarbeiter (links) als Angreifer.

Weiterführende Informationen finden Sie hier:[i]

2.1.14 — Moderne Messenger für sichere Kommunikation

Neben Telefon und E-Mail gehören moderne Messenger längst zum Alltag und zählen zu den am meisten verwendeten Kommunikationsmitteln. Im Jahr 2021 nutzten 83 Prozent der Deutschen mindestens wöchentlich einen Messenger-Dienst, bei den unter 30-Jährigen sind es sogar 99 Prozent. 73 Prozent der Nutzerinnen und Nutzer betreiben dabei Multihoming, das heißt, sie verwenden mindestens zwei verschiedene Messenger-Dienste parallel. Auch im Umfeld der Bundesverwaltung erfreuen sich Messaging-Lösungen wachsender Beliebtheit und sind in vielen Behörden im Einsatz[29]. Ihre Nutzung hat nicht zuletzt auch aufgrund der weiterhin andauernden COVID-19-Pandemie und des damit verbundenen verstärkten Arbeitens im Home Office weiter zugenommen.

Um die Vertraulichkeit der Kommunikation zu schützen, sind die meisten Messenger heutzutage in irgendeiner Form verschlüsselt. Welche Inhalte verschlüsselt werden – also ob nur Textnachrichten oder auch Bilder, Dateien und Audio-/Videotelefonate, ob nur in Einzel- oder auch in Gruppenkonversationen – und wie diese verschlüsselt werden – also ob Ende-zu-Ende- oder Transportverschlüsselung – ist dabei sehr unterschiedlich und mitunter auch eine Sache der gewählten Einstellungen. Neben den reinen Kommunikationsinhalten fallen bei der Verwendung eines Messengers eine Reihe weiterer Daten, sogenannte Metadaten, an. Einige dieser Metadaten sind aus technischer Sicht nicht zu vermeiden, andere hingegen (darunter Profilinformationen) werden durch manche Betreiber gezielt erhoben und beispielsweise für Werbezwecke genutzt oder weiterverkauft.

Das BSI beschäftigt sich daher intensiv mit dem Thema Messaging und begleitet wichtige Entwicklungen auf diesem Gebiet. So hat das BSI Ende 2021 mehrere Publikationen zu den technischen Grundlagen moderner Messenger[30] und dem Thema "Interoperabilität"[31] verfasst sowie kürzlich ein Expertenvideo[32] veröffentlicht. Ferner unterstützt das BSI andere Behörden und Mitglieder des Bundestages durch fachliche Expertise in diesem Bereich. Eines der vom BSI begleiteten Messaging-Projekte in der Bundesverwaltung stellt der zentrale Proof-of-Concept-Betrieb des Messengers Wire dar, bekannt unter dem Namen „Wire Bund“. Mitte des Jahres wurde ein wichtiger Meilenstein erreicht: eine kryptografisch abgesicherte Föderation verschiedener Wire-Instanzen, die eine backendübergreifende Ende-zu-Ende-verschlüsselte Kommunikation ermöglicht.

Anders als bei Telefon und E-Mail, wo es keine Rolle spielt, welchen Anbieter man nutzt, kann man mit einem Messenger nur jeweils mit Nutzerinnen und Nutzern des gleichen Messenger-Dienstes kommunizieren. Eine technische Hürde für diese fehlende Interoperabilität ist der Tatsache geschuldet, dass die meisten Messenger heutzutage verschlüsselt arbeiten und es bislang kein standardisiertes kryptografisches Protokoll gab, das dafür hätte zum Einsatz kommen können. Zwar basiert die Verschlüsselung vieler Messenger auf dem sogenannten Double-Ratchet-Protokoll, doch die meisten Messenger-Anbieter haben ihre eigene Variante des Protokolls implementiert. Die damit einhergegangenen Änderungen – selbst nur eines kleinen Details – führt in der Praxis dazu, dass die verschiedenen Messenger nicht miteinander kompatibel sind, d. h. beispielsweise keine Nachrichten zueinander ver- bzw. entschlüsseln können. In dieser Hinsicht stellt der IETF-Standard „Messaging Layer Security“[33], dessen Ausarbeitung das BSI eng begleitet, ein weiteres wichtiges Thema dar. Bei MLS handelt es sich um eine Weiterentwicklung des Double-Ratchet-Protokolls, das insbesondere ein effizientes Schlüsselmanagement auch in großen Gruppen ermöglicht. An der Ausarbeitung des Standards sind neben der Firma Wire eine Reihe namhafter Unternehmen (u. a. Mozilla, Twitter, Cisco, Google, Facebook) sowie Forschungseinrichtungen (INRIA) und Universitäten (MIT, University of Oxford) beteiligt. Wire Bund ist neben Wire einer der ersten Messenger, in dem das neue MLS-Protokoll bereits zum Einsatz kommt und es wird erwartet, dass viele der anderen Messenger auf dem Markt diesem Vorbild folgen werden.

2.2 — Wirtschaft

Die Erfolge bei der Digitalisierung entscheiden im hohen Maße über die Zukunft des Wirtschaftsstandortes Deutschland. Eine funktionierende und sichere IT schafft dafür die wesentlichen Voraussetzungen – sei es für das Betreiben Kritischer Infrastrukturen (KRITIS) oder die erfolgreiche Transformation der Geschäftsmodelle von kleinen und mittleren Unternehmen (KMU). Daher unterstützt das BSI mit zahlreichen Angeboten die *Resilienz* des Cyber-Standortes Deutschland sowie KRITIS-Betreiber bei der Umsetzung von Präventionsmaßnahmen gegen Cyber-Attacken. KMU profitieren

vom fachlichen Austausch sowie von praxisorientierten IT-Sicherheitsempfehlungen. Mit der Allianz für Cyber-Sicherheit wiederum stärkt das BSI die Widerstandsfähigkeit des Standorts Deutschland. Für mehr Informationssicherheit neuer Technologien gestaltet das BSI u. a. praxisgerechte Sicherheitsanforderungen, Standards und Handlungsempfehlungen. Auch als zentrale Zertifizierungs- und Standardisierungsstelle übernimmt das BSI Verantwortung und leistet obendrein einen wesentlichen Beitrag zum Gelingen großer Digitalisierungsprojekte.

2.2.1 — Erkenntnisse zur Gefährdungslage in der Wirtschaft

Die Wirtschaft war auch in diesem Berichtszeitraum erneut einer großen Anzahl von Cyber-Angriffen ausgesetzt, von denen der Großteil wiederum durch *Ransomware* geprägt war (vgl. Kapitel *Ransomware*, Seite 13).

Zentrale Herausforderung für die Unternehmen in Deutschland ist die Steigerung der Cyber-Resilienz, d. h. die Kombination aus guter Präventionsarbeit mit der Möglichkeit, auf Cyber-Angriffe zu reagieren mit dem Ziel, den Betrieb des Unternehmens aufrechtzuerhalten und zu sichern. Das BSI beobachtet eine starke Zunahme der Nachfrage nach den Unterstützungsangeboten – von den Standards zur Cyber-Sicherheit bis hin zu Austausch- und Unterstützungsformaten wie der Allianz für Cyber-Sicherheit. Für die Cyber-Sicherheitslage in Deutschland ist die Verfassung der IT-Sicherheit in der Wirtschaft essenziell, sodass eine Intensivierung der Bemühungen der Unternehmen in diesem Bereich für die Verbesserung der Cyber-Sicherheit von großer Bedeutung ist.

2.2.2 — Gefährdungslage Kritischer Infrastrukturen

Kritische Infrastrukturen (KRITIS) 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 auch die Verarbeitung und Speicherung von Daten in Rechenzentren oder die Versorgung der Bevölkerung mit Bargeld.

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 BSIG für KRITIS-Betreiber Maßnahmen zur Prävention (§ 8a BSIG) und zur Bewältigung (§ 8b BSIG) von IT-Sicherheitsvorfällen oder IT-Störungen vor.

Russischer Angriffskrieg gegen die Ukraine rückt die Verwundbarkeit Kritischer Infrastrukturen weiter in den Fokus

Bereits im vorangegangenen Berichtszeitraum verstärkte sich die Aufmerksamkeit der Öffentlichkeit auf Vorfälle im Gesundheitssystem durch die COVID-19-Pandemie. Durch den russischen Angriffskrieg gegen die Ukraine rückte die Sicherheit der Kritischen Infrastrukturen in Deutschland nun noch stärker in den Fokus der Öffentlichkeit. Schon vor Beginn des russischen Überfalls auf die Ukraine aktivierte das BSI das Nationale IT-Krisenreaktionszentrum und rief unter anderem Betreiber Kritischer Infrastrukturen zu erhöhter Wachsamkeit und Reaktionsbereitschaft auf.

Bedrohung durch Angriffe auf die Software-Lieferketten von IT-Dienstleistern

Das BSI beobachtet seit Jahren eine zunehmende Entwicklung hin zu aufwendig vorbereiteten APT-Angriffen, von der sich weltweit auch die Betreiber Kritischer Infrastrukturen bedroht sehen. Darüber hinaus bilden die in den letzten Jahren beobachteten Angriffe auf die Software-Lieferketten („Supply-Chain“) von IT-Dienstleistern zu ihrer Kundschaft eine neue, besonders beunruhigende Bedrohung.

Mit der Verbreitung von Schadcode über die regulären Update-Mechanismen der (Sicherheits-)Software global operierender IT-Dienstleister lassen sich etablierte Sicherheitsmechanismen umgehen. Die Manipulation von (Sicherheits-)Updates, die bei Kundinnen und Kunden eingespielt werden, machen Angriffe auf sehr gut geschützte IT-Systeme möglich. Solche Angriffe sind zudem äußerst schwer zu erkennen, da sich der *Quellcode* von den Kundinnen und Kunden üblicherweise nicht einsehen oder bewerten lässt.

Nur durch die detaillierte Analyse der Lieferbeziehungen kann einer Gefahr durch Angriffe auf die Liefer-

kette begegnet werden. Eine sorgfältige Auswahl der Lieferanten ist vor diesem Hintergrund für KRITIS-Betreiber von entscheidender Bedeutung.

Aktualisierung von branchenspezifischen Sicherheitsstandards im Berichtszeitraum

KRITIS-Betreiber müssen zur Umsetzung des § 8a Abs. 1 BSIG angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen treffen. Hierbei sollen sie den Stand der Technik einhalten. Zur Definition und Konkretisierung des Stands der Technik können die Branchen branchenspezifische Sicherheitsstandards (B3S) erarbeiten, für die das BSI auf Antrag feststellt, ob sie geeignet sind, die gesetzlichen Anforderungen zu erfüllen. Mehr als zwanzig KRITIS-Branchen haben bereits B3S erstellt oder erarbeiten solche. Aufgrund der dynamischen technischen Entwicklung muss die Eignung jedes B3S nach zwei Jahren erneut vom BSI festgestellt werden.

Im Berichtszeitraum hat das BSI für B3S aus den folgenden Branchen die Eignung festgestellt:

- B3S Lebensmittelhandel V2.2
- B3S für Verkehrssteuerungs- und Leitsysteme im kommunalen Straßenverkehr
- B3S Lebensmittelhandel V2.2
- B3S Wasser/Abwasser

Die aktuelle Liste der vom BSI positiv geprüften B3S steht auf der BSI-Website zur Verfügung:[m]

Meldungszahlen nach KRITIS-Sektoren im Berichtszeitraum

Mit dem IT-Sicherheitsgesetz wurde 2015 in § 8b Abs. 4 BSIG eine Meldepflicht für Betreiber Kritischer Infrastrukturen eingeführt. Die Meldepflicht gilt für Störungen, die zum Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen geführt haben oder führen können.

Im Berichtszeitraum gingen beim BSI 452 entsprechende Meldungen ein.

Sicherheitsmängel in ausgewählten KRITIS-Sektoren

KRITIS-Betreiber müssen gemäß § 8a Abs. 3 BSIG gegenüber dem BSI alle zwei Jahre den Nachweis erbringen, dass ihre IT-Sicherheit auf dem Stand der Technik ist. Die folgenden Statistiken beziehen sich daher auf diesen Zwei-Jahres-Zeitraum und nicht auf den Berichtszeitraum des Lageberichts. Die Nachweise enthalten Informationen zu Sicherheitsmängeln und umgesetzten Sicherheitsmaßnahmen.

Das BSI analysiert seit Jahren systematisch die Mängel, die im Rahmen der turnusmäßigen Nachweise aller KRITIS-Betreiber aufgedeckt und an das BSI übermittelt wurden. Durch die Klassifizierung der Mängel, die Aggregation zu übergreifenden Mangel-Kategorien und die anschließende Zeitreihenanalyse über mehrere Nachweiszyklen lassen sich für alle KRITIS-Sektoren Trends ableiten. Die Analyse der Nachweise ermöglicht es dem BSI, spezifische Schwerpunktthemen für einzelne Branchen zu identifizieren und in enger Zusammenarbeit mit den Betreibern entsprechende Maßnahmen zu entwickeln. Die aus den KRITIS-Nachweisen gewonnenen Erkenntnisse sind auch wichtige Informationen für die Branchenarbeitskreise des *UP KRITIS*.

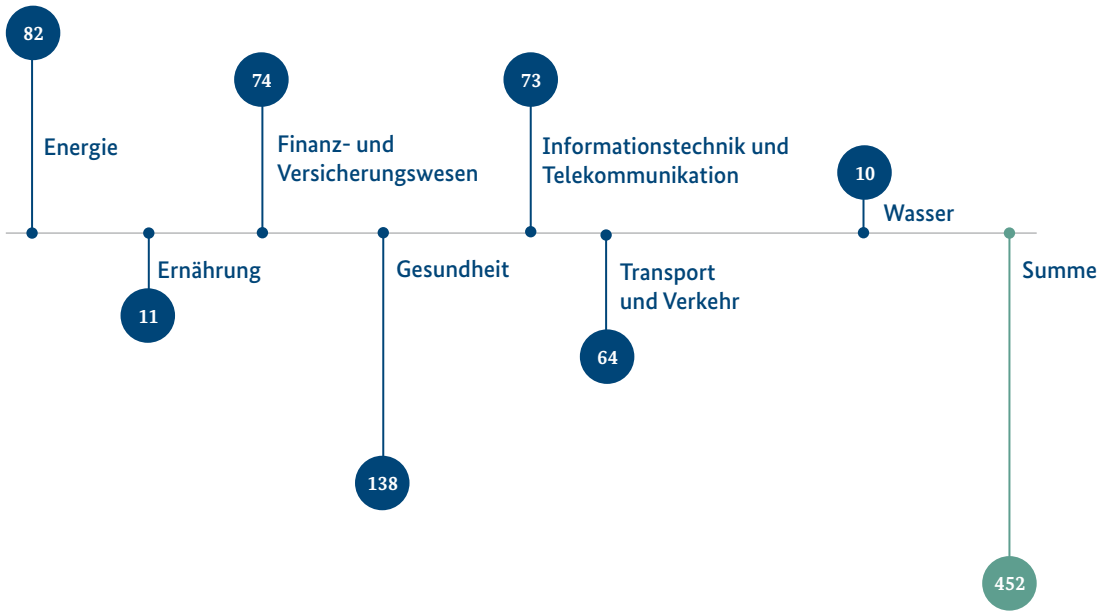
Im Zwei-Jahres-Zeitraum vom 1. April 2020 bis zum 31. März 2022 wurden im Rahmen der Prüfung der turnusmäßigen Nachweise in den Sektoren Energie, Ernährung, Finanz- und Versicherungswesen, Gesundheit (nur medizinische Versorgung), Informationstechnik und Telekommunikation sowie Wasser insgesamt 2.941 Sicherheitsmängel gefunden.

Für die genannten KRITIS-Sektoren wird im Folgenden die Häufigkeit von Sicherheitsmängeln dargestellt. Die Mängel wurden hierzu den Mangel-Kategorien der „Orientierungshilfe zu Nachweisen gemäß § 8a Abs. 3 BSIG“ des BSI zugeordnet, die in den folgenden Diagrammen zu übergreifenden Kategorien zusammengefasst wurden.

Weiterführende Informationen finden Sie hier:[n]

Meldungszahlen nach KRITIS-Sektoren im Berichtszeitraum (Juni 2021 bis Mai 2022)

Abbildung 22:
Meldungszahlen nach KRITIS-Sektoren im Berichtszeitraum (Juni 2021 bis Mai 2022)
Quelle: BSI



Mängel aus dem KRITIS-Sektor Energie

Im KRITIS-Sektor Energie ist der Anteil der Mängel in der Kategorie Managementsystem für Informationssicherheit (ISMS) im Vergleich zum Vorbericht angestiegen. Mängel in der Kategorie bauliche/physische Sicherheit machen den zweitgrößten Anteil aus, dies resultiert teilweise aus dem geringen Anteil an Vor-Ort-Prüfungen während der Pandemie. Mängel der Kategorie Asset Management bilden den drittgrößten Bereich.

Mängel aus dem KRITIS-Sektor Ernährung

Im KRITIS-Sektor Ernährung ist ein großer Anteil der identifizierten Mängel der Kategorie ISMS zuzuordnen. Auch Mängel im Bereich technische Informationssicherheit spielen mit über 20 Prozent eine große Rolle.

Mängel aus dem KRITIS-Sektor Finanz- und Versicherungswesen

Im KRITIS-Sektor Finanz- und Versicherungswesen wurden am häufigsten Mängel in den Kategorien ISMS, technische Informationssicherheit sowie Vorfallserkennung und -bearbeitung identifiziert. Im Vergleich zum vorherigen Auswertungszeitraum konnten aufgedeckte Mängel häufiger der Kategorie ISMS zugeordnet werden; im Vorjahresbericht entfiel noch fast ein Viertel aller Mängel auf die technische Informationssicherheit. Die Mängel-Kategorien Überprüfung im laufenden Betrieb und Asset Management spielten im aktuellen Auswertungszeitraum eine geringere Rolle.

Mängel aus dem KRITIS-Sektor Gesundheit (nur medizinische Versorgung)

Im KRITIS-Sektor Gesundheit (nur medizinische Versorgung) ist keine Mangel-Kategorie überdurchschnittlich stark vertreten. Die größten Anteile der identifizierten Mängel entfallen auf die Bereiche ISMS, Continuity- und Notfallmanagement für die kritische Dienstleistung und das Asset Management.

Mängel aus dem KRITIS-Sektor Informationstechnik und Telekommunikation

Im KRITIS-Sektor Informationstechnik und Telekommunikation wurden am häufigsten Mängel in den Bereichen ISMS, technische Informationssicherheit

sowie personelle und organisatorischen Sicherheit identifiziert. Im Vergleich zum vorherigen Auswertungszeitraum hat insbesondere der Anteil an Mängeln im Bereich ISMS einen deutlichen Zuwachs erfahren. Mängel in den Bereichen technische Informationssicherheit sowie personelle und organisatorische Sicherheit machen ebenfalls nach wie vor einen großen Anteil aus.

Mängel aus dem KRITIS-Sektor Wasser

Im KRITIS-Sektor Wasser wurden die meisten Mängel erneut dem Bereich ISMS zugeordnet. Mängel dieser Kategorie machten bereits im Vorjahr rund ein Drittel aller Mängel aus; im aktuellen Auswertungszeitraum stieg der Anteil auf über 50 Prozent. Die Kategorien bauliche/physische Sicherheit sowie technische Informationssicherheit machen zusammen 20 Prozent der identifizierten Mängel aus. Die Zusammenarbeit der Betreiber des Sektors Wasser mit dem BSI auf Basis der Mängelbeseitigung hat sich in den vergangenen Jahren intensiviert.

2.2.3 — UP KRITIS

Der *UP KRITIS* ist eine freiwillige Zusammenarbeit zwischen KRITIS-Betreibern, deren Fachverbänden und den zuständigen Behörden mit 840 teilnehmenden Organisationen. Im *UP KRITIS* gibt es Themen- und Branchenarbeitskreise, in denen sich die Mitglieder austauschen und an spezifischen Themen zusammenarbeiten. Das Plenum ist die Versammlung der Sprecherinnen und Sprecher aus den Arbeitskreisen sowie den zuständigen Behörden. Der Rat arbeitet auf politischer Ebene; er besteht aus hochrangigen Personen aus den KRITIS-Sektoren sowie aus den Behörden BMI, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) und BSI. Das BSI ist in zahlreichen Arbeitskreisen, dem Plenum, Stab und Rat des *UP KRITIS* vertreten.

Neue Branchenarbeitskreise

Mit dem *IT-Sicherheitsgesetz 2.0* hat die Bundesregierung die neun KRITIS-Sektoren um einen weiteren Sektor ergänzt: Neu hinzugekommen ist der Sektor „Siedlungsabfallentsorgung“. Damit werden auch die wichtigsten Entsorgungsunternehmen als Betreiber Kritischer Infrastrukturen eingestuft. Welche Unternehmen und Infrastruktur konkret betroffen sind, wird in der hierzu noch anzupassenden Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) detailliert dargestellt werden. Dies wird voraussichtlich zum Ende des Jahres hin geschehen. Der *UP KRITIS* hat aufgrund dieser Entwicklung im Sommer 2021 den zugehörigen Branchenarbeitskreis „Siedlungsabfallentsorgung" gegründet.

Schon seit längerer Zeit gibt es im *UP KRITIS* einen Branchenarbeitskreis für alle Versicherungen. Aufgrund der stark unterschiedlichen Strukturen und Prozesse bei privaten Versicherungen und der Branche Gesetzliche Krankenversicherungen hat das Plenum des *UP KRITIS* im Herbst 2021 einen eigenen Branchenarbeitskreis für die Branche der Gesetzlichen Krankenversicherungen gegründet.

Das BSI begleitet in vielen Arbeitskreisen des *UP KRITIS* die dort durchgeführten Tätigkeiten. Zahlreiche Publikationen wurden im Berichtszeitraum von Themenarbeitskreisen veröffentlicht.

Eine Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung finden Sie hier:[o]

Weiterführende Informationen zu UP KRITIS finden Sie hier:[p]

Operative Zusammenarbeit

Auf operativer Ebene arbeiten die Mitglieder des *UP KRITIS* zu Themen der aktuellen Lage zusammen. Der russische Angriffskrieg in der Ukraine führte bei vielen KRITIS-Betreibern zu operativen Herausforderungen. Im Frühjahr 2022 führte dies zu einem intensiven Informationsaustausch, für den ein eigener Themenarbeitskreis gegründet wurde.

Das Thema „Umgang mit der COVID-19-Pandemie“ erstreckt sich über den gesamten Berichtszeitraum. Erfahrungen aus dem Krisenmanagement während der Pandemie haben KRITIS-Betreiber im Themenarbeitskreis „Szenariobasierte Krisenvorsorge" ausgetauscht.

2.2.4 — Unternehmen im Fokus der europäischen und deutschen Cyber-Sicherheits-Regulierung

Am 28. Mai 2021 ist das IT-Sicherheitsgesetz. (IT-SiG 2.0) in Kraft getreten. Das IT-SiG 2.0 ist die Weiterentwicklung des ersten IT-Sicherheitsgesetzes aus 2015, mit dem KRITIS-Betreiber in Deutschland gesetzlich zur Registrierung und zur Meldung relevanter IT-Sicherheitsvorfälle beim BSI verpflichtet wurden.

Das IT-SiG 2.0 erweitert die Befugnisse des BSI als zentrale Meldestelle für die Informationssicherheit von Staat und Wirtschaft, enthält neue Anforderungen an die IT-Sicherheit der KRITIS-Betreiber und sieht höhere Bußgelder für Gesetzesverstöße vor.

Pflicht zum Einsatz von Systemen zur Angriffserkennung

Das IT-SiG 2.0 ergänzt die Vorgabe „angemessener Sicherheit" explizit um den Einsatz von Systemen zur Angriffserkennung. Durch den Einsatz von technischen Werkzeugen und die Implementierung organisatorischer Prozesse sollen Angriffe auf informationstechnische Systeme von KRITIS-Betreibern frühzeitig erkannt und so die Auswirkungen von Störungen minimiert werden. Das BSI hat zusammen mit dem Themenarbeitskreis Detektion des *UP KRITIS* die Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung zur Unterstützung der Umsetzung erstellt und veröffentlicht.

Unternehmen im besonderen öffentlichen Interesse (UBI)

Mit dem IT-SiG 2.0 wurden auch Rechte und Pflichten für weitere Unternehmen eingeführt, die von herausragender Bedeutung für die Gesellschaft sind. Im Gesetz werden diese Unternehmen als Unternehmen im besonderen öffentlichen Interesse (UBI) bezeichnet.

Zu den UBI zählen:

- Hersteller/Entwickler von Gütern im Sinne von § 60 Außenwirtschaftsverordnung (AWV), also Unternehmen, die im Bereich Waffen, Munition und Rüstungsmaterial oder im Bereich von Produkten mit IT-Sicherheitsfunktionen zur Verarbeitung staatlicher Verschlusssachen oder für die IT-Sicherheitsfunktion wesentlicher Komponenten solcher Produkte tätig sind (UBI 1),
- die nach ihrer inländischen Wertschöpfung größten Unternehmen Deutschlands sowie wesentliche Zulieferer für diese Unternehmen (UBI 2) sowie
- Betreiber eines Betriebsbereichs der oberen Klasse im Sinne der Störfall-Verordnung oder Betreiber, die nach § 1 Abs. 2 der Störfall-Verordnung diesen gleichgestellt sind (UBI 3).

Das IT-SiG 2.0 sieht für UBI Meldepflichten vor, wie sie bereits für KRITIS-Betreiber gelten. Daneben gelten für UBI 1 und UBI 2 jeweils eine Pflicht zur Registrierung beim BSI sowie zur Abgabe einer Selbsterklärung zur IT-Sicherheit. Für UBI 3 ist eine Registrierung freiwillig; eine Selbsterklärung muss nicht abgegeben werden.

Beim BSI registrierte UBI profitieren von einer Reihe von Dienstleistungen des BSI. Beispielsweise erhalten sie Warnmeldungen, Lagebildprodukte und Cyber-Sicherheitsempfehlungen. Darüber hinaus können sie auf spezielle Unterstützungsangebote des BSI zurückgreifen.

Für UBI 3 gelten die neuen Verpflichtungen seit dem 1. November 2021, für UBI 1 ab dem 1. Mai 2023 und für UBI 2 frühestens zwei Jahre nach Inkrafttreten der UBI-Verordnung, die definiert, welche Unternehmen den neuen Regelungen für UBI unterliegen.

Weiterführende Informationen finden Sie hier:[q]

Netzkodex über Cyber-Sicherheit

Mit dem letzten Energiebinnenmarktpaket[34] wurde unter anderem die Verordnung über die Netzzugangsbedingungen für den grenzüberschreitenden Stromhandel überarbeitet. Eine der Änderungen beinhaltete die Ermächtigungsgrundlage für den europäischen Verband der Übertragungsnetzbetreiber (ENTSO-E) und für den europäischen Verband der Verteilnetzbetreiber (EU DSO entity), einen Netzkodex zum Thema Cyber-Sicherheit zu erarbeiten.

Netzkodizes in der Branche Strom werden vornehmlich von ENTSO-E entwickelt und durch die Agentur für die Zusammenarbeit der Energieregulierungsbehörden

(ACER) sowie die europäische Kommission in eine europäische Verordnung überführt. Der Netzkodex über Cyber-Sicherheit beinhaltet Anforderungen an das europäische Stromverbundsystem mit dem Ziel, das Sicherheitsniveau der Mitgliedsstaaten anzugleichen und kontinuierlich zu erhöhen.

Stand der aktuellen Entwicklung

Nach Inkrafttreten des Strombinnenmarktpakets und der damit einhergehenden Änderung, dass auch zum Thema Cyber-Sicherheit ein Netzkodex zu erarbeiten ist, wurde seitens ENTSO-E und EU DSO entity mit der Entwicklung begonnen. Der erarbeitete Vorschlag von ENTSO-E und EU DSO entity wurde im Januar 2022 an ACER übergeben. Es ist davon auszugehen, dass der Netzkodex als europäische Verordnung voraussichtlich spätestens Anfang 2023 in Kraft treten wird.

Inhalt des Netzkodex

Durch den Netzkodex sollen insbesondere ein einheitliches Cyber-Sicherheitsniveau sowie ein einheitlicher Umgang mit Cyber-Sicherheitsvorfällen von Akteuren im europäischen Stromverbundsystem erreicht werden. Adressiert werden insbesondere Übertragungsnetzbetreiber, große Verteilnetzbetreiber, Anbieter kritischer Servicedienstleistungen sowie verschiedene Behörden. Kernanforderung ist die regelmäßige Durchführung von Risikobewertungen im Hinblick auf Cyber-Sicherheit in der Stromversorgung. Dazu werden Unternehmen identifiziert, die einen kritischen oder hohen Beitrag zur europäischen Stromversorgung leisten.

Für diese Unternehmen sollen einheitliche Vorgaben zur Durchführung von Risikoanalysen, Risikobewertungen und Risikobehandlungen unternehmensintern, national, regionsübergreifend und europäisch entwickelt werden. Zudem werden einheitliche Maßnahmen zur Risikobehandlung erarbeitet, u. a. durch die Definition von Mindest- und weiterführenden Cyber-Sicherheitsanforderungen auf Basis existierender Standards. Auch der Umgang mit Cyber-Sicherheitsvorfällen, die einen grenzüberschreitenden Bezug haben, wird durch die Entwicklung von einheitlichen Informations- und Reaktionsprozessen sowie die Einführung eines europäischen Krisenmanagements weiterentwickelt.

Die Bedeutung des Netzkodex im Hinblick auf die bestehende nationale Gesetzgebung

Der Netzkodex wird die bereits existierenden Cyber-Sicherheitsanforderungen im Energiebereich um Anforderungen ergänzen, die primär den grenzüberschreitenden Aspekt der Stromversorgung tangieren. Der Netzkodex wird damit zur Erhöhung des Cyber-Sicherheitsniveaus im gesamten europäischen Stromverbundsystem beitragen.

2.2.5 — Besondere Situation der kleinen und mittleren Unternehmen in Deutschland

2,6 Millionen kleine und mittlere Unternehmen (KMU) in Deutschland stehen vor den Herausforderungen der Digitalisierung und damit einhergehend der Cyber-Sicherheit. Dieser Teilbereich von Unternehmen, der anteilmäßig 99,4 Prozent der deutschen Wirtschaftsunternehmen ausmacht, gliedert sich wie folgt auf:

Unternehmen in Deutschland nach Größe
Angaben in %

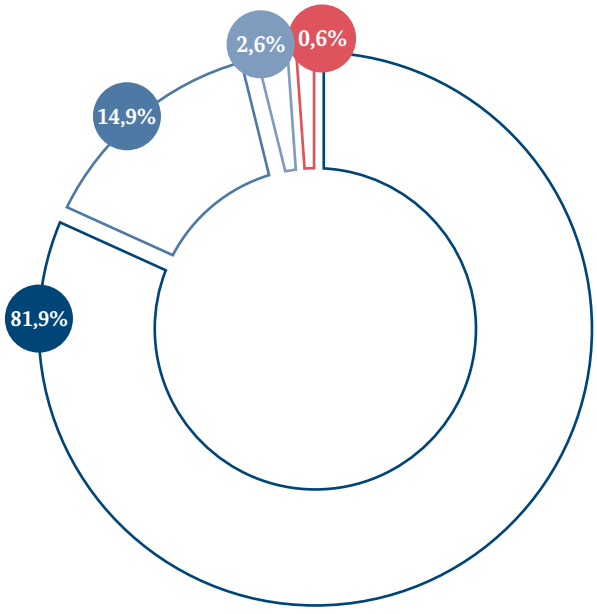


Abbildung 23:
Quelle: Statistisches Bundesamt, Stand: Juli 2021

Gerade die Kleinst- (weniger als zehn Mitarbeitende) und die kleinen (weniger als 50 Mitarbeitende) Unternehmen verfügen oftmals nicht über das erforderliche Personal, das sich um Betrieb und Absicherung der Informationstechnik des Unternehmens kümmert.

Viele Unternehmen besitzen laut Erkenntnissen des BSI und einer Studie des Bundesministeriums für Wirschaft und Energie (BMWI, jetzt Bundesministerium für Wirtschaft und Klimaschutz (BMWK))[35] auch im Jahr 2022 weder Kenntnisse über die allgemeine Cyber-Bedrohungslage noch über das eigene Risikoprofil. Es mangelt ihnen daher an einem Bewusstsein, mehr in ihre Sicherheit zu investieren. Diejenigen hingegen, die bereits ein Problembewusstsein entwickelt haben und IT-Personal einstellen möchten, erleben häufig, dass sie in einem Angebotsmarkt als potenzieller Arbeitgeber nicht gegen die Gehälter bei Großunternehmen oder IT-Dienstleistern bestehen können. Und diejenigen, die den Bereich IT/IT-Sicherheit an einen Dienstleister auslagern möchten, müssen häufig feststellen, dass es in ihrer Region entweder zu wenig qualifizierte Dienstleister gibt oder nur solche, die nicht zu ihrer eigenen Unternehmensgröße passen. Dies alles führt dazu, dass einige KMU zum einen Opfer Cyber-Krimineller werden und zum anderen auf einen Vorfall nicht angemessen reagieren können.

Eine im Auftrag des BMWi im Jahr 2021 veröffentlichte Studie[36] kam zu folgendem Ergebnis: „Im Ereignisfall wissen KMU oftmals nicht, an wen sie sich wenden können, um fachlich versierte Hilfe zu erhalten. Im Gegensatz zu Einbrüchen in der analogen Welt ist der digitale Schaden für viele KMU nicht immer und nicht unmittelbar ersichtlich. Die Hemmschwelle, Vorfälle und Angriffe an die Polizei, die Landeskriminalämter oder andere behördlichen Stellen zu melden, ist hoch.Daher hat das BKA eine kurze Handreichung für betroffene Unternehmen im Ernstfall veröffentlicht[37].

Um KMU hierzu eine passgenaue Unterstützung zu liefern, hat das BSI die für diese Zielgruppe wichtigsten Informationen in einem eigenen Bereich auf der BSI-Website zusammengestellt:[r]

Informationen zur präventiven Absicherung von IT-Systemen und weiterführende Angebote der Allianz für Cyber-Sicherheit werden unter anderem durch ein Verzeichnis qualifizierter IT-Dienstleister ergänzt, die im Notfall helfen können. Zudem können KMU, die von einem Cyber-Angriff betroffen sind, diesen über die Website an das BSI melden. Unternehmen, die besser für Cyber-Bedrohungen gerüstet sein wollen, finden hilfreiche Anleitungen und Empfehlungen in unterschiedlichen IT-Grundschutz-Profilen. Das BSI hat unter anderem für Handwerksbetriebe ein IT-Grundschutz-Profil veröffentlicht. Eine detaillierte Hilfestellung bietet ergänzend ein Routenplaner, mit dem sich ein betrieblicher Prozess zur Steigerung der Informationssicherheit Schritt für Schritt umsetzen lässt. Mit Blick auf Prävention können Cyber-Versicherungen – als ein relativ neues Produkt der Versicherungsbranche – für Unternehmen interessant sein, da ein cyber-sicherheitsrelevanter Vorfall ein Unternehmen schnell auch finanziell beeinträchtigen kann.

2.2.6 — Cyber-Sicherheit im Automobilbereich

Das Thema Cyber-Sicherheit steht auch 2022 im Fokus der Automobilindustrie. Nachdem 2020 internationale Regelungen für die Cyber-Sicherheit von Kraftfahrzeugen auf Ebene der Wirtschaftskommission für Europa der Vereinten Nationen (UNECE) beschlossen wurden (UNECE-Regulierung 155), werden diese nun nach EU-Recht (EU-Verordnung 2019/2144) ab Juli 2022 für die Fahrzeughersteller verbindlich. Durch die Regulierung werden Automobilhersteller verpflichtet, möglichen IT-bezogenen Gefährdungen durch ein sogenanntes Cyber Security Management System (CSMS) zu begegnen, das geeignete Entwicklungs- und Reaktionsprozesse vorsieht, z. B. zum IT-Störungs-Management (Incident Management) und zur Behebung von Schwachstellen.

Einige Hersteller haben bereits ein CSMS implementiert und sich dieses durch IT-technische Dienste auditieren lassen, was eine Voraussetzung für eine anschließende Genehmigung von Fahrzeugtypen nach der genannten Regulierung darstellt. Das BSI hat zur Unterstützung des Kraftfahrt-Bundesamtes (KBA) ausgewählte Auditierungsverfahren begleitet. Das KBA hat im Dezember 2021 die weltweit erste Typgenehmigung im Bereich des automatisierten Fahrens für ein automatisches Spurhaltesystem (Automated Lane Keeping System – ALKS) für ein Modell des Herstellers Mercedes-Benz erteilt. Dieses System entspricht der Automatisierungsstufe 3 nach der Norm SAE J3016, bei der die Fahrerin oder der Fahrer die automatische Steuerung nicht dauernd überwachen muss. Voraussetzung für die Genehmigung war die

Erfüllung der Anforderungen zur Cyber-Sicherheit nach der UNECE-Regulierung 155.

Neben der Begleitung von CSMS-Audits und Typgenehmigungen im Rahmen des *Witnessings* bei der Benennung von Technischen Diensten haben das KBA und das BSI ihre Zusammenarbeit auf Grundlage der 2020 abgeschlossenen Verwaltungsvereinbarung auch für den Bereich der Marktüberwachung und den Austausch von Informationen zu IT-bezogenen Vorfällen und Schwachstellen vertieft.

Im Juli 2021 trat das Gesetz zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes – Gesetz zum autonomen Fahren – in Kraft. Es ermöglicht unter anderem den Einsatz von Kraftfahrzeugen mit autonomer Fahrfunktion in festgelegten Betriebsbereichen des öffentlichen Straßenverkehrs. Damit wird erstmals die rechtliche Grundlage für den Betrieb von automatisierten Fahrzeugen auf Stufe 4 (nach der zuvor genannten Norm) im Regelbetrieb geschaffen. Einsatzszenarien sind zum Beispiel fahrerlose Busse, die auf festgelegten Strecken mit niedriger Geschwindigkeit fahren (Shuttle-Verkehr und sogenannte People-Mover), oder automatisches Einparken in speziell ausgerüsteten Parkhäusern (Automated Valet Parking). Das Gesetz sowie die Verordnung zur Durchführung des Gesetzes zum autonomen Fahren definieren u. a. Anforderungen an die technische Beschaffenheit und Ausrüstung sowie Pflichten an die Beteiligten beim Betrieb derartiger Kraftfahrzeuge. Die IT-Sicherheit sowie die Einbindung des BSI bei der Bewertung derartiger Fahrzeugsysteme für Erprobungsgenehmigungen wird hierbei explizit gefordert. Im Hinblick auf die IT-Sicherheit beteiligt nach §1i StVG das KBA das BSI bei der Erstellung, Umsetzung und bei der Weiterentwicklung und Bewertung entsprechender technischer Anforderungen.

Im Januar 2022 publizierte das BSI die Technische Richtlinie BSI-TR-03164 „Guidance for Cooperative Intelligent Transport Systems (C-ITS)“. In kooperativen intelligenten Transportsystemen kommunizieren vernetzte Verkehrsteilnehmer und Verkehrsinfrastruktur miteinander. Ziel ist es, auf Basis der ausgetauschten Informationen den Straßenverkehr sicherer, komfortabler und effizienter zu gestalten. Auf europäischer Ebene wurden dafür eine Certificate Policy (CP) und weitere Standards entwickelt. Die Technische Richtlinie ist als Ergänzung zur CP und den einschlägigen Standards zu sehen und dient als Richtlinie für den Betrieb von Public-Key-Infrastrukturen und C-ITS-Stationen im europäischen Anwendungskontext. Ziel der Technischen Richtlinie BSI TR-03164 ist es, Lücken in den Vorgaben zu schließen und Vorgaben zu konkretisieren, um ein durchgehend hohes und konsistentes Sicherheitsniveau bei allen Instanzen zu ermöglichen und die Interoperabilität der C-ITS-Teilnehmer zu gewährleisten.

Das BSI hat 2021 erstmalig das Branchenlagebild Automotive veröffentlicht. Dieses betrachtet neben der IT im Fahrzeug auch die Cyber-Sicherheit im Unternehmenskontext und der Lieferkette im Herstellungsprozess. So können unzureichend geprüfte oder manipulierte Hard- oder Software die Sicherheit des Fahrzeugs einschränken, wenn dies im Produktionsprozess nicht rechtzeitig erkannt wird. Dabei stehen nicht nur Hersteller weltweit im Fokus der Angreifenden, sondern auch deren Zulieferer. Dadurch kann es zu erheblichen Beeinträchtigungen in der Lieferkette kommen. Im Jahr 2021 waren mehrere Automobilzulieferer von Ransomware-Vorfällen betroffen (siehe auch Kapitel *Ransomware*, Seite 13). Es kam zu massiven Unterbrechungen der Produktion.

2.2.7 — Cyber-Sicherheit im Luftverkehr

Zusammen mit dem BMI und den Luftsicherheitsbehörden der Länder in Deutschland hat das BSI die Grundsätze zur Umsetzung der Durchführungsverordnung (EU) 2019/1583 erstellt, welche Ende 2021 durch das BMI veröffentlicht worden sind. Diese Grundsätze dienen der Umsetzung der zum 31. Dezember 2021 in Kraft getretenen DVO 2019/1583 und bieten den nach den §§ 5 und 8 des Luftsicherheitsgesetzes (LuftSiG) regulierten Unternehmen die Rahmenbedingungen zur Umsetzung der Informationssicherheit. Dabei wurden die Grundsätze im Nationalen Luftsicherheitsprogramm (NLSP) festgeschrieben. Somit müssen diese Vorgaben im Rahmen der regelmäßig neu durchzuführenden Zulassung überprüft und gegenüber der Landesluftsicherheitsbehörde nachgewiesen werden. Auch die Anforderungen an die Prüfung zur Einhaltung der Konformität mit den gesetzlichen Vorgaben wurden in den Grundsätzen festgeschrieben.

In Deutschland ist das BSI derzeit für die Organisation und Steuerung der Maßnahmen zur Informationssicherheit für die nach §§ 5 und 8 LuftSiG regulierten Unternehmen zuständig. Darunter fallen die 28 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 Digitales und Verkehr (BMDV). Zwischen dem BMDV und dem BMI wurde zwischenzeitlich eine Ressortvereinbarung unterschrieben mit dem Ziel, dass das BSI zukünftig für die §§ 9 und 9a LuftSiG zuständig sein wird.

Ausgelöst durch den russischen Angriff auf die Ukraine konnte sich das Warn- und Meldewesen für die Informationstechnik in der Luftsicherheit bereits in einer ersten Belastungsprobe beweisen. Im Rahmen der täglichen Sonderberichterstattung und der intensivierten Lagebeobachtung im Sektor Luftfahrt, konnten die theoretischen Prozesse und Abläufe auf ihre Praxistauglichkeit überprüft und optimiert werden.

2.2.8 — Digitalisierung der Energiewirtschaft

Cyber-Angriffe auf Unternehmen, staatliche Einrichtungen und Kritische Infrastrukturen der Ukraine haben gezeigt, dass kritische Infrastrukturen zunehmend in den Fokus geraten. Durch die Verwendung von intelligenten Messsystemen und der damit verbundenen Nutzung zertifizierter Smart-Meter-Gateways werden wichtige Systeme des Energienetzes über eine sichere Kommunikationsinfrastruktur vernetzt und Cyber-Angriffen somit wirksam begegnet.

Neben der Gewährleistung der IT-Sicherheit können Smart-Meter-Gateways u. a. Netzzustandsdaten und Einspeisewerte bereitstellen, so dass Stromnetzbetreiber mit Hilfe intelligenter Messsysteme wichtige Informationen über die aktuelle Belastung ihres Netzes erhalten. Dadurch können mögliche Engpässe rechtzeitig erkannt und diesen vorgebeugt werden. Zudem helfen die Informationen, den Ausbau des Stromnetzes effizient und kostengünstig zu gestalten. Flexible Verbrauchseinrichtungen (Wärmepumpen, Elektromobile, usw.) und dezentrale Erzeugungsanlagen können zudem zukünftig über das Smart-Meter-Gateway gesteuert und somit netz- und marktdienlich eingesetzt werden. Die sichere und standardisierte Fernsteuerung von Verbrauchs- und Erzeugungsanlagen über das Smart-Meter-Gateway ist elementar für ein zukunftsfähiges *Smart Grid*.

Für das Gelingen der Digitalisierung der Energiewende und der Schaffung eines sicheren intelligenten Stromnetzes *(Smart Grid)* ist die Entwicklung und Anwendung der BSI-Standards zur Gewährleistung von Cyber-Sicherheit erforderlich. Derzeit haben vier Hersteller von Smart-Meter-Gateways das Produktzertifizierungsverfahren des BSI nach CC erfolgreich abgeschlossen. Gemeinsam mit dem Bundesministerium für Wirtschaft und Klimaschutz (BMWK) wurden mit Verbänden und Unternehmen der Energiewirtschaft 2021 technische Eckpunkte für die Weiterentwicklung der Standards entwickelt. Die BSI-Standards wurden in Form der Aktualisierung der Technischen Richtlinie TR-03109-1 ebenfalls weiterentwickelt. Bereits zum 31. Januar 2022 konnten insgesamt drei unabhängige Hersteller eine Zertifizierung nach TR-03109-1 erfolgreich abschließen. Darüber hinaus werden 2022 mit der TR-03109-5 Mindestvorgaben an Produkte veröffentlicht, die zukünftig sicher in das HAN (Home Area Network) des Smart-Meter-Gateways angebunden werden können.

Durch den geplanten massiven Ausbau von erneuerbaren Energien und die zunehmende Vernetzung sind die Bemühungen des BSI in Zusammenarbeit mit dem BMWK, Partnerbehörden und der Branche zur Förderung des stufenweisen Rollouts von sicheren und zertifizierten Smart-Meter-Gateways weiterhin zu intensivieren und zugleich der gemeinsame Dialog zu den Zielbildern der sicheren Digitalisierung fortzuführen.

2.2.9 — Cyber-Sicherheit in der industriellen Versorgungskette

Die Digitalisierung greift entlang der industriellen Versorgungskette zwischen Hersteller, Zulieferer, Spediteur etc. immer weiter. IT-Sicherheit ist dabei von großer Bedeutung, u. a. da ein Angriff auf die digitalen Prozesse zu einer Störung der industriellen, physischen Versorgungskette führen kann.

Für viele dieser digitalen Prozesse müssen einzelne Produkte, ihre Eigenschaften und die sie betreffenden Ereignisse verfolgbar und auslesbar sein. Dies ermöglichen sogenannte Digitale Zwillinge (d. h. digitale Repräsentationen physischer Objekte), die auch IT-Sicherheitsanforderungen wie etwa Fälschungssicherheit oder Vertraulichkeit erfüllen müssen. Das BSI beteiligt sich daher an der Standardisierung eines Digitalen Zwillings. Die Aktivität läuft im Gremium DKE/AK 931.0.16 als IEC 63278 „Asset Administration Shell for Industrial Applications“.

Eine weitere Gefahr für industrielle Versorgungsketten ergibt sich durch kompromittierte Hardware und Software, die als Zulieferprodukte in die Produktionsumgebung gelangen können (vgl. Kapitel *Schwachstellen in Software-Produkten*, Seite 32). Es ist unter heutigen Bedingungen nicht möglich, jedes einzelne Zulieferprodukt einer Sicherheitsüberprüfung zu unterziehen. Eine Software Bill of Materials (SBOM), die die installierte Software eines Produktes beurkunden soll, ist leicht fälschbar. Daher zielen die Anstrengungen von Sicherheitsforscherinnen und -forschern darauf ab, die SBOM fälschungssicher zu machen und an einzelne Produkte zu binden[38].

Die digitalen Geschäftsbeziehungen, die entlang der industriellen Versorgungskette entstehen, beruhen auf einer Vielzahl von Nachweisen und Unternehmensidentitäten, die von unterschiedlichen Autoritäten ausgegeben werden können. Gemeinsam mit der Plattform Industrie 4.0 geht das BSI der Frage nach, wie sich eine rechtssichere Bindung von Nachweisen an Unternehmensidentitäten erreichen und mit digitalen Prozessen überprüfen lässt. Als wichtigen Baustein hierfür sieht das BSI die eIDAS-Verordnung, bei deren Ausgestaltung und praktischen Umsetzung das BSI mitwirkt.

2.2.10 — Moderne Telekommunikationsinfrastrukturen (5G/6G)

Mit der Einführung und Integration moderner Mobilfunkstandards sowie Technologien im Bereich 5G treten neue Bedrohungen für öffentliche und private Mobilfunknetze auf. Alte Mobilfunkgenerationen werden parallel weiterbetrieben und es entstehen hochkomplexe Netze. Das BSI hat den gesetzlichen Auftrag, für die Sicherheit dieser Netze ein Gesamtbild zu erstellen, um in Kooperation mit den beteiligten Behörden, Netzbetreibern und allen anderen Interessengruppen die Umsetzung von Sicherheitsanforderungen zu begleiten.

Mit der Umsetzung der gesetzlichen Verpflichtung zur Zertifizierung von kritischen Komponenten im 5G-Netz leistet das BSI einen wichtigen Beitrag zum Gesamtkonzept der Informationssicherheit im Mobilfunkbereich. Dazu benennt das BSI zulässige Zertifizierungsprogramme und gestaltet diese mit.

Weiterführende Informationen zu TR-03163 finden Sie hier:[s]

Das BSI entwickelte etwa ein neues 5G-Sektor-spezifisches Zertifizierungsprogramm, welches auf einem industrieübergreifenden Rahmenwerk für Sicherheit in der Mobilfunkbranche basiert. Im Berichtszeitraum wurden bereits zwei Zertifizierungen mittels des Programms umgesetzt (siehe Kapitel *Überführung der Produktzertifizierung in den europäischen Rechtsakt zur Cyber-Sicherheit*, Seite 79 und *NESAS-CCS-GI* für mehr Informationen).

Weiterführende Informationen finden Sie hier:[t]

Neben den Arbeiten zum sicheren Ausbau von Mobilfunknetzen, ist auch die Analyse von Cyber-Angriffen und Schwachstellen von essenzieller Bedeutung zur Sicherstellung der *Resilienz* von Mobilfunknetzen. Auf nationaler Ebene waren im Berichtszeitraum starke Beeinträchtigungen und größere Ausfälle lokal oder regional begrenzt und vor allem durch die Flutkatastrophe im Sommer 2021 bedingt.

Förderprogramm "Cyber-Sicherheit und digitale Souveränität in den Kommunikationstechnologien 5G/6G" des BSI

Das BSI fördert seit Juni 2022 Forschungs- und Entwicklungsvorhaben zur Stärkung der digitalen Souveränität und der Cyber-Sicherheit für 5G/6G-Kommunikationstechnologien. Die ausgewählten Projekte tragen dazu bei, dass Deutschland bei 5G/6G in der Weltspitze eine führende Rolle als Technologieanbieter einnimmt und die neuen Kommunikationstechnologien etabliert werden. Dazu werden in den Vorhaben u. a. moderne Netztechnologien entwickelt und erprobt, die das Risiko für den Einsatz von 5G/6G-Technologien senken und Sicherheitslücken schließen.

Weiterführende Informationen finden Sie hier:[u]

2.2.11 — Sicherheit von Cloud-Diensten

Cloud Computing bietet durch hohe Skalierbarkeit, Rechenleistung und Verfügbarkeit einen großen Nutzen. Ebenso wie bei klassischer Informationstechnik bestehen bei der Nutzung von Cloud-Diensten nicht nur Chancen, sondern auch spezifische Risiken. Im Jahr 2021 gab es einige größere Sicherheitsvorfälle bei Cloud-Anbietern, deren Analyse dabei helfen kann, die komplexe Cloud-Technologie sicherer zu nutzen.

Anfang des vergangenen Jahres kam es zu einem Brand bei einem Cloud-Anbieter, der zum Verlust ganzer Rechenzentren führte. Hierbei wurden auch Kundendaten zerstört. Dies zeigt, wie wichtig es ist, vor der Nutzung von Cloud-Diensten das Sicherheitsbedürfnis bezogen auf die verarbeiteten Daten genau zu analysieren. Bei der Buchung eines Cloud-Dienstes sollten dann alle zur Erfüllung dieser Bedürfnisse notwendigen Optionen mit gebucht werden.

In einem anderen Fall führte ein Hardware-Defekt dazu, dass Alarmierungssignale verschickt wurden, die fälschlicherweise auf einen Abfall der Umgebungstemperatur in einem Teil des Cloud-Rechenzentrums hinwiesen. Die gefährdeten Systeme wurden daraufhin heruntergefahren. Erst viele Stunden später konnte nach Abklärung der Ursache wieder auf die Daten zugriffen werden. Hier lag ein extrem seltener Vorfall vor. Doch eine vor der Nutzung der Cloud-Dienste durchgeführte Risikoanalyse kann zeigen, ob ein solcher Ausfall von Cloud-Diensten gravierende Folgen hätte. Wenn ja, könnte sich dieses Risiko beispielsweise durch eine Multi- oder Hybrid-Cloud-Strategie reduzieren oder gar vollständig mitigieren lassen.

Bei einem anderen großen Cloud-Anbieter konnten Sicherheitsforschende zweimal kurz nacheinander über verschiedene Cloud-Dienste Zugangsschlüssel anderer Cloud-Kundinnen und -Kunden erlangen, mit denen auf deren Daten hätte zugegriffen werden können. Die Ursachen hierfür waren ein unzureichend abgesicherter Einsatz von Drittanbietersoftware und eine fehlerhafte Konfiguration durch den Cloud-Anbieter. In beiden Fällen wurden die Schwachstellen innerhalb kurzer Zeit durch den Cloud-Anbieter behoben oder Kundinnen und Kunden darüber informiert, wie sie die Schwachstellen schließen können. Die Wahrscheinlichkeit, dass ein solcher Vorfall sehr schnell auffällt, ist sehr groß, da bei Cloud-Angeboten eine intensive Überwachung der Aktivitäten stattfindet, allein schon, um die anfallenden Kosten sekundengenau abrechnen zu können. Dennoch sollten sich Cloud-Kundinnen und -Kunden grundlegend der Risiken von geteilten Plattformen bewusst sein und je nach Sensibilität der verarbeiteten Daten zusätzliche Schutzmaßnahmen, wie beispielsweise die Verschlüsselung der Daten bei Planung der Nutzung, mit erwägen. Auch ist wichtig, dass in der Einsatzphase darauf geachtet wird, ob Schwachstellen zu dem genutzten Angebot gemeldet werden und ob hier das Einspielen eines Patches auf Kundenseite erforderlich ist, damit eventuelle Schwachstelle behoben werden.

Bei einem weiteren größeren Vorfall im letzten Jahr war ein Cloud-Anbieter direktes Ziel eines Angriffs. Den Angreifenden gelang es, innerhalb der Cloud-Umgebung einen Cloud-Dienst so zu manipulieren, dass bei dessen Einsatz *Ransomware* auf Kundensystemen installiert wurde. Solche Angriffe stellen für den Einsatz von Cloud-Diensten eine sehr ernstzunehmende Gefahr dar. Cloud-Kundinnen und -Kunden können zur besseren Absicherung darauf achten, dass der Cloud-Anbieter den Schutz der Bereitstellungsumgebung mit Sicherheitsnachweisen belegt. Darüber hinaus ist es wichtig, dass auch die an den Cloud-Dienst angeschlossene Kundenumgebung nach Stand der Technik abgesichert ist.

Dieser Überblick zu exemplarischen Vorkommnissen im vergangenen Jahr zeigt einige der möglichen Risiken bei der Nutzung von Cloud-Diensten sowie einige ausgewählte Tipps zur Absicherung dagegen. Das BSI bietet darüber hinaus verschiedene Veröffentlichungen an, die Unternehmen und Institutionen helfen, sich gegen diese und vergleichbaren Vorfälle systematisch zu wappnen.

Im IT-Grundschutz-Kompendium[39] sind Bausteine zur Absicherung der Kundenumgebung sowie zur sicheren Nutzung von Cloud-Diensten zu finden. Der BSI-Leitfaden "Sichere Nutzung von Cloud-Diensten"[40] beschreibt ausführlich Hinweise und Erläuterungen zu den Nutzerrechten und -pflichten während aller Phasen der Cloud-Nutzung. Der „Kriterienkatalog C5“[41] legt u. a. Sicherheitskriterien fest, nach denen der Cloud-Anbieter seine angebotenen Dienste absichern muss. Doch auch für Cloud-Kundinnen und -Kunden sind hier Anleitungen zu finden, was beachtet werden muss, damit die zur Verfügung gestellten Sicherheitsfunktionen auch bestmöglich eingesetzt werden können. Für Bundesbehörden ist der „Mindeststandard des BSI zur Nutzung externer Cloud-Dienste“ verbindlich anzuwenden, in welchem die einzelnen Schritte zu einer sicheren Nutzung von Cloud-Diensten dargelegt sind. Auch

Unternehmen und andere Institutionen können diese bewährten Vorgehensweisen nutzen.

Weiterführende Informationen finden Sie hier:[v]

2.2.12 — Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme

Im Zuge der Digitalisierung werden Geschäftsvorfälle heutzutage immer häufiger elektronisch erfasst. Die Nutzung unterschiedlichster Arten von Registrierkassen prägt den Einzelhandel deutlich. Von der klassischen Kasse, über Tablets und Smartphones bis hin zu Kassen in Serverfarmen sind alle erdenklichen Typen vertreten. Dadurch haben sich die technischen Herausforderungen für die Steuerprüfung stark verändert, da nachträgliche Manipulationen 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 Regelung fördert explizit eine technologieoffene Ausgestaltung der Technischen Sicherheitseinrichtung. 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.

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

Mittlerweile haben neun verschiedene Technische Sicherheitseinrichtungen die Zertifizierung 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. Vier weitere Lösungen können als sogenannte Cloud-TSE in Rechenzentren eingebunden werden. Eine Cloud-Lösung für mobile Endgeräte auf Android-Basis existiert ebenfalls.

2.2.13 — Überführung der Produktzertifizierung in den europäischen Rechtsakt zur Cyber-Sicherheit

Der europäische Rechtsakt zur Cyber-Sicherheit, der sogenannte Cybersecurity Act (CSA), ist am 27. Juni 2019 in Kraft getreten. Eines der Ziele dieser EU-Verordnung ist die Entwicklung europäischer Schemata für die Cyber-Sicherheitszertifizierung. Mit einem Zertifikat kann eine Organisation nachweisen, dass ein Produkt oder eine Dienstleistung definierten Sicherheitsanforderungen entspricht. Durch die geplante europaweite gegenseitige Anerkennung von Zertifikaten soll außerdem der digitale Binnenmarkt gestärkt werden. Unter Leitung der Agentur der Europäischen Union für Cyber-Sicherheit (ENISA) wurden zu diesem Zweck mehrere Ad-hoc Arbeitsgruppen (AHWG) gegründet. In Bezug auf die Produktzertifizierung arbeitet die AHWG für das auf Common Criteria (CC) basierte europäische Schema zur Cyber-Sicherheitszertifizierung (EUCC) bereits seit November 2019. Die AHWG zur Entwicklung des europäischen Schemas für 5G Mobilfunkausrüstung (EU5G) ist seit November 2021 aktiv.

Berichte aus den Gremien

Das SOGIS-MRA-Abkommen über die gegenseitige Anerkennung von CC-Zertifikaten in Europa wird vom EUCC-Schema abgelöst, das als erstes Schema unter dem CSA in Kraft treten wird. Im Berichtszeitraum hat das BSI in der EUCC-AHWG eine führende Rolle bei der Entwicklung des EUCC-Schemas eingenommen. Hierzu zählt seit März 2022 die aktive Teilnahme am strategisch bedeutenden Aufbau der Strukturen und Gruppen für die Aufrechterhaltung des EUCC-Schemas.

Durch die Mitarbeit in den Arbeitsgruppen konnte das BSI frühzeitig notwendige Änderungen identifizieren und Prozesse einleiten, um eine reibungslose

Umstellung auf das EUCC-Schema zu gewährleisten, sobald der entsprechende Durchführungsrechtsakt (Implementing Act) von der Europäischen Kommission verabschiedet wird. Zudem hat das BSI als eine der ersten europäischen Cyber-Sicherheitsbehörden die geforderte strikte interne Trennung von Zertifizierung und Aufsichtsführung vollzogen.

Das BSI hat als erste europäische Cyber-Sicherheitsbehörde ein nationales Zertifizierungsschema für 5G-Mobilfunkausrüstung auf der Grundlage des Network Equipment Security Assurance Scheme *(NESAS)* aufgebaut. Dieses internationale Rahmenwerk wird von der GSMA, der globalen Interessenvertretung der Mobilfunkanbieter und Hersteller, in Zusammenarbeit mit dem BSI entwickelt. Das BSI verfügt damit über das erste Zertifizierungsschema dieser Art in Europa und nimmt damit eine Vorreiterrolle bei der europäischen Harmonisierung in der EU5G AHWG ein.

Mit der Beschleunigten Sicherheitszertifizierung (BSZ) hat das BSI ein weiteres horizontales Zertifizierungsschema auf nationaler Ebene geschaffen. Die BSZ zeichnet sich durch planbare Evaluierungslaufzeiten und einen risikogetriebenen Ansatz bei der Evaluierung aus. Das BSI plant die gegenseitige Anerkennung vergleichbarer nationaler Zertifikate in Europa und entwickelt gemeinsam mit anderen Nationen einen entsprechenden europäischen Standard. Ziel ist auch hier die Schaffung eines europäischen Schemas unter dem CSA.

Zertifizierung in Zahlen

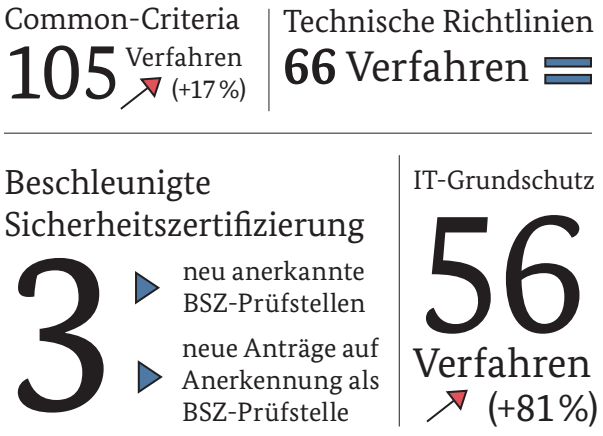


Abbildung 24: Zertifizierung in Zahlen
Quelle: Schwachstellen-Statistik

2.2.14 — IT-Grundschutz

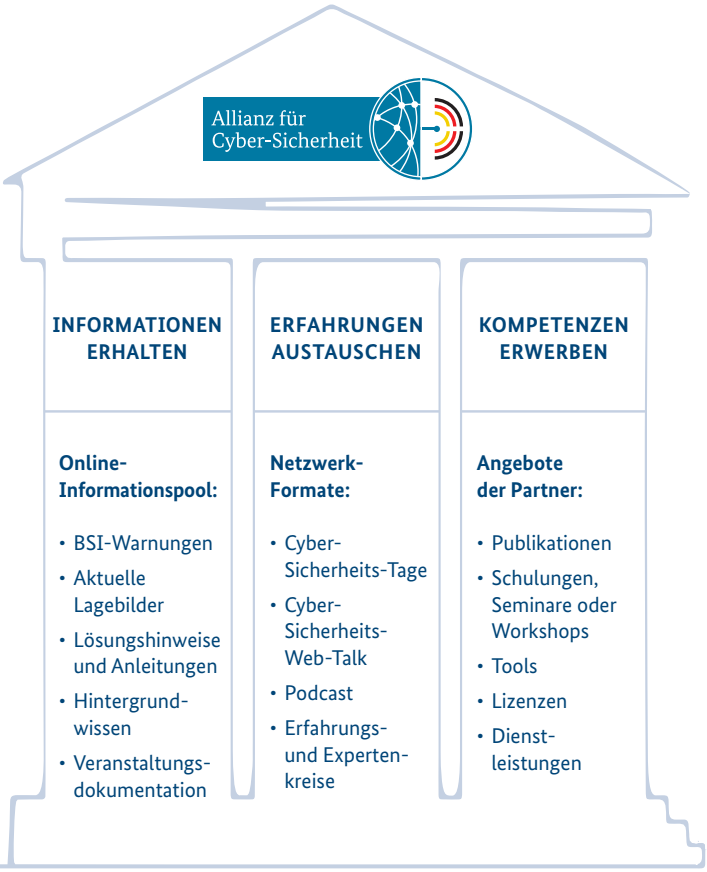
Die vielfältigen und dynamischen Angriffe, die in Kapitel 1 beschrieben werden (vgl. *Gefährdungen der Cyber-Sicherheit in Deutschland*, Seite 10), verdeutlichen einmal mehr, wie wichtig ein systematisches, ganzheitliches und pragmatisches Vorgehen zur Absicherung von digitalen Informationen ist. Der IT-Grundschutz des BSI bietet das seit rund 30 Jahren. Er basiert auf zwei Kernkomponenten: den BSI-Standards, welche die IT-Grundschutz-Methodik beschreiben, und dem IT-Grundschutz-Kompendium, das die IT-Grundschutz-Bausteine enthält. In den IT-Grundschutz-Bausteinen werden typische technische, infrastrukturelle, organisatorische und personelle Sicherheitsanforderungen zusammengefasst. Zusammen mit den BSI-Standards bieten die IT-Grundschutz-Bausteine Institutionen ein wichtiges Instrument zur Etablierung eines ISMS und somit auch zum Schutz geschäftsrelevanter Informationen.

In der Edition des IT-Grundschutzes für 2022 sind sieben neue IT-Grundschutz-Bausteine hinzugekommen, beispielsweise in den Bereichen Gebäudeautomation und Fernwartung im industriellen Umfeld. Diese neu hinzugekommenen Themen ermöglichen es, die Informationssicherheit ganzheitlich auch über die „klassische“ Büro-IT hinaus zu betrachten.

Ist Unterstützung notwendig, können Institutionen auf die Expertise der wachsenden Anzahl von ungefähr 150 ausgebildeten IT-Grundschutz-Beratern zurückgreifen. Im Jahr 2020 gab es 89 IT-Grundschutz-Berater und im Jahr 2021 bereits 140 IT-Grundschutz-Berater. Die durch das BSI zertifizierten Beraterinnen und Berater können bei der Etablierung eines ISMS nach IT-Grundschutz unterstützen. Über 3.000 Personen haben die Schulung und Prüfung zum IT-Grundschutz-Praktiker abgeschlossen. Nach 1.504 IT-Grundschutz-Praktikern im Jahr 2020 und 2.644 im Jahr 2021 bescheinigt der stetige Anstieg die Nachfrage. Die IT-Grundschutz-Praktikerinnen und Praktiker leisten in ihren Institutionen einen wichtigen Beitrag bei der Umsetzung von IT-Grundschutz und können zusammen mit IT-Grundschutz-Beraterinnen und Beratern auf Basis des IT-Grundschutzes Maßnahmen definieren und umsetzen.

Zehn Jahre ACS – Zehn Jahre ein starkes Netzwerk

Abbildung 25:
Der kooperative Ansatz der Allianz für Cyber-Sicherheit



2.2.15 — Allianz für Cyber-Sicherheit

2022 feiert die Allianz für Cyber-Sicherheit (ACS) ihr großes Jubiläum: Vor zehn Jahren wurde Europas größte Public-Private-Partnership im Bereich Cyber-Sicherheit ins Leben gerufen. Das Ziel: Kooperation und Vernetzung, um Unternehmen und Organisationen stark in der Prävention und resilient im Kampf gegen Cyber-Angriffe zu machen. Der Schlüssel zum Erfolg lag in der Idee von Kooperation und gegenseitiger Vernetzung: Eine Public-Private-Partnership sollte die Expertise und Erfahrung des BSI und der Unternehmen in Deutschland bündeln und mit Best-Practice-Produkten sowie Informationen und Handreichungen Prävention vorantreiben.

Eine Idee überzeugt – Viel Rückenwind für eine Kooperationsplattform

Der Gründungsgedanke der ACS war in der Welt. Mit dem Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien (Bitkom e.V.) fand sich ein starker Partner aus dem privaten Sektor.

Im März 2012 kündigten BSI und Bitkom e.V. auf der CEBIT in Hannover die Gründung der ACS an – die nach einer erfolgreichen Pilotphase, in der bereits viele Unternehmen als Mitglieder gewonnen und auch erste Partnerbeiträge initiiert werden konnten, offiziell auf der it-sa 2012 in Nürnberg folgte. Der kooperative Ansatz der ACS basierte von Anfang an auf diesen drei Säulen: Informationen erhalten, Erfahrungen austauschen, Kompetenzen erwerben. Darauf baut die ACS ihre Arbeit, ihr Angebot und heute, zehn Jahre nach ihrer Gründung, auch ihre Erfolgsgeschichte auf.

Denn aus der Gründungsidee ist ein starkes Netzwerk geworden. Neben den Erfahrungs- und Expertenkreisen treffen sich Deutschlands Cyber-Sicherheits-Initiativen regelmäßig unter dem Dach der ACS. Vielfältige Angebote, wie 31 Cyber-Sicherheits-Tage, neun Cyber-Sicherheits-Web-Talks, zwei hybride Veranstaltungen, 18 Podcast-Folgen und 153 Dokumente im Infopool

ermöglichen einen regen Informations- und Erfahrungsaustausch. Das Netzwerk kann auf das Know-how von über 6.400 Teilnehmern, darunter 106 Multiplikatoren sowie von 177 Partnern und deren zahlreiche Angebote zurückgreifen – und wächst kontinuierlich.

2.2.16 — Cyber-Sicherheitsnetzwerk

Das Cyber-Sicherheitsnetzwerk (CSN) ist ein freiwilliger Zusammenschluss von qualifizierten Helferinnen und Helfern, die sich bereit erklären, ihre Expertise und ihr Know-how zur Behebung von IT-Sicherheitsvorfällen zur Verfügung zu stellen.

Mit dem CSN ist es beabsichtigt, besonders für kleine und mittlere Unternehmen, aber auch für Verbraucherinnen und Verbraucher, eine wertvolle Unterstützung bei einem IT-Sicherheitsvorfall bereitzustellen. Das BSI bildet den Rahmen für die Initiative. Das Netzwerk bietet zahlreiche Angebote, um sich auf einen Vorfall vorzubereiten und im Worst Case handlungsfähig zu sein, denn ein solcher Vorfall kann eine existenzbedrohende Situation für ein Unternehmen bedeuten.

Das CSN steht als erste Anlaufstelle bei IT-Sicherheitsvorfällen zur Verfügung und bietet eine effiziente Unterstützung. Je nach IT-Sicherheitsvorfall stellt sich die Frage: Wer kann wie helfen? Das CSN hat hierfür die Digitale Rettungskette als eine Kernkomponente entwickelt. Sie legt ein abgestimmtes Arbeiten der Helfer im CSN fest. Das ermöglicht eine Kette unterschiedlicher, reaktiver Hilfsangebote, beginnend bei Identifizierung eines geeigneten Helfers, über Hilfestellungen, bis hin zur umfassenden Lösungsbetreuung und Vorfallklärung. In einer Pilotphase wird die Digitale Rettungskette erprobt und kontinuierlich erweitert.

Eine qualitativ hochwertige Vorfallbearbeitung der Helferinnen und Helfer wird durch ein einheitliches und qualitätsgesichertes Qualifizierungsprogramm sichergestellt. Das Angebot eines Erfahrungsaustauschs in regionalen Foren oder das jährlich stattfindende Forum des CSN runden die Angebotspalette ab.

Weiterführende Informationen zum Basiskurs finden Sie hier:[w]

Mit den regionalen Foren bietet das CSN sowohl Unternehmen als auch den Helferinnen und Helfern die Möglichkeit, in einer gesicherten Umgebung die Bewältigung eines Vorfalls zu trainieren. Als Begleitmaterial zu den Foren stellt das CNS einen Trainingskoffer mit einer kostenfreien Übungs- bzw. Spielsammlung zur Verfügung.

Kurzprofil des CSN

Abbildung 26:
Kurzprofil des CSN

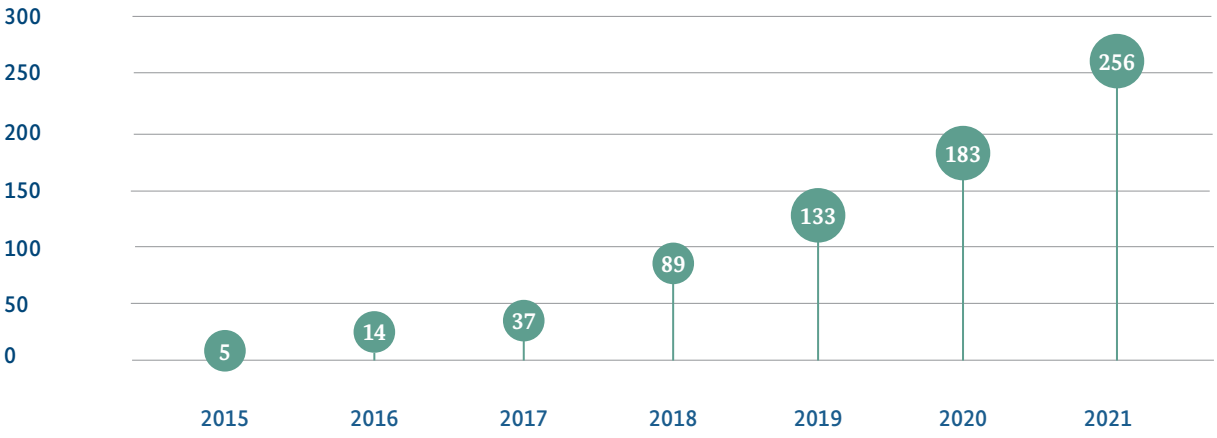
2.2.17 — Sonstige Lösungen für die Wirtschaft

Investitionsprüfung

Das BSI wird vom BMI zur Abwehr potenzieller Gefahren bei Investitionen in inländische Unternehmen und Produktionsstätten durch ausländische Investoren nach §§ 4ff. des Außenwirtschaftsgesetzes (AWG) bzw. §§ 55ff. und §§ 60ff. der Außenwirtschaftsverordnung (AWV) beteiligt. Federführend für den Bund ist das BMWK für die AWG-Verfahren zuständig. Das BSI wird bei Verfahren mit einem möglichen Cyber-Sicherheitsbezug durch das BMI zur Gefahrenbewertung bzw. -abwehr beteiligt und erhält hierzu entsprechende Prüfaufträge (Erlasse). Um den offenen Kapitalverkehr durch die Verfahren nicht unnötig zu belasten, führte das BSI die teilweise sehr komplexen Einzelprüfungen sehr zügig durch, d. h. im Regelfall innerhalb von wenigen Arbeitstagen bis zu maximal ein oder zwei Arbeitswochen.

AWG-Erlasse 2015-2021
Anzahl

Abbildung 27:
AWG-Erlasse 2015-2021
Quelle: BSI



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 liegen, dem Einbau oder der Verheimlichung von Schwachstellen, der Gefährdung von kritischen Infrastrukturen oder dem Verlust von Technologieträgern im Bereich von Schlüsseltechnologien (z. B. Halbleiter oder Künstliche Intelligenz). 2021 war das BSI beispielsweise am Verfahren bzw. Erwerb eines der weltweit führenden Zulieferer der Halbleiterindustrie beteiligt und hat dort seine technische Expertise eingebracht.

Seit 2015 hat sich entsprechend der Steigerung der Investitionsprüfungen auch das Aufkommen von Prüfaufträgen durch das BMI im Rahmen von AWG-Verfahren enorm gesteigert, d. h. 2021 wurden 256 Erlasse durch das BSI bearbeitet, 2015 waren es noch fünf. Die hier zu verzeichnende enorme Zunahme von Prüfvorgängen setzte sich auch 2022 weiter fort und im Laufe des Jahres werden weitere Rekordwerte erwartet. Die Gründe hierfür liegen in der erweiterten rechtlichen Prüfgrundlage, der Beteiligung an EU-Investitionsverfahren sowie der erhöhten öffentlichen Sensibilität hinsichtlich handelspolitischer Auswirkungen auf die nationale Sicherheitslage und technologische Souveränität (siehe *Die Lage der IT-Sicherheit in Deutschland 2021*).

Marktaufsicht

Im September 2021 begann der Aufbau der Marktaufsicht über zertifizierte Dienstleister und Produkte im BSI. Auf der Grundlage des § 9c Abs. 8 BSIG kann die Marktaufsicht stichprobenartig, anlasslos oder anlassbezogen die von den Herstellern zugesicherten Eigenschaften aller zertifizierten und gekennzeichneten Produkte und Dienstleistungen im BSI prüfen. Ziel ist die Erkennung und schnellstmögliche Beseitigung von Schwachstellen, um die IT-Sicherheit in Deutschland weiter zu stärken.

Mit der Vergabe der ersten IT-Sicherheitskennzeichen sind bereits im März 2022 die ersten formellen und anlassbezogenen Amtshandlungen erfolgt. In Vorbereitung auf die Implementierung des CSA ist die Marktaufsicht im Aufbau der nationalen Aufsichtsbehörde (National Cybersecurity Certification Authority, NCCA) involviert. Nach der Implementierung wird auch für die im Rahmen des CSA vergebenen Zertifikate die Aufsicht übernommen werden.

2.3 — Staat und Verwaltung

Eine Kernaufgabe des BSI ist die Abwehr von Cyber-Angriffen auf Regierungsnetze und die Bundesverwaltung. Für Behörden bei Bund, Ländern und Kommunen stellt das BSI ein breites Angebot zur Erhöhung der Informationssicherheit zur Verfügung: Die Basis bilden die Informationssicherheitsberatung, IT-Grundschutz und Mindeststandards sowie Zertifizierung und Zulassung. Bei IT-Sicherheitsvorfällen unterstützen *CERT-Bund*, mobile Einsatzteams (MIRT) oder das Nationale Cyber-Abwehrzentrum betroffene Behörden. Zentraler Ansprechpartner für Länder und Kommunen ist das nationale Verbindungswesen des BSI. Verbindungsstellen befinden sich in Hamburg, Berlin, Bonn, Wiesbaden und Stuttgart.

2.3.1 — Die Gefährdungslage in der Bundesverwaltung

Die Regierungsnetze sind tagtäglich Angriffen aus dem Internet ausgesetzt. Neben überwiegend ungezielten Massenangriffen finden sich hierbei auch gezielte Angriffe auf die Bundesverwaltung. Das BSI setzt verschiedene, sich gegenseitig ergänzende Maßnahmen zum Schutz der Regierungsnetze vor diesen Angriffen ein.

Eine präventive Komponente stellen Webfilter dar, die den Zugriff auf Webseiten oder die Verbindung zu Webservern blockieren, die mit Schadprogrammen im Zusammenhang stehen. Dadurch wird zum Beispiel der Zugriff auf hinter Download-Links versteckte Schadprogramme, die im Rahmen von Social-Engineering-Angriffen über E-Mail, Social-Media oder Webseiten verbreitet werden, verhindert. Auch die Kommunikation von Schadsoftware mit den entsprechenden Webservern, zum Beispiel zum Nachladen von weiteren Komponenten oder Befehlen, wird unterbunden. Im aktuellen Berichtszeitraum mussten rund 78.000 *maliziöse* Webseiten zusätzlich gesperrt werden. Während die Anzahl der monatlich gesperrten Webseiten von Juni 2021 bis Februar 2022 relativ stabil blieb, hat sich die Bedrohungseinschätzung im März 2022 vor dem Hintergrund des russischen Angriffskrieges gegen die Ukraine deutlich verändert, sodass spürbar mehr *maliziöse* Webseiten für den Zugriff aus der Bundesverwaltung gesperrt werden mussten. Der Index sprang binnen Monatsfrist um 158 Prozent auf 353 Punkte (vgl. Abbildung 28) – der höchste Wert seit Beginn der Aufzeichnungen.

Direkt in E-Mail-Anhängen versendete Schadprogramme werden mittels automatisierter Antivirus-Schutzmaßnahmen erkannt und die Zustellung zum Empfänger gestoppt. Dies betraf im Berichtszeitraum durchschnittlich 34.000 E-Mails pro Monat. Nach einer sehr starken Angriffswelle im vorangegangenen Berichtszeitraum und der Abschaltung der Emotet-Infrastruktur Ende Januar 2021 zeigt der „Index über Schadprogramm-Angriffe auf die Bundesverwaltung“ zunächst eine Normalisierung des Niveaus. Im März 2022 markiert sodann ein deutlicher Ausschlag des Indikators den sprunghaften Anstieg von Emotet-Spam (vgl. Abbildung 29). In dem Botnetz waren bereits seit Herbst 2021 wieder Aktivitäten zu beobachten, die sich seit März 2022 spürbar verstärkten.

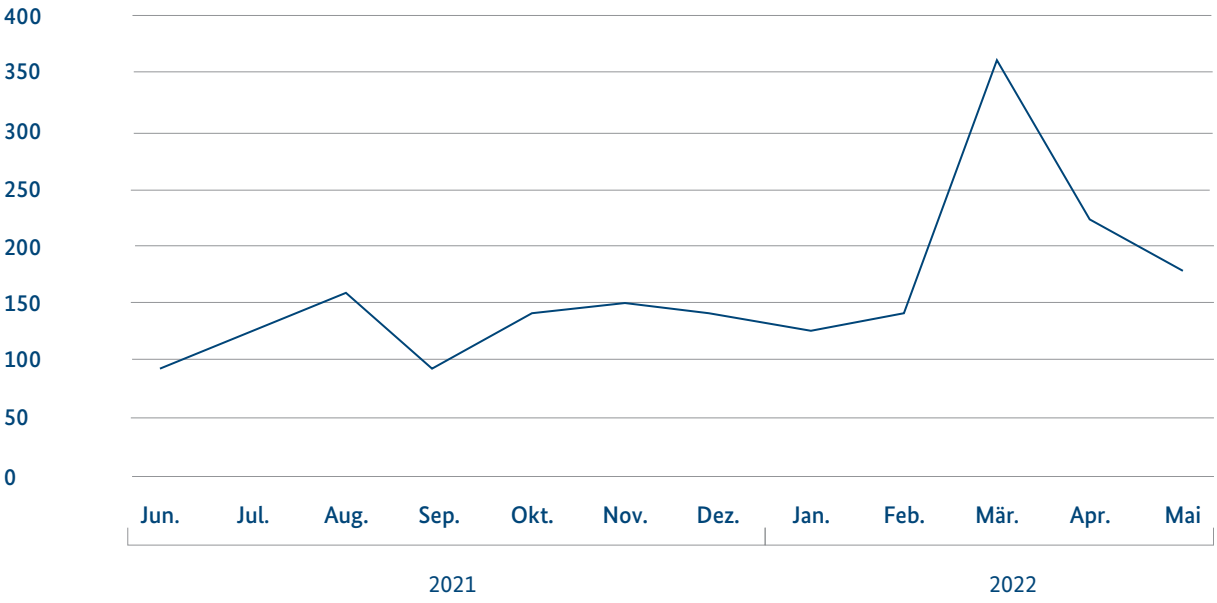
Rund 5.200 E-Mails pro Monat wurden ausschließlich auf Basis von eigens durch das BSI erstellter Antivirus-Signaturen als schädlich identifiziert. Insbesondere um gezielte Angriffe auf die Bundesverwaltung erkennen zu können, betreibt das BSI zusätzlich zu den bereits beschriebenen Maßnahmen nachgelagert ein System zur Detektion von Schadprogrammen im Datenverkehr der Regierungsnetze. Mit einer Kombination von automatisierten Testverfahren und manueller Analyse konnten die Analystinnen und Analysten des BSI durchschnittlich weitere knapp 2.500 Angriffe pro Monat identifizieren, die weder durch eine kommerzielle noch durch eine der oben genannten automatisierten Lösungen erkannt wurden.

Ergänzend wird die Sicherheit der Regierungsnetze mit einem zentralen Schutz vor 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. Aufkommen und Entwicklung der Spam-E-Mails in den Netzen des Bundes werden durch den Spam-Mail-Index gemessen. Dieser erreichte im Berichtszeitraum durchschnittlich 111 Punkte. Im vergangenen Berichtszeitraum hatte der Indikator noch bei 114 Punkten gelegen. Dabei waren teils erhebliche Schwankungen zu verzeichnen. Während das Spam-Aufkommen im Spätsommer und Herbst 2021 auf unterdurchschnittlichem Niveau lag, sprangen die Index-Werte im Dezember 2021 und insbesondere im Februar 2022 deutlich nach oben.

Die Gefährdungslage in der Bundesverwaltung
2018=100

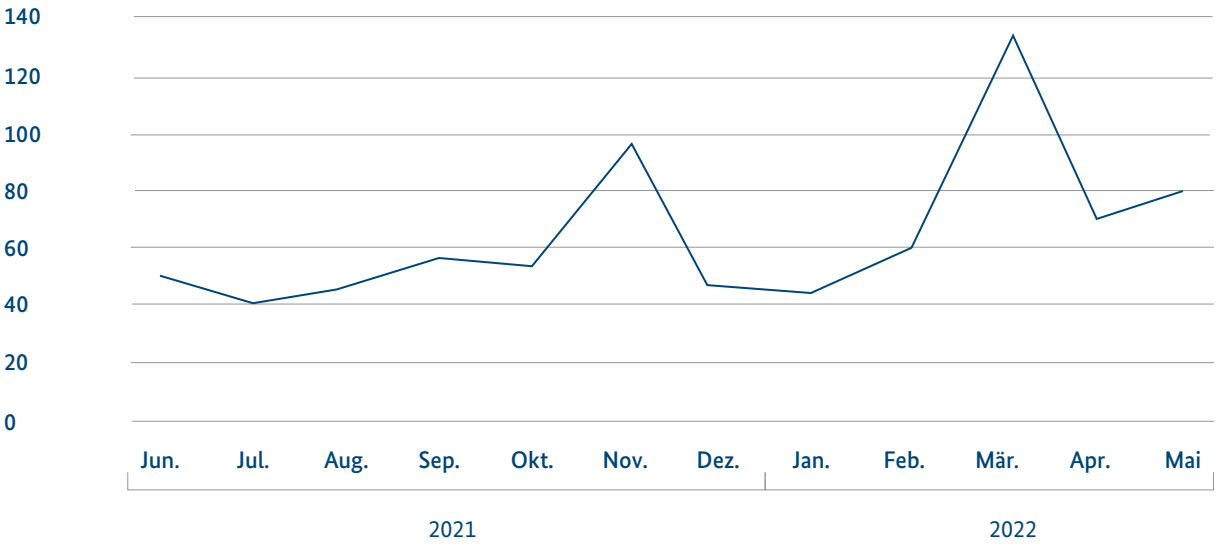
Abbildung 28:
Index über die neuen Sperrungen maliziöser Webseiten
Quelle: Webfilter-Messung



Index über die Malware-Angriffe auf die Bundesverwaltung[1]

[1]ohne Angriffe auf Behörden, die nicht an den zentralen Schutzmaßnahmen des BSI teilnehmen

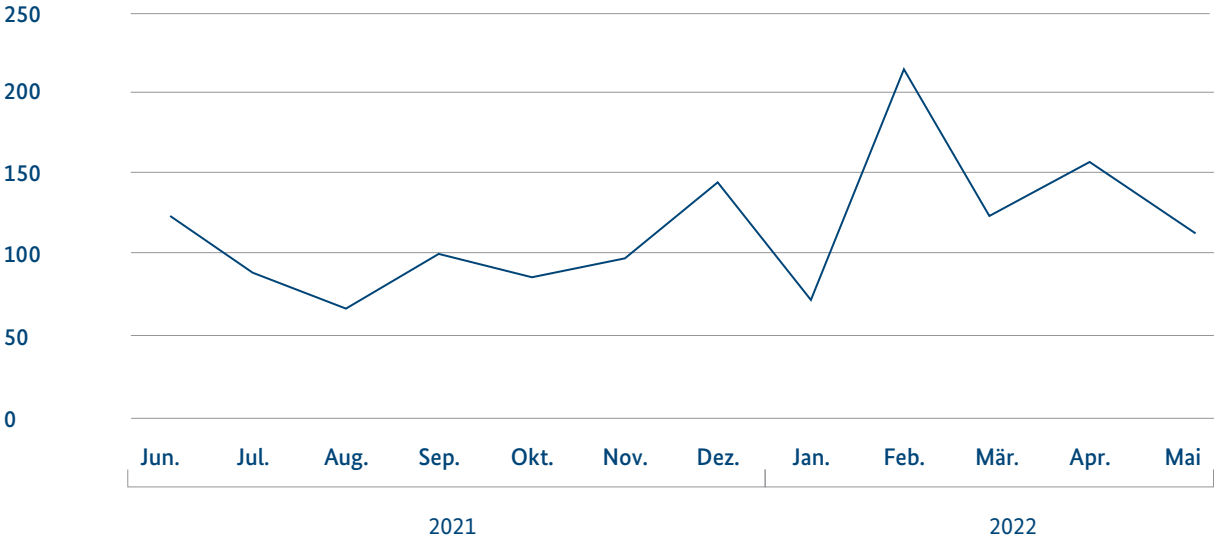
Abbildung 29:
Quelle: Erhebung über die Malware-Angriffe auf die Bundesverwaltung



Spam-Mail-Index für die Bundesverwaltung[1]
2018=100

Abbildung 30:
Quelle: Erhebung über den E-Mail-Verkehr mit der Bundesverwaltung

[1]Ohne Spam-Mails an Behörden, die nicht an den zentralen Schutzmaßnahmen des BSI teilnehmen



Im Dezember 2021 trieb eine Sextortion-Kampagne im Anschluss an die Onlineshopping-Events Black Friday und Cyber Monday die Werte nach oben (vgl. auch Kapitel *Spam und Phishing*, Seite 26). Die Spam-Filter der Bundesverwaltung wehren solche Spam-Wellen zuverlässig ab, sodass sie die adressierten Nutzerinnen und Nutzer nicht erreichen.

2.3.2 — Computer Emergency Response Team für Bundesbehörden

Mit den Fachreferaten des *Computer Emergency Response Team* des Bundes *(CERT-Bund)* ist das BSI die zentrale Anlaufstelle für präventive und reaktive Maßnahmen mit Bezug auf sicherheits- und verfügbarkeitsrelevante Vorfälle in Computersystemen. Um diesen vielfältigen Aufgaben gerecht zu werden, ist das *CERT-Bund* 2021 zu einem eigenständigen Fachbereich mit fünf Referaten ausgebaut worden: Grundsatz und Warn- und Informationsdienst (WID), Vorfallsbearbeitung und Verbindungsstelle Nationales Cyber-Abwehrzentrum, Mobile Incident Response Team (MIRT), Technische Analyse sowie Industrielle Steuerungs- und Automatisierungssysteme. Diese bearbeiten ein breites Themenspektrum, das zum Beispiel Cyber-Sicherheitswarnungen, den Prozess der Schwachstellenkoordinierung (CVD) (vgl. Kapitel *Schwachstellen in Software-Produkten*, Seite 32) oder auch die Vorfallsbearbeitung und die *CERT-Bund* Reports umfasst. Zu Vor-Ort-Einsätzen durch das MIRT kommt es nur bei herausgehobenen Fällen nach § 5b BSIG. Solche liegen insbesondere dann vor, wenn es sich um Angriffe von besonderer technischer Qualität handelt oder die zügige Wiederherstellung der Sicherheit oder Funktionsfähigkeit der betroffenen informationstechnischen Systeme von besonderem öffentlichen Interesse sind.

Daneben engagiert sich *CERT-Bund* weiterhin sehr aktiv in verschiedenen CERT- bzw. Cyber-Sicherheits-Communities.

Mit dem IT-SiG 2.0 hat das BSI die Befugnis erhalten, gemäß § 7b BSIG IP-Adressen von Einrichtungen des Bundes, Kritischen Infrastrukturen, digitalen Diensten und Unternehmen im besonderen öffentlichen Interesse anlassbezogen auf Schwachstellen zu prüfen. Dementsprechend wurden erste Port-Scans von 2.298 IP-Adress-

blöcken mit mehr als einer Million IP-Adressen der mittelbaren und unmittelbaren Bundesverwaltung durchgeführt. Die Ergebnisse werden nun zusammen mit den betroffenen Behörden verifiziert. Erste Verbesserungen ließen sich bereits identifizieren und entsprechende Maßnahmen einleiten. Darüber hinaus ist, wie bereits beschrieben, die Verbindungsstelle zum Nationalen Cyber-Abwehrzentrum beim *CERT-Bund* angesiedelt. Dabei stellt das BSI die Räumlichkeiten und die Infrastruktur für das Nationale Cyber-Abwehrzentrum zur Verfügung und trägt aktiv zu dessen Weiterentwicklung bei. Aufgrund der Verankerung in *CERT-Bund* können zum Beispiel kurze Wege bei der Zusammenarbeit mit den anderen Sicherheitsbehörden bei Vorfällen realisiert werden.

Im Berichtszeitraum gab es mehrere herausgehobene Ereignisse wie etwa Log4Shell (vgl. Vorfall *Log4j: Schwachstelle in quelloffener Bibliothek*, Seite 37) und den russischen Angriffskrieg gegen die Ukraine (vgl. *Cyber-Sicherheitslage im Kontext des russischen Angriffskrieges gegen die Ukraine*, Seite 45), die zu einem deutlich erhöhten Arbeitsaufkommen geführt haben. Dies zeigt sich zum Beispiel sowohl bei den Cyber-Sicherheits-Warnungen als auch bei den aufgewendeten Personentagen im Bereich der Vorfallsbearbeitung.

2.3.3 — Nationales Verbindungswesen

Die Gestaltung der Informationssicherheit in der Digitalisierung für die Verwaltung kann nur gemeinsam von Bund und Ländern zum Erfolg geführt werden. Aus diesem Grund hat das BSI seine Unterstützungsmöglichkeiten für die Länder weiter ausgebaut und fördert die Zusammenarbeit auf verschiedenen Ebenen. Übergeordnetes Ziel der Zusammenarbeit ist es, ein einheitlich hohes IT-Sicherheitsniveau in Deutschland zu schaffen.

Das Nationale Verbindungswesen mit seinen Verbindungsstellen in Berlin, Bonn, Hamburg, Stuttgart und Wiesbaden erleichtert durch seine direkten Ansprechpartnerinnen und Ansprechpartner für alle 16 Bundesländer den Austausch erheblich und trägt so wesentlich zu einer verstärkten Kooperation bei. Über die 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 in den Kooperationsvereinbarungen wider, die seit Ende 2021 sukzessive mit den Ländern geschlossen werden. Auf dieser Basis werden konkrete Kooperationsprojekte umgesetzt, die das Cyber-Sicherheitsniveau in Bund und Ländern maßgeblich erhöhen.

2.3.4 — Zusammenarbeit mit Ländern und Kommunen

Mit dem Land Niedersachsen wurde 2021 die erste Kooperationsvereinbarung zum Ausbau der Bund-Länder-Zusammenarbeit unterzeichnet. Hierbei wurden insgesamt 17 Kooperationsfelder identifiziert, u. a. die gegenseitige Unterstützung bei herausgehobenen Cyber-Sicherheitsvorfällen. Darüber hinaus arbeitet das BSI in unterschiedlichen Themenfeldern, beispielsweise in den Bund-Länder-Gremien, mit den Ländern zusammen und bietet diesen auf vielfältige Weise, beispielsweise durch Beratung, Unterstützung an. Da Cyber-Bedrohungen nicht an Ländergrenzen haltmachen, baut das BSI die Zusammenarbeit in diesem Bereich fortlaufend aus.

Eine effiziente Zusammenarbeit mit den bundesweit fast 11.000 Kommunen erfordert strukturierte Ansätze, die nur gemeinsam mit Multiplikatoren aus den kommunalen Spitzenverbänden und Institutionen der Länder erfolgen können. Ziele sind dabei insbesondere die Sensibilisierung der Management-Ebene und Unterstützung der operativen Ebene bei der Umsetzung von Informationssicherheit. Dabei steht neben der gemeinschaftlichen Erstellung von IT-Grundschutzprofilen auch die Bereitstellung von skalierbaren Handreichungen für den Einstieg und Umsetzung des IT-Grundschutzes im Fokus.

Gemeinsam mit den Ländern und den kommunalen Spitzenverbänden nimmt das BSI regelmäßig an Kongressen und Tagungen teil und erstellt Fachbeiträge. Des Weiteren werden Informationsveranstaltungen konzipiert und durchgeführt.

So wurde 2021 die Roadshow Kommunen im BSI konzipiert und vorbereitet. Hierbei handelt es sich um eine virtuelle Veranstaltungsreihe für die Zielgruppe Kommunen, die ab 2022 gemeinsam mit interessierten Ländern durchgeführt wird.

2.3.5 — Cyber-Sicherheit von Landtagswahlen

Wahlen besitzen in Demokratien einen hohen Stellenwert, denn diese sind der Ausgangspunkt jeglicher Legitimation für Regierungen und parlamentarisches Handeln. Nach dem „Superwahljahr 2021" finden im Jahr 2022 vier Landtagswahlen statt. Neben drei weiteren Landtagswahlen folgt 2023 mit der Sozialwahl eine bundesweite Wahl. Cyber-Angriffe mit Wahlbezug in anderen Ländern zeigen, dass staatliche und nichtstaatliche Akteure versuchen, demokratische Prozesse anzugreifen, sie zu stören oder gar zu sabotieren. Beispiele, u. a. in Frankreich und im Vereinigten Königreich, führen die Gefährdung von Wahlen durch Cyber-Angriffe vor Augen: Bei dem sogenannten Macron-Hack hatten Angreifer einen Tag vor der Stichwahl bei den Präsidentenwahlen 2017 mehr als 20.000 gestohlene E-Mails aus dem Wahlkampfteam eines der Kandidaten veröffentlicht. 2019 wurden durch „Hack & Leak" vertrauliche Dokumente zum Freihandelsabkommen zwischen den USA und UK im Vorfeld der General Elections geleakt, um die Wahl zu beeinflussen.

Neben staatlich gesteuerten Angriffsversuchen, die sich gezielt sowohl gegen das Wahlumfeld als auch den öffentlichen Meinungsbildungsprozess richten (vgl. Kapitel *Advanced Persistent Threats*, Seite 38), bedrohen auch Cybercrime-Aktivitäten, wie Ransomware-Angriffe (vgl. Kapitel *Ransomware*, Seite 13) 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. Prozesse werden zunehmend digitalisiert. Dieser Trend wird 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. Institutionen und Akteure veröffentlichen im Rahmen ihrer Kommunikation mit den Bürgerinnen und Bürgern bzw. Wählerinnen und Wählern bewusst öffentliche Informationen, wie Wahlprogramme oder Informationen zum Wahlablauf, digital. Zugleich verarbeiten sie auch interne, nichtöffentliche Daten, die nur für einen eingeschränkten Beteiligtenkreis vorgesehen und freigegeben sind. Diese Daten gelten in unterschiedlichster Form als schützenswert. Verfügbarkeit, Vertraulichkeit, Integrität sowie Authentizität der Informationen in diesem Bereich können bedroht sein.

Entsprechend der föderalen, rechtlichen Rahmenbedingungen unterstützt das BSI auch die Absicherung der Landtagswahlen durch unterschiedliche Angebote.

- Zur Absicherung des formalen Wahlprozesses und seiner IT-Unterstützung steht das BSI den Landeswahlleitungen als Ansprechpartner zur Verfügung. Für die zahlreichen an den Wahlen beteiligten Parteien sowie 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.

- 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.

2.3.6 — Informationssicherheitsberatung

Die Informationssicherheitsberatung für den Bund berät die Stellen des Bundes zu allen Fragen der Informationssicherheit. Schwerpunkte bilden dabei der Aufbau, der Erhalt und die Verbesserung des Informationssicherheitsmanagements. Zudem besteht eine weitere Aufgabe der Sicherheitsberatung in der Bearbeitung von Grundsatzangelegenheiten.

Ein wesentlicher Schwerpunkt der Arbeiten lag im Berichtszeitraum auf der Absicherung des Wahlprozesses. So wurden Fraktionen, Kandidierende und Parteien in Fragen der Informationssicherheit beraten. Unterstützend hat die Informationssicherheitsberatung den IT-Sicherheitsleitfaden für Kandidierende bei Bundes- und Landeswahlen bereitgestellt. Die Pandemie setzte im Jahr 2021 ein weiteres Thema: Die Informationssicherheitsberatung hat das Informationssicherheitskonzept für den digitalen Impfnachweis geprüft. Zudem wurde durch eine intensive Zusammenarbeit mit der Bundesakademie für öffentliche Verwaltung die Aus- und Weiterbildung von Informationssicherheitsbeauftragten unterstützt.

2.3.7 — Geheimschutzberatung zu VS-IT

Nach den gesetzlichen Regelungen wirkt das BSI bei der Umsetzung der Allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung, VSA) mit. Die Modernisierung der VSA 2018 sollte insbesondere der fortschreitenden Digitalisierung im Geheimschutz Rechnung tragen. Seitdem ist der Bedarf an Beratung und Prüfung zu technisch innovativen Digitalisierungsprojekten mit Geheimschutzrelevanz erheblich gestiegen. Großprojekte wie gegenwärtig z. B. die IT-Konsolidierung Bund, Ressortübergreifende VS-Kommunikation, ebenenübergreifende VS-IT-Projekte etc. sowie perspektivisch weitere Digitalisierungsvorhaben bringen einen sich stetig erhöhendem Beratungs- und Prüfaufwand, mit sich, insbesondere in der VS-IT-Sicherheit. Um diese Herausforderungen noch effizienter zu meistern, erfolgte mit der Umorganisation des BSI zum 13. Dezember 2021 eine Aufteilung der bisherigen Geheimschutzberatung nach den beiden zentralen Handlungsfeldern – VS-IT einerseits und materielle Sicherheit andererseits.

Die Geheimschutzberatung zu VS-IT berät und unterstützt die Stellen des Bundes im Geltungsbereich der VSA und andere öffentliche Stellen auf Ersuchen zu VS-IT. Schwerpunktmäßig begleitet die Geheimschutzberatung Digitalisierungsvorhaben mit besonderer strategischer und politischer Bedeutung. Neben der Beratung werden auch in bestimmten Fällen Freigabeprüfungen durchgeführt und Freigabevoten zur Konzeption und zum Betrieb von VS-IT erstellt. Diese sind dann entscheidende Voraussetzung für die Sicherstellung eines ganzheitlichen und einheitlichen Geheimschutzes.

Im Berichtszeitraum waren wesentliche Aufgaben unter anderem Prüfungen im Zusammenhang mit Freigaben von VS-IT und die Erstellung von Freigabevoten für verschiedene komplexe IT-Projekte des Bundes, wie beispielsweise die E-Akte Bund und die Betriebsplattform Bund. Zusätzlich wurde die Aufnahme eines IT-Grundschutzbausteins für den Geheimschutz in das IT-Grundschutzkompendium initiiert, um die operative Umsetzung der Geheimschutzanforderungen in den Behörden zu erleichtern. Weiterhin wurde die Mitarbeit in Gremien der NATO im Bereich VS-IT intensiviert und durch eine intensive Zusammenarbeit mit der Bundesakademie für öffentliche Verwaltung (BAKöV) die Aus- und Weiterbildung von Geheimschutzbeauftragten und deren Mitarbeitenden sowie VS-Registratoren unterstützt.

2.3.8 — 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 Schengenraums. Hierzu werden das europäische Ein-/Ausreiseregister (Entry-Exit-System, EES) und das europäische Reiseinformations- und Reisegenehmigungssystem (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 gehandhabt. Neben der Erhöhung der Sicherheit im Schengenraum, insbesondere im Kontext grenzüberschreitender Kri-

minalität, illegaler Migration und Epidemien, ist ein weiteres Ziel dieses Vorhabens unter anderem die Etablierung effizienterer Grenzkontrollprozesse.

Initial im Rahmen der Flüchtlingskrise 2015 vorangetrieben, haben die Zielsetzungen der europäischen Register auch heute nichts an Aktualität verloren. Stets zu wissen, wer die Grenze des Schengenraumes übertritt, wer bereits in einem EU-Staat Asyl beantragt hat und wer gegebenenfalls eine Gefahr für die öffentliche Sicherheit darstellt, sind nicht zuletzt in der aktuellen Flüchtlingsbewegung vielfach geäußerte Bedarfe – jedoch auch Kernaspekte bei der Novellierung der europäischen Registerlandschaft. Auch die sichere und zeiteffiziente biometrische Registrierung von Geflüchteten ist eine aktuelle Herausforderung, zu deren Bewältigung das BSI durch die Aufbereitung des aktuellen Standes der Technik in den technischen Richtlinien beiträgt. Mit den sich erholenden Passagierzahlen im Luftverkehr gewinnen auch Themen wie die Bekämpfung grenzüberschreitender Kriminalität und illegaler Migration sowie der Bedarf an einer effizienten Grenzkontrolle wieder an Bedeutung.

Das BSI gestaltet die Umsetzung der genannten europäischen Vorhaben sowohl auf europäischer als auch nationaler Ebene aktiv mit. Bei der europäischen Arbeit an den weiterführenden Rechtsakten behielt das BSI die Sicherheit digitaler Identitäten im Blick und wies auf logische Schwachstellen in systemübergreifenden Prozessen des europäischen Identitätsmanagements hin. National wurde im November 2021 die Version 5.2 der technischen Richtlinie BSI TR-03121 veröffentlicht, welche erstmalig ein eigenes Volume für die Anwendungsfälle in Ausländerbehörden beinhaltet und als Grundlage für zukünftige Ausschreibungen dienen kann. Ebenso wurde 2022 mit weiteren Bundesbehörden unter Federführung des BSI ein Leitfaden für die Prozesse des digitalen hoheitlichen Identitätsmanagements beim Umgang mit den neuen europäischen Registern fortgeschrieben. 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, national und international, zu unterstützen.

2.3.9 — Technologieverifikation in sogenannten Technologie Labs

Das BSI untersucht spezifische IT-sicherheitstechnische Fragestellungen bei Produkten ausgewählter Hersteller bis hinunter auf die Ebene des *Quellcodes*. Mit dem dadurch gewonnenen, vertieften Technologieverständnis können Lösungen zu den unterschiedlichsten Aspekten erarbeitet werden. Im Berichtszeitraum ließ sich ein Teil der geplanten Vor-Ort-Prüfungen aufgrund der Corona-Lage nicht durchführen. Sämtliche im Ausland geplanten Prüftermine wurden ausgesetzt. Zudem war eine Anreise zu den in Bonn liegenden Security Labs nur eingeschränkt möglich. Prüfungen in Bonn fanden daher in reduziertem Umfang statt. Aus diesem Grund wurden vermehrt Online-Workshops und konzeptionelle Arbeiten durchgeführt.

Alle genannten Ziele können nur mit Unterstützung der Hersteller erreicht werden. Aus diesem Grund wird nur in langfristige Kooperationen investiert.

2.3.10 — App-Testing für mobile Lösungen

Applikationen auf mobilen Geräten erweitern die Funktionalität des Grundsystems und spielen eine wesentliche Rolle für den Erfolg von mobilen Lösungen. Der Einsatz von Apps birgt jedoch Sicherheitsrisiken sowohl für die Sicherheit der verarbeiteten Daten als auch für die Sicherheit der Gesamtlösung. Diese Sicherheitsrisiken müssen bewertet werden, um eine Gesamtaussage zur Sicherheit einer mobilen Lösung treffen zu können.

Der vom BSI zur Verfügung gestellte App-Testing-Dienst für Bundesbehörden, der zusammen mit der Firma Deutsche Telekom Security GmbH erbracht wird, bietet eine wesentliche Entscheidungsgrundlage für die jeweils Verantwortlichen, ob und unter welchen Bedingungen sich eine App einsetzen lässt. Damit wird eine größtmögliche Flexibilität beim Einsatz zusätzlicher benötigter Apps auf dienstlich bereitgestellten Geräten bei gleichzeitiger Gewährleistung einer grundlegenden IT-Sicherheit erreicht.

Bei den App-Prüfungen werden sowohl sicherheitstechnische als auch datenschutzrelevante Aspekte berücksichtigt. Die Prüfberichte enthalten zudem gegebenen-

Eckpunkte des Technologie-Verifikations-Programms:

- *Fokus liegt auf technischen (nicht politischen) Themen.*
- *Es gilt der Grundsatz der Gleichbehandlung aller Hersteller.*
- *Technisches Know-how bei ausgewählten Schlüsseltechnologien wird vertieft.*
- *Enge Zusammenarbeit mit den Forschungsabteilungen des Herstellers, um aktiv bei der Gestaltung der Informationssicherheit neuer Technologien mitzuwirken, um Sicherheitsstandards branchenweit zu etablieren.*
- *Arbeit findet in lokalen und in internationalen Security Labs statt, um sowohl den Informationsfluss zu optimieren als auch lokale Source-Code-Analysen zu ermöglichen.*
- *Durchführung der Prüfungen immer durch BSI-Personal. Unterstützung durch 3rd-Party-Labs ist jedoch jederzeit möglich. Rechtliche Grundlage der Prüfungen ergibt sich aus dem § 7a Abs. 1 BSIG.*
- *Zu Anfang steht immer die Evaluation der Schlüsseltechnologie. Nachgelagerter Sourcecode-Review dient lediglich zur Verifizierung einer korrekten Implementierung im konkreten System.*
- *Gewonnenes Verständnis wird bei Bedarf in technischen Richtlinien veröffentlicht und zur Erstellung eines einheitlichen Prüfkatalogs verwendet.*
- *Zusammenhang zwischen der verifizierten Schlüsseltechnologie und den operativen Netzen von Bedarfsträgern wird hergestellt.*
- *Risikobasierter Ansatz: Es geht hauptsächlich darum, Detektionsmöglichkeiten zu verbessern, anstatt Angriffe gänzlich zu verhindern.*
- *Regelmäßiger technischer Austausch mit internationalen Herstellern der Informations- und Kommunikations-Industrie.*

falls Hinweise und Empfehlungen an die Nutzerinnen und Nutzer, welche Einstellungen oder Randbedingungen für eine möglichst sichere Nutzung der betreffenden App beachtet werden sollten.

Sofern im Einzelfall erforderlich, wird auch von der Verwendung einer App explizit abgeraten, wenn die Prüfergebnisse dies nahelegen.

Die behördlichen Nutzer des App-Testings können sowohl auf einen größeren Bestand bereits vorhandener Prüfergebnisse geprüfter Apps zurückgreifen als auch bei Bedarf neue Prüfungen anstoßen. Dabei ist es auch möglich, Apps fortlaufend prüfen zu lassen, damit sich einmal zur Nutzung freigegebene Apps auf dem aktuellen Stand halten lassen.

Im Mai 2022 wurde der App-Testing-Dienst von registrierten Nutzern aus 65 Behörden und Organisationen verwendet. Für 655 verschiedene bereits geprüfte Apps stehen über 1.100 Prüfergebnisse zum Abruf bereit. Bei rund 70 Prozent der Prüfergebnisse wurden Hinweise und Empfehlungen gegeben, was bei einer Nutzung der betreffenden App beachtet werden sollte. Bei jeder sechsten geprüften App wurde sogar von einer Verwendung abgeraten.

Der App-Testing-Dienst trägt zur Stärkung der IT-Sicherheit im Bereich mobiler Applikationen auf dienstlichen Smartphones bei.

2.3.11 — Onlinezugangsgesetz: die IT-Sicherheitsverordnung Portalverbund

Das „Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen“ (Onlinezugangsgesetz – OZG) sieht die Digitalisierung aller Verwaltungsleistungen auf Kommunal-, Landes- und Bundesebene vor, sodass Bürgerinnen und Bürgern diese Leistungen einfach

und sicher online über Verwaltungsportale beantragen können. Der digitale Behördengang soll bundesweit einheitlich gestaltet sein, sodass die Verwaltungsportale zusätzlich zu einem interoperablen Verbund, dem Portalverbund, zusammengeschaltet sind. Um die IT-Sicherheit des Portalverbundes sicherzustellen, hat das BMI in seiner „Verordnung zur Gewährleistung der IT-Sicherheit der im Portalverbund und zur Anbindung an den Portalverbund genutzten IT-Komponenten“ (IT-Sicherheitsverordnung Portalverbund – ITSiV-PV) vom 06.01.2022 die Bedeutung des BSI in der Umsetzung des OZG, insbesondere der BSI-Grundschutzstandards 200-1, 200-2 und 200-3, sowie einige seiner Technischen Richtlinien hervorgehoben. In der ITSiV-PV ist festgehalten, dass die genannten Anforderungen des BSI an die IT-Sicherheit den aktuellen Stand der Technik abbilden und daher von den Komponenten des Portalverbunds verpflichtend einzuhalten sind.

Weiterführende Informationen finden Sie hier:[x]

Die Technische Richtlinie TR-03160 „Servicekonten“[42] behandelt die Servicekonten, die Antragstellende zur Identifizierung nutzen können. Sie macht dazu Vorgaben, um Missbrauch und Identitätsdiebstahl auf dem jeweils benötigten Vertrauensniveau zu verhindern und gleichzeitig die Interoperabilität zwischen den verschiedenen Servicekonten zu gewährleisten. Aktuell wird sie um einen Teil erweitert, der sich mit dem Postfach zum Empfangen von Bescheiden befasst. Zusätzlich ist ein weiterer Teil geplant, welcher die besonderen Anforderungen an Organisationskonten berücksichtigt.

Darüber hinaus nennt die ITSiV-PV die Technischen Richtlinien TR-03107-1 „Elektronische Identitäten und Vertrauensdienste im E-Government Teil 1“[43] und TR-03147 „Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen“[44], welche u. a. Anforderungen an die technischen Grundlagen der Identifizierung und *Authentisierung* und die damit verknüpften Mechanismen zur digitalen Willenserklärung formulieren. Die Technische Richtlinie TR-03116-4 „Kryptographische Vorgaben für Projekte der Bundesregierung Teil 4“[45] beschreibt Sicherheitsanforderungen für den Einsatz von Kommunikationsverfahren in Anwendungen des Bundes.

Für den Portalverbund selbst ist zusätzlich eine eigene, neue Technische Richtlinie in Entwicklung, die spezifische Maßnahmen zur Absicherung des Gesamtverbunds und seiner individuellen Komponenten gegen Angriffsszenarien, wie beispielsweise unerlaubten Datenabfluss, beschreibt. Im Zuge dieser Technischen Richtlinie betrachtet das BSI derzeit gezielt einzelne Aspekte des Portalverbunds, etwa unterschiedliche, im Einsatz befindliche Lösungen von Portalen. Diese werden in Abstimmung mit den Portaleignern auf mögliche Schwachstellen untersucht, die sich potenzielle Angreifer zu Nutze machen könnten. Die daraus gewonnenen Erkenntnisse fließen in die entstehende Technische Richtlinie ein.

Abschließend ist das BSI bei Fragen zur IT-Sicherheit der Modernisierung der Registerlandschaft beteiligt. Sie dient als notwendige Grundlage für die bedienerfreundliche Nutzung des Portalverbunds und zur Umsetzung des Once-Only-Prinzips, das die mehrfache Eingabe von Daten überflüssig machen soll. Das Ziel der Registermodernisierung ist es, den medienbruchfreien Austausch von Registerdaten und Nachweisen zwischen verschiedenen Behörden, aber auch für Verwaltungsleistungen innerhalb des Portalverbunds, zu gewährleisten.

2.4 — Internationales

IT-Sicherheit ist mehr als eine nationale Aufgabe, sondern eine europäische und internationale. Um der Internationalisierung der Cyber-Kriminalität effektiv begegnen zu können, ist mehr denn je eine Bündelung der Kräfte auf internationaler Ebene notwendig. Das zeigt nicht zuletzt der Einsatz von Cyber-Angriffen in internationalen Konflikten (vgl. Kapitel *Cyber-Sicherheitslage im Kontext des russischen Angriffskrieges gegen die Ukraine*, Seite 45). Aus diesem Grund arbeitet das BSI seit seiner Gründung weltweit mit Partnern zusammen: bilateral, multilateral oder in Gremien und Arbeitsgruppen. Dabei sind die Expertinnen und Experten des BSI als Gesprächs- und Diskussionspartner sowie Vortragende gefragt.

Ziel des BSI ist es, 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 dafür angemessen nachzukommen, intensiviert und erweitert das BSI kontinuierlich seine Beziehungen zu Behörden, Organisationen

und Unternehmen sowie Akteuren der Wissenschaft und Zivilgesellschaft weltweit. 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. Im Zuge der Digitalisierung gibt es in vielen Staaten und Regionen eine Notwendigkeit, Kapazitäten im Bereich der IT-Sicherheit aufzubauen („Cyber Security Capacity Building"). Dem damit einhergehenden Beratungs- und Unterstützungsbedarf begegnet das BSI durch den aktiven Aufbau von Partnerschaften in Zentral- und Südamerika, Afrika und dem Nahen Osten. Dadurch kann das BSI Know-how weitergeben, international Standards setzen und das Cyber-Sicherheitsniveau weltweit erhöhen. Durch eine Kooperation mit dem BMZ und der GIZ wird die Expertise des BSI zudem in der deutschen Entwicklungszusammenarbeit nutzbar.

2.4.1 — Engagement des BSI im EU-Rahmen

Eine zunehmende Anzahl von Gesetzesvorhaben mit weitreichender Bedeutung für die Cyber-Sicherheit Deutschlands und der Europäischen Union (EU) prägen das europäische regulatorische Lagebild. Besondere Aufmerksamkeit verdienen dabei der Vorschlag für eine Richtlinie über Maßnahmen für ein hohes gemeinsames Cyber-Sicherheitsniveau in der Union, die sogenannte NIS 2-Richtlinie, sowie zwei Initiativen zur Erhöhung der Cyber- und Informationssicherheit in den Organen, Einrichtungen und sonstigen Stellen der EU. Während des Berichtszeitraums durchliefen diese Vorhaben unterschiedliche Verhandlungsstadien zwischen den Organen der EU. Die NIS 2-Richtlinie wird voraussichtlich noch 2022 in Kraft treten. Die Diskussionen zu den anderen beiden Initiativen wurden erst im März 2022 durch die Europäische Kommission initiiert. Als nationaler Kompetenzträger für die Cyber-Sicherheit hat sich das BSI intensiv in die Verhandlungen eingebracht. Im Vordergrund stand dabei das Anliegen, eine substanzielle Erhöhung der IT-Sicherheit für Staat, Wirtschaft und Gesellschaft in Deutschland und Europa zu erreichen.

Parallel wurden hierzu wichtige Anliegen in unterschiedlichen EU-Fachgremien, etwa aus den Bereichen Zertifizierung, operative Cyber-Sicherheit oder dem Schutz kritischer Infrastrukturen, weiterverfolgt. Positiv hervorzuheben ist zudem, dass die Zahl der BSI-Expertinnen und -Experten, die zu relevanten EU-Einrichtungen abgeordnet wurden, erhöht werden konnte.

2.4.2 — Engagement des BSI in der NATO

Das BSI nimmt für die Bundesrepublik Deutschland gegenüber der NATO die Rollen als National CIS Security Authority (NCSA) und als National Cyber Defence Authority (NCDA) wahr. Im Rahmen des NATO-Engagement sind dies die Aktivitätsfelder Information Assurance und Cyber Defence. Das BSI wirkt dabei in einer Reihe von NATO-Gremien aktiv mit und bringt unter anderem im Capability Panel 4 (CaP4) und den darunterliegenden Capability Teams fachliche BSI-Interessen ein. Im Rahmen der Umsetzung der NATO Cyber-Defence-Strategy wirkt das BSI beständig darauf hin, seine Rolle als NCDA zu stärken.

Mit Übernahme der Leitung des NATO Cloud Security Technical Directive Writing Teams, das aus Belgien, Deutschland, Frankreich, Großbritannien sowie dem NATO Office for Security (NOS) und der NATO Communications and Information Agency (NCIA) besteht, hat das BSI maßgeblich an der Erstellung der NATO „Technical and Implementation Directive for the Protection of NATO Information within Public Cloud-Based Communication and Information Systems for NATO UNCLASSIFIED" mitgewirkt. Das BSI konnte dabei auch seine im Kriterienkatalog *Cloud Computing* Compliance Criteria Catalogue (C5) gestellten Mindestanforderungen an sicheres *Cloud Computing* erfolgreich einbringen.

2.4.3 — Multilaterales und bilaterales Engagement des BSI

Anknüpfend an das 2020 erstmals stattgefundene Cyber Security Directors' Meeting hat das BSI im Februar 2022 eine Anschlussveranstaltung im Rahmen der Münchner Sicherheitskonferenz organisiert. Angesichts der grenzübergreifenden Gefährdungslage und Herausforderungen der Digitalisierung bot die Veranstaltung wieder die einzigartige Möglichkeit, abseits des Tagesgeschäfts strategisch bedeutsame Themen zu diskutieren, die alle europäischen Cyber-Sicherheitsbehörden gleichermaßen betreffen und vor große Herausforderungen stellen. Die Veranstaltung war auch 2022 ein voller

Erfolg. Das BSI baut damit seine Position als Thought Leader der Informationssicherheit weiter aus und leistet einen wichtigen Beitrag zur besseren Vernetzung der europäischen Cyber-Sicherheitsbehörden.

Die Abordnung von BSI-Mitarbeitenden ins Ausland ist ein weiterer Bestandteil zur besseren Vernetzung und Zusammenarbeit mit internationalen Stakeholdern. Im Berichtszeitraum hat das BSI abgeordnete nationale Expertinnen und Experten zur ESA/ESTEC, ENISA und EU-Kommission entsendet. Darüber hinaus stellt das BSI derzeit die deutsche Sprecherin im NATO Cyber Defence Commitee und ist auch weiterhin mit einer Verbindungsperson in Brüssel vor Ort präsent.

Auch 2021 hat das BSI gemeinsam mit seiner französischen Partnerbehörde, der Agence nationale de la sécurité des systèmes d'information (ANSSI), wieder ein deutsch-französisches IT-Sicherheitslagebild veröffentlicht, diesmal zum Thema *Ransomware*. Die jährliche Publikation, die 2021 bereits zum vierten Mal erschienen ist, ist sichtbares Zeichen der engen deutsch-französischen Zusammenarbeit im Bereich der IT-Sicherheit und verdeutlicht gleichzeitig, dass die Bedrohungen nicht an Landesgrenzen haltmachen.

2.4.4 — Aufbau der National Cybersecurity Certification Authority

Auf Grundlage der Novellierung des BSIG im Mai 2021 wurde der § 9a neu eingeführt, der festlegt, dass das BSI die nationale Behörde für die Cyber-Sicherheitszertifizierung (engl. National Cybersecurity Certification Authority, *NCCA*) im Sinne der Verordnung (EU) 2019/881 (Cybersecurity Act (CSA), siehe Kapitel *IT-Grundschutz*, Seite 80) ist. Als *NCCA* ist das BSI im Zuge dessen die staatliche Zertifizierungsstelle für die Vertrauenswürdigkeitsstufe „high“ im Sinne des CSA. Das BSI nimmt durch den zeitnahen Aufbau der deutschen *NCCA* eine Vorreiterrolle in Europa ein und kann so im Rahmen von bilateralen Erfahrungsaustauschen auf eine einheitliche Umsetzung der Vorgaben des CSA in den Mitgliedstaaten hinwirken. Aus diesem Grund fanden bereits bilaterale Gespräche mit den Vertreterinnen und Vertretern der europäischen Partnerbehörden, wie der französischen ANSSI, statt.

Die europäische Zusammenarbeit steht im Fokus der *NCCA* im BSI. Hierfür wird ein Netzwerk aufgebaut, um den regelmäßigen Austausch mit den *NCCAs* der europäischen Mitgliedsstaaten sowie mit der Europäischen Kommission und der ENISA sicherzustellen. Das Ziel ist die zeitnahe Entwicklung und Umsetzung der Schemata für die europäische Cyber-Sicherheitszertifizierung, um so die IT-Sicherheit für den europäischen Binnenmarkt durch die Vereinheitlichung der Anforderungen zu stärken. Im Juli 2021 hatten alle europäischen Mitgliedstaaten die Möglichkeit, den Entwurf des Implementing Acts des CC-basierten europäischen Schemas für die Cyber-Sicherheitszertifizierung (EUCC) der Europäischen Kommission zu kommentieren, das als erstes CSA-Schema im Sommer 2022 auf den Weg gebracht werden soll. In diesem Zusammenhang bringt sich das BSI aktiv in den jeweiligen Gremien wie der Europäischen Gruppe für Cyber-Sicherheitszertifizierung (ECCG), deren Untergruppen sowie den Ad-hoc Arbeitsgruppen (AHWG) der ENISA an der Ausgestaltung des sogenannten Implementing Acts und der Guidance-Dokumente ein, wo auch das Management von Schwachstellen sowie der Einsatz von Kryptografie verhandelt werden, um Bedrohungen für IKT-Produkte, -Dienste und -Prozesse präventiv abzuwehren. Zusätzlich begleitet das BSI die Schema-Entwicklungen der ENISA für *Cloud* (EUCS) und 5G Mobilfunkausrüstung (EU5G) aktiv und prüft kritisch bzw. bewertet strategisch neue regulatorische Initiativen der Europäischen Kommission, wie der delegierte Rechtsakt der Radio Equipment Directive (RED), die Überarbeitung der Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS2), der Entwurf einer KI-Verordnung und die Neuerungen der Produktsicherheitsverordnung sowie der Maschinenrichtlinie mit dem Ziel der Verbesserung der europäischen IT-Sicherheitslage.

Um bestmöglich auf die kommenden Anforderungen vorbereitet zu sein, steht das BSI als *NCCA* mit den Konformitätsbewertungsstellen fortwährend im Austausch, die künftig die Cyber-Sicherheitszertifizierung unter dem CSA für die Vertrauenswürdigkeitsstufen „niedrig“ und „mittel“ durchführen. Darüber hinaus durchlaufen die Prüfstellen ein Pilotierungsverfahren der ENISA zur Akkreditierung, unabhängig von den Vertrauensstufen des CSA, für das sie im August 2021 durch das BSI angemeldet wurden und welches im Oktober 2021 startete. Die herstellenden Unternehmen, mit denen das BSI bis dato im Rahmen der CC-Zertifizierung vertrauensvoll zusammenarbeitet, wurden in einer virtuellen Informationsveranstaltung im Dezember 2021 über die anstehenden Neuerungen informiert mit der Zusage, dass

dieser fruchtbare Austausch fortgesetzt wird, um die Umsetzung der Vorgaben des CSA für ein einheitliches Sicherheitsniveau zur Reduzierung von Bedrohungen zu garantieren. Das BSI stellt außerdem Informationen im Rahmen der Öffentlichkeitsarbeit zur Verfügung, um eine größtmögliche Transparenz zu den gesetzlichen Vorgaben und deren Umsetzung zu erzeugen, sowohl über die Webseite als auch über einen Artikel zum Thema *NCCA* in der Ausgabe 02/2021 des BSI-Magazins und in diversen Vorträgen.

Weiterführende Informationen finden Sie hier:[y]

2.4.5 — Nationales Koordinierungszentrum für Cyber-Sicherheit

Mit der am 28. Juni 2021 in Kraft getretenen EU-Verordnung 2021/887 wurde das europäische Kompetenzzentrum für Cyber-Sicherheit in Industrie, Technologie und Forschung (ECCC) mit Sitz in Bukarest und ein Netz von nationalen Koordinierungszentren (NCC) eingerichtet. Das ECCC soll als Hauptinstrument der Europäischen Union zur Bündelung von Investitionen in Forschung, Technologie und industrieller Entwicklung agieren, insbesondere im Bereich Cyber-Sicherheit der beiden EU-Förderprogramme „Digitales Europa“ (DEP) und „Horizont Europa“ (HEP). Es soll eine stärkere Koordinierung von Forschung und Innovation sowie von Einführungsstrategien auf europäischer und nationaler Ebene gewährleisten. Das Kompetenzzentrum wird durch die Mitgliedstaaten und die EU-Kommission verwaltet. Dafür wurde ein Verwaltungsrat (Governing Board) eingerichtet, in dem das BSI Deutschland vertritt.

Die nationalen Koordinierungszentren bilden die Anlaufstelle für das ECCC auf staatlicher Ebene. So entsteht ein Netzwerk, das den Austausch zwischen den Mitgliedstaaten und innerhalb der Cyber-Sicherheits-Community intensiviert, damit besser und schneller mögliche internationale Projektpartnerschaften gefunden und geschlossen werden können und somit die digitale Souveränität in Europa gestärkt wird. Darüber hinaus stellen die Koordinierungszentren Fachwissen und Unterstützung bei der Erfüllung der strategischen Aufgaben des ECCC bereit. Gleichzeitig können so nationale Interessen in den europäischen Forschungsprogrammen platziert werden.

Das deutsche nationale Koordinierungszentrum für Cyber-Sicherheit in Industrie, Technologie und Forschung (NKCS, engl. NCC-DE) ist eine gemeinsame, virtuelle Institution der Ressorts BMI, BMWK, Bundesministerium für Verteidigung (BMVg) und Bundesministerium für Bildung und Forschung (BMBF) sowie weiterer Organisationen (BSI, DLR-PT und FI CODE) und bietet der nationalen Cyber-Sicherheits-Community einen umfangreichen Dienste-Katalog zur Unterstützung an. Als die Cyber-Sicherheitsbehörde des Bundes fungiert das BSI dabei als Kopfstelle sowie „Single Point of Contact“ und wurde am 10. Dezember 2021 vom BMI durch Staatssekretär Dr. Richter offiziell als diese notifiziert. Bereits etablierte Strukturen in den Ressorts und Institutionen, beispielsweise zur Vergabe von Forschungsmitteln, werden unmittelbar genutzt. In seiner Rolle als Kopfstelle des NKCS wird das BSI sowohl mit den beteiligten Ressorts und deren nachgeordneten Bereichen als auch mit dem europäischen Kompetenzzentrum und den NCCs anderer Nationen eng zusammenarbeiten.

Weiterführende Informationen finden Sie hier:[z]

2.4.6 — eID: Novellierung der eIDAS-Verordnung

Auch im weiteren Verlauf der Corona-Pandemie haben digitale Geschäftsprozesse eine weiter steigende Bedeutung erfahren. Damit einhergehend steigt der Bedarf an sicherer elektronischer Identifizierung/elektronischen Identitäten, um die Integrität digitaler Prozesse, ein hohes Maß an Vertrauen zwischen Nutzerinnen und Nutzern sowie Dienstleistern zu gewährleisten und Onlinebetrug sowie insbesondere Identitätsdiebstahl zu erschweren.

Neben vielen kleineren Änderungen sieht der 2021 im Rahmen der turnusgemäßen Revision der eIDAS Verordnung veröffentlichte neue Verordnungsentwurf eine „European-Digital Identity Wallet“ vor, die als elektronisches Identifizierungsmittel (eID) grenzüberschreitend nutzbar sein soll, allerdings neben klassischen Identitätsattributen (Vorname, Name etc.) noch weitere Attribute (z. B. Bildungsabschluss) in verifizierbarer Art für Diensteanbieter bereitstellen kann. Das BSI ist an der dafür notwendigen Definition von Rahmen-

bedingungen intensiv beteiligt, bringt die bestehende deutsche Infrastruktur ein und setzt sich weiterhin für sichere und nutzerfreundliche eID Lösungen ein, die grenzüberschreitend verwendet werden können.

Daneben haben weitere Staaten elektronische Identifizierungssysteme im Rahmen der bestehenden eIDAS Verordnung zur grenzüberschreitenden Anerkennung notifiziert, die nach Ablauf einer einjährigen Übergangszeit einer gegenseitigen Anerkennungsverpflichtung unterliegen. Auch hier hat sich das BSI im Rahmen von Peer-Reviews intensiv beteiligt. Insgesamt betrifft die Anerkennungsverpflichtung nun 21 elektronische Identifizierungssysteme europaweit.

2.4.7 — Mindestanforderungen für die IT- und Cyber-Sicherheit von Satelliten

In einer global vernetzten Welt fordern Staat, Wirtschaft und Gesellschaft jederzeit verfügbare Dienste für Kommunikation, Navigation, Position und Zeitbestimmung sowie Klimaüberwachung oder Wettervorhersage. Die Realisierung dieser Dienste ist in vielen Bereichen nur durch die Unterstützung satellitenbasierter Infrastrukturen möglich.

Das BSI als die Cyber-Sicherheitsbehörde des Bundes ist für die Cyber-Sicherheit von IT- und Kommunikationssystemen verantwortlich. Das gilt unabhängig davon, ob die Systeme terrestrisch, luftgestützt oder weltraumbasiert sind. Deshalb bedient das BSI intensiv das Gebiet Cyber- und IT-Sicherheit aller Satellitensysteme; Low Earth Orbit (LEO), Medium Earth Orbit (MEO) und Geostationary Earth Orbit (GEO).

Aus Sicht des BSI ist es unabdingbar, zur Beantwortung der weltraumspezifischen Cyber-Sicherheitsfragen eine national abgestimmte Zielsetzung und definierte Handlungsfelder verbindlich festzulegen. Vor dem Hintergrund der schnell zunehmenden Kommerzialisierung des Weltraums (New Space), ist auch die Frage nach ggf. erforderlichen nationalen und internationalen Regulierungswerkzeugen zu klären.

Das BSI hat bereits jetzt in Zusammenarbeit mit dem Kommando Cyber- und Informationsraum (KdoCIR), der Deutsche Raumfahrtagentur im DLR und der nationalen Weltraumindustrie Mindestanforderungen entwickelt und als IT-Grundschutz-Profil formuliert.

Weiterführende Informationen finden Sie hier:[aa]

Modernisierung der Kryptografie für die nächste Generation des europäischen Flaggschiffs GALILEO

Das europäische Navigationssystem GALILEO steht aktuell im Fokus der Projekte zur Cyber-Sicherheit von Satelliten. Zusammen mit anderen Mitgliedsstaaten wurde unter der Federführung des BSI bereits 2018 ein Anforderungskatalog erstellt, um Satellitensysteme und insbesondere deren Kommunikationsinfrastrukturen zukunftssicher zu gestalten. Eine wesentliche Forderung ist die *Resilienz* gegenüber der Bedrohung durch Quantencomputer. Zusammen mit internationalen Partnern unterstützt das BSI die Europäische Weltraumorganisation (ESA) und die Kommission bei der Umsetzung dieser Anforderungen für die zweite Generation GALILEOs. Die ersten Satelliten mit modernisierter Kryptografie sollen nach Plan der Europäischen Kommission bereits im Jahr 2024 gestartet werden. Parallel begleitet das BSI die Anpassung der Bodeninfrastruktur.

2.5 — Aktuelle Trends und Entwicklungen in der IT-Sicherheit

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

2.5.1 — Künstliche Intelligenz

Künstliche Intelligenz stellt als Zukunftstechnologie sowohl eine Chance für die Informationssicherheit als auch ein Risiko und mögliches Angriffswerkzeug dar.

KI lässt sich schon heute missbrauchen, um Medien wie Bilder, Sprache oder Texte zu manipulieren *(„Deepfakes“)*, um zum Beispiel Fake News zu generieren oder Fernidentifikationsverfahren zu täuschen (vgl. Kapitel *Mediale Identitäten*, Seite 65). Nach Erkenntnissen des BSI ist ein Missbrauch der Technologien in den heute häufig genutzten Videokonferenzen bereits möglich. Derzeit lassen sich Videomanipulationen oft noch an typischen Artefakten erkennen, aber die Entwicklung der Technologie schreitet voran. Daher werden zuverlässige technische Detektionsmechanismen und Techniken zur Sicherstellung der Integrität von Medien benötigt, um solche Angriffe zu erkennen oder zu erschweren.

KI-Methoden lassen sich auch zur Verbesserung der Informationssicherheit einsetzen. Ein mögliches Szenario ist beispielsweise die (semi-)automatische Generierung von Lageberichten. So untersucht das BSI in einem aktuellen Projekt, wie durch KI-Methoden textuelle Informationen aus dem Bereich Cyber-Sicherheit automatisiert analysiert und extrahiert werden können, um die Analysten zu entlasten und die passenden Textpassagen zu einer gestellten Frage zu finden.

Im Bereich der sicheren Softwareentwicklung kann KI ebenfalls einen Beitrag leisten. Im Projekt ML-SAST, dessen Zwischenbericht veröffentlicht wurde, wird aufgezeigt, wie KI-Methoden bestehenden Techniken zur statischen Codeanalyse zu einer deutlich höheren Treffergenauigkeit verhelfen können.

KI-Ansätze wie Deep-Learning-Algorithmen können allerdings auch selbst zum Ziel eines Angreifers werden, beispielsweise mit dem Ziel die Entscheidungsfindung eines solchen Algorithmus zu manipulieren. Um dem entgegenzutreten, untersucht das BSI in einer kürzlich veröffentlichten Studie zum Projekt „Sicherheit von KI-Systemen: Grundlagen“ mögliche Angriffe auf Deep-Learning-Algorithmen, um im nächsten Schritt passende Gegenmaßnahmen zu entwickeln.

Im Bereich der biometrischen Verfahren gewinnt Deep Learning immer mehr an Bedeutung. Daher wurde im November 2021 das Biometrie-Evaluations-Zentrum (BEZ) in Sankt Augustin bei Bonn offiziell eröffnet, in dem das BSI mit dem Institut für Sicherheitsforschung (IFS) der Hochschule Bonn-Rhein-Sieg kooperiert. Auf Basis der dort stattfindenden Forschung zur Zuverlässigkeit und Schwachstellen biometrischer Systeme und deren KI-Komponenten sollen Beratungsleistungen angeboten und Prüfmethoden für Zertifizierungen und neue Sicherheitstechnologien entwickelt werden.

Nicht nur die Absicherung aktueller Techniken, sondern auch die Entwicklung sicherer Standards und Normen für KI hat sich das BSI zum Ziel gesetzt. Einen wichtigen Schritt zur Sicherheit von KI-Diensten in der *Cloud* stellt hierbei der Kriterienkatalog AIC4 dar, für den im vergangenen Jahr bereits Prüfungen bei mehreren Unternehmen durchgeführt wurden. Aktuell arbeitet das BSI an einer Weiterentwicklung von AIC4, in welche die neuen Technologieentwicklungen sowie Erkenntnisse aus den bereits durchgeführten Prüfungen einfließen. Die Erfahrungen aus AIC4 bringt das BSI auch in die nationalen und internationalen Standardisierungsgremien ein. Dazu arbeitet das BSI bei der DIN, den europäischen CEN/CENELEC, ETSI und ENISA sowie bei der ISO aktiv mit.

Weitere KI-Themen, mit denen sich das BSI im Berichtszeitraum beschäftigte und Erkenntnisse der Öffentlichkeit zur Verfügung stellte, sind die Erklärbarkeit von KI-Systemen sowie die Sicherheit von Quantum Machine Learning, einer zukünftigen Technik, die Gebiete der Künstlichen Intelligenz und des Quantencomputings miteinander verbindet.

Anhand der vielfältigen Themen und Herausforderungen im Bereich IT-Sicherheit und KI, die besonders in der jetzigen Zeit einem ständigen Wandel ausgesetzt sind und immer mehr an Bedeutung gewinnen, wird klar, dass das BSI hier seine Aktivitäten verstärken muss.

Aufgrund der vielfältigen Themen und Herausforderungen im Bereich IT-Sicherheit und KI, die einem ständigen Wandel ausgesetzt sind und immer mehr an Bedeutung gewinnen, verstärkt das BSI seine Aktivitäten in diesem Bereich. Hierzu wurde auf dem Campus der Universität des Saarlandes in Saarbrücken ein neuer KI-Stützpunkt errichtet. Das BSI vernetzt sich dort mit den ansässigen Forschungszentren im Bereich KI und IT-Sicherheit. So wird beispielsweise derzeit eine Studie zum Thema „Sicherheit von symbolischen und hybriden KI-Systemen“ in Zusammenarbeit mit dem Deutschen Forschungsinstitut für Künstliche Intelligenz (DFKI) erstellt und es werden mehrere Master-Arbeiten betreut. Aufgrund der geografischen Lage soll von Saarbrücken aus auch die Zusammenarbeit mit Frankreich und Luxemburg im Bereich von KI und IT-Sicherheit weiter intensiviert werden.

2.5.1.1 — Künstliche Intelligenz in Anwendungen

In den letzten Jahren ist die Leistungsfähigkeit von Systemen auf Basis von KI stark gestiegen, weshalb sie in immer mehr Anwendungsbereichen zum Einsatz kommen. Hierzu zählen auch sicherheitskritische Anwendungen wie zum Beispiel das automatisierte Fahren. KI-Systeme weisen jedoch trotz ihrer enormen Leistungssteigerungen auch verschiedene Risiken auf, die angemessen berücksichtigt werden müssen. Hierzu zählt die oft mangelnde Robustheit gegenüber Veränderungen in den verarbeiteten Eingabedaten, die zum Beispiel beim automatisierten Fahren in Abhängigkeit von der Tageszeit und dem Wetter auftreten. Eine weitere Herausforderung besteht in der Anfälligkeit der KI-Systeme für qualitativ neuartige Angriffe, mit denen Angreifer gezielt unerwünschte Entscheidungen hervorrufen können. In vielen Anwendungen bestehen weitere Risiken, wie die Möglichkeit von diskriminierenden Entscheidungen durch KI-Systeme im Finanz- oder Gesundheitssektor.

Die Europäische Kommission hat im April 2021 einen Verordnungsentwurf zu KI vorgelegt, der aktuell verhandelt wird und der die beschriebenen Herausforderungen von KI-Systemen regulatorisch angeht. Die KI-Verordnung der EU wird besonders Hochrisiko-KI-Systemen, zum Beispiel im Mobilitätsbereich, weitreichende Anforderungen auferlegen. Vor der geplanten Operationalisierung der Verordnung innerhalb der kommenden zwei bis drei Jahre sind allerdings noch wesentliche technische Fragen zu klären, um die allgemeinen Anforderungen der Verordnung auf ein angemessenes technisches Niveau zu übertragen und hinreichend genaue Prüfverfahren zu entwickeln. Das BSI beteiligt sich aktiv an verschiedenen Arbeitsgruppen bei DIN, ETSI und ENISA, die an dieser umfangreichen Aufgabe mitwirken.

Im Kontext der KI-Verordnung fand im Oktober 2021 auch der Workshop „Auditing AI-Systems: From Principles to Practice“ statt, der vom BSI wie im Vorjahr gemeinsam mit dem Verband der TÜV (VdTÜV) und dem Fraunhofer Heinrich-Hertz-Institut ausgerichtet wurde. Der Fokus des Workshops lag auf dem Austausch von Erfahrungen, die bei der Umsetzung erster Absicherungs- und Prüfansätze in praktischen Projekten gesammelt und auch mit einer Vertreterin der EU-Kommission diskutiert worden sind. Basierend auf dem Workshop hat die seit 2019 bestehende Arbeitsgruppe von BSI und VdTÜV ein Whitepaper erarbeitet, in dem die aktuelle Prüfbarkeit von KI-Systemen kompakt in Matrixform dargestellt wird. Dies bildet einerseits die Grundlage für zukünftige Bestandsaufnahmen und dient andererseits dazu, bestehende Lücken bei der Operationalisierung der KI-Verordnung zu identifizieren.

Zusätzlich hat das BSI im Dezember 2021 das Projekt AIMobilityAuditPrep gestartet, in dem erste konkrete Kriterien und Prüfverfahren für KI-Verfahren im automatisierten Fahren erarbeitet werden. Diese Vorarbeiten sollen mittelfristig die Verfassung einer technischen Richtlinie des BSI ermöglichen.

Das Whitepaper finden Sie hier:[bb]

2.5.1.2 — Künstliche Intelligenz in der Kryptografie

KI hat längst Einzug in verschiedene Bereiche der Kryptografie gehalten: Insbesondere in der Seitenkanalanalyse haben sich Machine-Learning-Methoden inzwischen fest etabliert. Die besten Ergebnisse lassen sich erzielen, wenn maschinelles Lernen mit Expertenwissen über mögliche Quellen von Seitenkanalinformationen kombiniert wird, wobei der Einsatz neuronaler Netze besonders erfolgreich ist. Das BSI beschäftigt sich daher aktuell im Rahmen zweier Projekte näher mit dem Thema: Im Projekt KISKA (KI-Methoden in der SeitenKanalAnalyse) soll herausgefunden werden, wie sich bereits existierende Ansätze aus dem Bereich der Seitenkanalanalyse symmetrischer Verfahren auf asymmetrische Verfahren anpassen bzw. verallgemeinern lassen. Ferner arbeitet das BSI an der Erstellung eines KI-Seitenkanalleitfadens, mit dem unter anderem die Ziele verfolgt werden, Evaluatoren und Herstellern einen Überblick über den aktuellen Stand der Forschung auf dem Gebiet zu verschaffen und auf Angriffsmethoden hinzuweisen, die bei der Evaluierung und Zertifizierung von Implementierungen beachtet werden müssen.

KI-Techniken können auch im Bereich der Kryptoanalyse verwendet werden. Im Rahmen von zwei aufeinander aufbauenden BSI-Projekten untersucht ein Team der Ruhr-Universität Bochum Möglichkeiten, Künstliche Intelligenz bei der Analyse und Bewertung von symmetrischen Kryptoverfahren einzusetzen. Ein Ziel dieser Projekte ist die Entwicklung von KI-gestützten

Werkzeugen, die zu einer Sicherheitsbewertung von Blockchiffren beitragen können.

2.5.2 — Kryptografie

Die fortschreitende Entwicklung von Quantencomputern bedroht die Sicherheit vieler klassischer und weit verbreiteter Public Key-Verfahren wie *RSA* und ECC. Deshalb ist die Entwicklung und Standardisierung von Verfahren, die voraussichtlich auch mit Quantencomputern nicht gebrochen werden können (Post-Quanten-Kryptografie), von hoher Dringlichkeit. Das BSI handelt dazu für den Hochsicherheitsbereich unter der Arbeitshypothese, dass kryptografisch relevante Quantencomputer Anfang der 2030er-Jahre zur Verfügung stehen werden. Dabei ist zu betonen, dass diese Aussage nicht als Prognose zur Verfügbarkeit von Quantencomputern zu verstehen ist, sondern einen Richtwert für die Risikobewertung darstellt. Einen Überblick zum gesamten Themenkomplex liefert der Leitfaden „Kryptografie quantensicher gestalten“ des BSI (siehe Info-Kasten).

Die Standardisierung von Post-Quanten-Verfahren geschieht aktuell im Wesentlichen in einem vom US-amerikanischen National Institute of Standards and Technology (NIST) im Jahre 2016 initiierten Prozess mit internationaler Beteiligung. Im Juli 2022 wurden nun erste Verfahren von NIST zur Standardisierung ausgewählt und Entwürfe für Standards werden im Laufe des nächsten Jahres erwartet. Die Forschung zu Post-Quanten-Verfahren ist sehr aktiv: Im Jahr 2022 konnten zwei zum NIST-Prozess eingereichte Verfahren, die es bereits in die 3. Bzw. 4. Runde geschafft hatten, durch neue Angriffe gebrochen werden. Die Sicherheit der vom BSI empfohlenen sowie der von NIST bislang zur Standardisierung ausgewählten Verfahren beruht jedoch auf ganz anderen mathematischen Problemen. Daher sind diese Verfahren von den neuen Angriffen nicht betroffen. Auch sie müssen jedoch weiter aktiv untersucht werden und das BSI empfiehlt zunächst grundsätzlich den hybriden Einsatz von Post-Quanten-Kryptografie in Kombination mit klassischer *Public-Key-Kryptografie*.

Neben der Standardisierung von Verfahren laufen zurzeit viele konkrete Aktivitäten zur Migration auf Post-Quanten-Kryptografie. Der kürzlich auf dem Markt erschienene SINA Communicator H ist das erste GEHEIM-zugelassene VS-IT-Produkt in Deutschland, das eine hybride Schlüsseleinigung mit einem Post-Quanten-Verfahren umsetzt. Das BSI hat außerdem zwei Projekte ins Leben gerufen, in denen quantencomputerresistente Verfahren im E-Mail-Client Thunderbird sowie in der Kryptografie-Bibliothek Botan implementiert werden. In Kooperation mit KPMG wurde eine Umfrage zur Awareness zum Thema PQ-Migration gestartet.

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 Dezember 2021 veröffentlichte das BSI den Leitfaden *"Kryptografie quantensicher gestalten"* (siehe Info-Kasten), in dem sich auch detailliertere Erläuterungen, Empfehlungen und Einschätzungen zum Einsatz von QKD finden.

Weiterführende Informationen finden Sie hier:[cc]

Derzeit gibt es noch keine nach internationalen Standards zertifizierten QKD-Produkte. Anfang 2021 wurde jedoch ein erstes Protection Profile für QKD-Geräte fertiggestellt. Das Protection Profile wurde im Auftrag des BSI in Zusammenarbeit mit der ETSI Industry Specification Group QKD erstellt. In einem nächsten Schritt soll das Protection Profile zertifiziert werden. Für die spätere Anwendbarkeit ist ein Ökosystem für QKD-Produkte aufzubauen, in dem Prüfkriterien und Bewertungsmethoden – beispielsweise für *Seitenkanalangriffe* – abgestimmt und weiterentwickelt werden.

Die Entwicklung von QKD-Geräten in der EU befindet sich noch in einem frühen Stadium. Allerdings arbeiten mittlerweile auch einige deutsche Firmen und Startups an der Entwicklung von QKD-Geräten. Daneben werden in Deutschland und Europa zahlreiche Projekte im Bereich QKD gefördert. Im europäischen Projekt EuroQCI, dem mittlerweile alle 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. In Deutschland erforscht die BMBF-geförderte Initiative QuNET verschiedene Aspekte der Quantenkommunikation. Das BSI begleitet die Forschungsinitiative als Mitglied im Beirat. QuNET hat sich hochsichere Kommunikation zwischen Behörden als Anwendungsfall zum Ziel gesetzt. Im August 2021 wurde im Rahmen des QuNET-Projekts eine QKD-Strecke zwischen dem BSI und dem BMBF in Bonn aufgebaut und eine mit Post-Quanten-Algorithmen und QKD gesicherte Videokonferenz demonstriert.

2.5.4 — Self-Sovereign Identities und Blockchain-Technologie

Angesichts der Digitalisierungsvorhaben in Wirtschaft, Industrie und Verwaltung zeigt sich in der öffentlichen Diskussion der zunehmende Wunsch, den Nutzerinnen und Nutzern von Diensten größtmögliche Datensouveränität einzuräumen. Statt Nutzerprofile bei zentralen Anmeldediensten zu hinterlegen, sollen Nutzerinnen und Nutzer ihre Identitätsdaten in einer lokalen Anwendung (Wallet) speichern und selbst verwalten. So können sie von Fall zu Fall entscheiden, wem gegenüber sie welche Informationen offenlegen. Auch der Entwurf für die Novellierung der eIDAS-Verordnung (siehe Kapitel *Nationales Koordinierungszentrum für Cyber-Sicherheit*, Seite 95) sieht für die European Digital Identity Wallet (EUDI Wallet) eine solche Form der selektiven Offenlegung von Identitätsdaten vor.

Das geschilderte Konzept ist unter dem Begriff Self-Sovereign Identities (SSI) bekannt. Für seine konkrete Umsetzung gibt es bislang keine etablierten Empfehlungen. Das BSI hat daher im Dezember 2021 ein Eckpunktepapier zu SSI veröffentlicht, um auf die IT-sicherheitsrelevanten Aspekte hinzuweisen.

Das Eckpunktepapier zu SSI finden Sie hier:[dd]

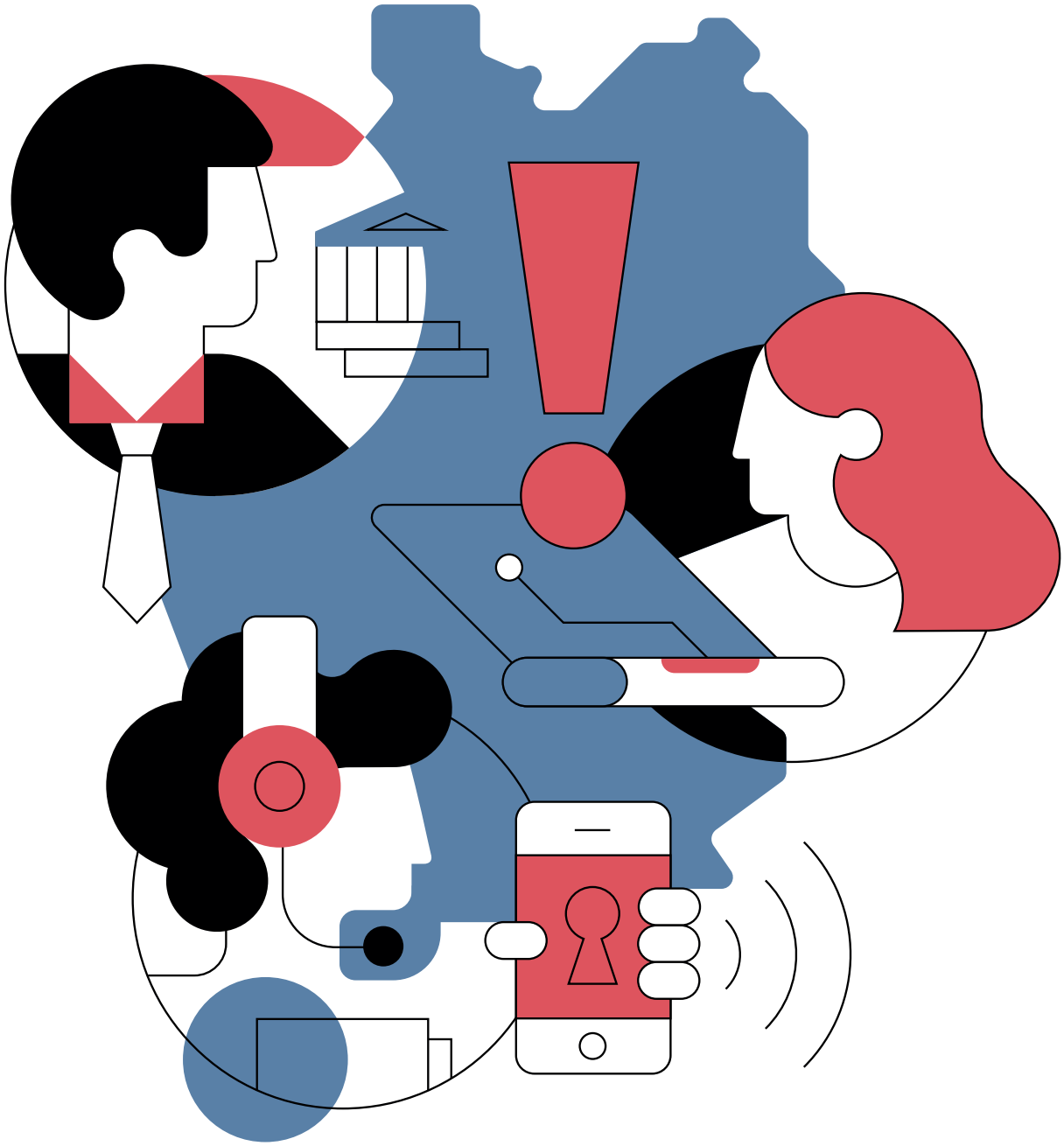
Leitfaden „Kryptografie quantensicher gestalten“

Der Leitfaden „Kryptografie quantensicher gestalten“ gibt einen Überblick über die relevanten Entwicklungen im Bereich der Quantentechnologien sowie Handlungsempfehlungen zur Migration auf quantensichere Kryptografie.

Der Wechsel zu quantensicherer Kryptografie führt zu zahlreichen offenen Fragen (beispielsweise Auswahl geeigneter Algorithmen, notwendige Anpassungen bei Protokollen und Standards u. v. m.), die in diesem Dokument diskutiert werden.

Weiterführende Informationen finden Sie hier:[ee]

Fazit



Fazit

Angriffskrieg auf die Ukraine verschärft die Cyber-Sicherheitslage in Deutschland

Der Bericht zur Lage der IT-Sicherheit in Deutschland steht in diesem Jahr unter dem besonderen Eindruck des russischen Angriffskrieges auf die Ukraine. Denn in diesem Konflikt werden nicht nur konventionelle Streitkräfte und Waffen, sondern auch digitale Angriffsmethoden eingesetzt. Deshalb hat das BSI die Lage seit Februar intensiv beobachtet, seinen Eigenschutz sowie seine Krisenreaktion gestärkt und das Nationale IT-Krisenreaktionszentrum aktiviert. Darüber hinaus hat das BSI auch seine Zielgruppen, darunter die Bundesverwaltung, Betreiber Kritischer Infrastrukturen und weitere Organisationen und Unternehmen frühzeitig und wiederholt sensibilisiert und zu einer erhöhten Wachsamkeit und Reaktionsbereitschaft aufgerufen.

Seit Beginn des Angriffskriegs Russlands auf die Ukraine ist es in Deutschland zu einzelnen zusätzlichen IT-Sicherheitsvorfällen gekommen. So kam es mit dem Ausfall der satellitengestützten Kommunikation zur Fernwartung von Windenergieanlagen zu Kollateralschäden in Teilen Europas. Auch waren Betreiber Kritischer Infrastrukturen Angriffsziele von Hacktivisten. Daneben ist es bis Redaktionsschluss des Berichtes in Deutschland zu einzelnen zusätzlichen IT-Sicherheitsvorfällen gekommen, die allerdings nur selten spürbare Auswirkungen hatten.

Unbeeindruckt davon hält auch die Bedrohung durch Cyber-Kriminelle weiter unvermindert an. Erneut stehen Cyber-Angriffe mit *Ransomware* im Mittelpunkt, die aufgrund ihrer Natur weitreichende Folgen für Betroffene und unbeteiligte Dritte haben. Auch DDoS-Angriffe (Überlastangriffe) bedrohen weiterhin die Informationssicherheit insbesondere von Online-Shops und Anbietern webbasierter Dienste.

Insgesamt spitzte sich im Berichtszeitraum die bereits zuvor angespannte Lage weiter zu. Die Bedrohung im Cyber-Raum ist damit so hoch wie nie.

Bedrohung durch Cyber-Erpressung steigt weiter

Die bereits im vergangenen Berichtszeitraum beobachtete Ausweitung von Methoden der Cyber-Erpressung hat sich im aktuellen Berichtszeitraum fortgesetzt. Insbesondere die Erpressung umsatzstarker Unternehmen hat weiter zugenommen. Sowohl die von IT-Sicherheitsdienstleistern berichteten Lösegeld- und Schweigegeld-Zahlungen als auch die Anzahl der Opfer sind weiter gestiegen. Dass nicht nur umsatzstarke Unternehmen Ziel von Ransomware-Angriffen werden können, zeigen die Auswirkungen in mehreren betroffenen Kommunen, in denen die Verwaltungsprozesse teils über Monate massiv gestört waren – mit erheblichen Folgen für die Bürgerinnen und Bürger. Wie wichtig eine gezielte Stärkung der Cyber-Sicherheit auf kommunaler Ebene ist, zeigt auch das große Interesse an den vom BSI im Berichtszeitraum gezielt für Kommunen angebotenen Webinaren und der erstmals durchgeführten virtuellen „Roadshow Kommunen".

Zudem kam es im aktuellen Berichtszeitraum auch immer wieder zu Erpressungen mit erbeuteten Identitätsdaten. Angesichts der Entwicklung im zurückliegenden Berichtszeitraum muss festgehalten werden, dass die Menge an Identitätsdaten in den Händen von Cyber-Kriminellen stetig zunimmt. Diese Bedrohung kann jede Bürgerin und jeden Bürger direkt treffen. Das BSI empfiehlt daher, sich mit dem eigenen Umgang mit Identitätsdaten auseinanderzusetzen und stellt dafür zielgruppengerechte und vielfältige Informationen zur Verfügung.

Verbraucherinnen und Verbraucher waren zudem Ziel von mehreren, teils ungewöhnlich ausgeprägten Sextortion-Kampagnen. In diesen Spam-Mails behaupten Angreifer, über kompromittierende, intime Geheimnisse des Opfers zu verfügen, und drohen, diese zu veröffentlichen. Um die Veröffentlichung der vermeintlich vorhandenen kompromittierenden Informationen zu verhindern, solle das Opfer einen bestimmten Betrag in *Bitcoin* überweisen.

Neue Dimension bei Schwachstellen

Die Lage bei Schwachstellen war im Berichtszeitraum überdurchschnittlich bedrohlich. Das lag einerseits daran, dass mit Schwachstellen in MS Exchange und Log4j besonders kritische Schwachstellen in weitverbreiteten Produkten auftraten und nur zögerlich geschlossen werden konnten. Insbesondere bei Log4Shell herrschte eine langanhaltende Unsicherheit, wie viele IT-Produkte tatsächlich betroffen waren und wie das Problem umfänglich behoben werden konnte. Zum anderen hat aber auch die Anzahl der bekannt gewordenen Schwachstellen insgesamt weiter zugenommen. So verzeichnete das CVSS-Scoring-System im Jahr 2021 mit 20.174 Schwachstellen in Software-Produkten rund 10 Prozent mehr als im Jahr zuvor. Das spiegelt sich auch in den im Jahr 2021 vom Warn- und Informationsdienst des BSI veröffentlichten Meldungen über Schwachstellen in den 150 gängigsten Produkten. Mit 6.910 stieg die Anzahl um rund zehn Prozent im Vergleich zum Vorjahr.

Im zweiten Halbjahr 2021 kam es zudem zu herausragenden Supply-Chain-Angriffen über die Software Virtual System Administrator (VSA) eines amerikanischen Software-Herstellers, die auch in Deutschland vielfach verwendet wird und deshalb zahlreiche Kundinnen und Kunden betraf. VSA wird beispielsweise zur Fernwartung und zum Monitoring von IT-Systemen eingesetzt. Schwachstellen in VSA sind deshalb besonders kritisch, weil sich über den Verwaltungsserver von VSA auf jeden verwalteten Client zugreifen und auch Software verteilen lässt. Das BSI hat deshalb am 4. Juli 2021 eine Cyber-Sicherheitswarnung herausgegeben, die anschließend regelmäßig aktualisiert wurde. Das BSI beobachtete die Betroffenheit deutscher Organisationen intensiv, beriet Betroffene zu IT-forensischen Maßnahmen und übermittelte Erste-Hilfe-Dokumente.

Zeitenwende für Cyber-Sicherheit made in Germany

Schon vor dem Digitalisierungsschub, den die Corona-Pandemie verstärkt hat, und vor der neuen Bedrohungslage in Folge des russischen Angriffskrieges auf die Ukraine, war Cyber-Sicherheit ein wesentlicher Erfolgsfaktor für eine zunehmend digital vernetzte Gesellschaft und Wirtschaft. Doch die beschleunigte Digitalisierung in allen Bereichen des alltäglichen Lebens – von den Lieferketten der international agierenden Konzerne, den Geschäftsprozessen auch in kleinen und kleinsten Unternehmen über die Dienstleistungen öffentlicher Institutionen bis hin zu den digitalen Anwendungen, die fast jede Bürgerin und jeder Bürger täglich im Alltag nutzt – macht auch bei der Cyber-Sicherheit made in Germany eine Zeitenwende notwendig.

Das Wohlergehen der Bevölkerung hängt stärker als je zuvor unmittelbar und in großem Umfang davon ab, wie erfolgreich es gelingt, die digitale *Resilienz* der Gesellschaft zu stärken. Und das bedeutet nicht nur *Resilienz* gegen Angriffe von Cyber-Kriminellen, gegen Soft- und Hardware-Ausfälle oder Konfigurationsfehler, die die Verfügbarkeit von gewohnten und alltäglichen Dienstleistungen gefährden können. Das vergangene Jahr hat auch gezeigt, dass unvorhergesehene Ereignisse die Bedrohungslage auf ein neues Level heben können, dass Kollateralschäden durch Cyber-Angriffe in Nachbarländern auch unmittelbare Auswirkungen auf Deutschland und Europa haben können.

All dies macht deutlich, dass präventive IT-Sicherheitsmaßnahmen die wirkungsvollsten IT-Sicherheitsmaßnahmen sind. Vor diesem Hintergrund ist die von der Bundesregierung geplante Modernisierung der Cyber-Sicherheitsarchitektur und der Ausbau des BSI zur Zentralstelle für Informationssicherheit im Bund-Länderverhältnis ein wichtiger Schritt für eine eng verzahnte föderale Cyber-Abwehr. Denn nur eine intensive, dauerhafte und fortgesetzte Zusammenarbeit zwischen Bund und Ländern ermöglicht es, den Gefahren im „grenzenlosen Cyberraum“ eine effektive Antwort entgegen zu setzen. Das BSI wird seinen Beitrag weiter und schnell erhöhen und wirkungsvolle Prävention gegen IT-Sicherheitsvorfälle vorantreiben. Denn jedes Computersystem, das nicht gehackt werden kann, jede IT-basierte Dienstleitung, die nicht gestört werden kann, ist ein elementarer Beitrag zu einer funktionierenden digital vernetzten Gesellschaft.

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.

Advisories / Security Advisories
Empfehlungen der Hersteller an IT-Sicherheitsverantwortliche in Unternehmen und anderen Organisationen zum Umgang mit aufgefundenen Schwachstellen.

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.

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

Brute Forcing
Angriffsmethode nach dem Versuch-Irrtum-Prinzip. Angreifer probieren automatisch viele Zeichenkombinationen aus, um zum Beispiel Passwörter zu knacken und sich Zugang zu passwortgeschützten Systemen zu verschaffen

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 entgegenzunehmen.

Coordinated Vulnerability Disclosure (CVD)
Das Prinzip des Coordinated Vulnerability Disclosure umfasst die koordinierte Veröffentlichung von Informationen zu einer Schwachstelle sowie die Bereitstellung von *Patches* bzw. Mitigationsmaßnahmen für betroffene Software-Produkte in einer transparenten, systematischen zeitlichen Abfolge.

CVSS-Score
Industriestandard, mit dem die Kritikalität von Schwachstellen international vergleichbar bewertet wird.

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 Services 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.

Double Extortion
Angreifer versuchen nicht nur Lösegeld für verschlüs-

selte Daten zu erpressen, sondern auch Schweigegeld für exfiltrierte Daten.

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.

Hybride Bedrohungen
Illegitime Einflussnahme fremder Staaten mit Hilfe von Maßnahmen in verschiedenen Räumen. Physische Angriffe können zum Beispiel durch Cyber-Angriffe oder Desinformationskampagnen begleitet werden.

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.

IT-Sicherheitsgesetz 2.0
Das „Zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ (IT-SiG 2.0) ist am 28. Mai 2021 in Kraft getreten. Das IT-SiG 2.0 ist die Weiterentwicklung des ersten IT-Sicherheitsgesetzes aus 2015.

Lateral Movement
Lateral Movement bezeichnet das sukzessive Bewegen eines Angreifers durch ein infiltriertes Netzwerk. Angreifer setzen dies in der Regel ein, um die für eine Verschlüsselung oder Zerstörung relevanten Daten zu finden.

Legitime Programme
Programme, die unschädliche, erwünschte Operationen ausführen.

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.

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.

NCCA
Das BSI ist die nationale Behörde für Cyber-Sicherheitszertifizierung (engl. National Cybersecurity Certification Authority, kurz NCCA) im Sinne des Artikels 58 Abs. 1 der Verordnung (EU) 2019/881 (Cybersecurity Act, CSA) in Verbindung mit § 9a BSIG. Unter Beachtung des Artikels 58 Abs. 4 CSA führt das BSI als NCCA die Aufsichtsführung und Zertifizierung streng getrennt und unabhängig voneinander durch.

NESAS
Network Equipment Security Assurance Scheme

NESAS CCS-GI
NESAS Cybersecurity Certification Scheme – German Implementation

Password-Spraying
Angriffsmethode, bei der der Angreifer beliebte oder typische Passwörter (z.B. Test1234) verwendet, um auf zahlreiche Konten gleichzeitig Zugriff zu erlangen.

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

Perimeter-Systeme
Server, Firewalls, VPN-Gateways und Router, die direkt aus dem Internet erreichbar sind.

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 einer Internetnutzerin oder 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.

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.

Quellcode
Der Quellcode eines Computerprogrammes ist die in einer Programmiersprache verfasste, für Menschen lesbare Beschreibung des Ablaufs des Programms. Der Quellcode wird durch ein Programm in eine Abfolge von Anweisungen übersetzt, die der Computer ausführen kann.

Ransomware
Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes (engl. 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 oder Ähnliches.

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.

RSA
Der Begriff bezeichnet ein Verfahren der Public-Key-Kryptografie, welches für Signaturen und Verschlüsselung eingesetzt wird und nach den Entwicklern Rivest, Shamir und Adleman benannt ist. Ein Teil des öffentlichen Schlüssels von RSA besteht aus dem RSA-Modul n, einer natürlichen Zahl, die das Produkt zweier geheimer Primzahlen p und q ist. Die Sicherheit von RSA beruht insbesondere auf der Schwierigkeit den RSA-Modul n zu faktorisieren, d.h. nur aus Kenntnis von n die beiden Primfaktoren p und q zu berechnen.

RNG
Der Begriff ist eine Abkürzung für Random Number Generator, dem englischen Wort für Zufallszahlengenerator.

Security Advisory
Empfehlungen an IT-Sicherheitsverantwortliche zum Umgang mit aufgefundenen Schwachstellen.

SCAS
Security Assurance Specification

Scam-Mail
Betrugsmail. Kategorie von Spam-Mails, mit denen Angreifer vorgeben, z. B. Spendengelder zu sammeln.

Scraping
Auslesen von Inhalten aus Webseiten.

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.

SIM-Swapping
Bestellung einer weiteren SIM-Karte zur Mobilfunktnummer im Namen der Nutzerin oder des Nutzers, sodass mTANs an mehrere Geräte gesendet werden.

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.

Smart Grid
Intelligentes Stromnetz, in dem die Aktionen von Erzeugern, Verbrauchern und Speichern intelligent integriert werden. So solle eine effiziente, nachhaltige, wirtschaftliche und sichere Elektroenergieversorgung gewährleistet werden.

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.

Trusted Execution Environment (TEE)
Eine Trusted Execution Environment (TEE) bezeichnet einen isolierten Teil innerhalb eines Systems, welcher eine besonders geschützte Laufzeitumgebung bereitstellt. Die TEE kann bspw. Bestandteil des Hauptprozessors (CPU) oder Teil des Ein-Chip-Systems (SoC) eines Smartphones sein. Die TEE schützt die Integrität und Vertraulichkeit der enthaltenen Daten und des Schlüsselmaterials vor unautorisierten Dritten, z. B. auch der Nutzerin oder dem Nutzer eines Geräts. Lediglich autorisierten Stellen ist es möglich Anwendungen in die TEE einzubringen oder zu verändern.

UP KRITIS
Der UP KRITIS 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.

Webshell
Schadcode, den Angreifer nach dem Einbruch auf einem Webserver installieren. Webshells ermöglichen Angreifern den Remote-Zugang zu Servern und können für die Ausführung von Schadcode verwendet werden.

Wiper
Schadsoftware, die Daten vernichtet. Im Gegensatz zu Ransomware zielen Wiper nicht auf Verschlüsselung mit anschließender Erpressung, sondern auf Sabotage durch endgültige Vernichtung von Daten.

Witnessing
Unter einer Witness-Begutachtung eines Technischen Dienstes versteht man die Begleitung eines durch den Technischen Dienst durchgeführten Audits durch Mitarbeiterinnen und Mitarbeiter des KBA u. a. zur Bewertung der Auditierung, der zugehörigen internen Verfahren und der Kompetenz der Auditoren/innen.

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).

Quellenverzeichnis

1) https://therecord.media/ransomware-tracker-the-latest-figures/
2) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2021.pdf
3) https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Fragen-und-Antworten/fragen-und-antworten_node.html
4) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2021.pdf
5) https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-269486-1032.pdf
6) https://www.bsi.bund.de/Schwachstellenmeldung
7) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf
8) Bundesamt für Verfassungsschutz, "Sicherheitshinweis für die Wirtschaft | 01/2022 | 04.03.2022": https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/wirtschafts-wissenschaftsschutz/2022-03-04-Sicherheitshinweis.pdf
9) https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr
10) https://de.radware.com/2021q3-ddos-report/
11) https://www.link11.com/de/bedrohungslage
12) https://azure.microsoft.com/en-us/blog/business-as-usual-for-azure-customers-despite-24-tbps-ddos-attack/
13) https://blog.cloudflare.com/cloudflare-thwarts-17-2m-rps-ddos-attack-the-largest-ever-reported/
14) https://www.inforisktoday.com/meris-how-to-stop-most-powerful-botnet-on-record-a-17574; https://www.cysecurity.news/2022/01/russia-recorded-largest-botnet-attack.html
15) https://www.documentcloud.org/documents/7070798-FLASH-MU-000132-DD.html
16) https://www.zdnet.de/88395308/erneute-welle-von-ddos-erpressungen-durch-fancy-lazarus/
17) hhttps://www.link11.com/de/blog/bedrohungslage/cyber-angriffe-am-black-friday-wochenende-brechen-rekorde/
18) https://fermatattack.secvuln.info
19) https://securitylab.github.com/advisories/GHSL-2021-1012-keypair/
20) https://www.spiegel.de/wissenschaft/technik/russland-ukraine-was-der-ausfalleines-satellitennetzwerks-mit-deutschen-windkraftanlagen-zu-tun-hat-a-22850ad5-dee2-42c4-8c5a-c2b39ac42da4 (Stand: 20.04.2022)
21) https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/ (Stand: 29.04.2022)
22) https://www.lefigaro.fr/secteur/high-tech/les-telecoms-victimes-de-cyberattaques-russes-20220228 (Stand: 20.04.2022)
23) https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/ (Stand: 29.04.2022)
24) https://cert.gov.ua/article/39518 (Stand: 13.05.2022); https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf (Stand: 13.05.2022); https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ (Stand: 13.05.2022)
25) https://www.vzbv.de/pressemitteilungen/anbieter-und-hersteller-zu-it-sicherheit-verpflichten
26) https://cdr-initiative.de/uploads/files/210503_Umfrage_FInal_Faktenblatt_CDR.pdf
27) https://www.bmj.de/DE/Themen/FokusThemen/CDR_Initiative/_downloads/cdr_plattform.pdf
28) https://cdr-initiative.de/kodex
29) https://www.bundesnetzagentur.de/DE/Fachthemen/Digitalisierung/start.html
30) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/messenger.html
31) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSI-Magazin_2022_01.html
32) https://www.bsi.bund.de/SharedDocs/Videos/DE/BSI/VerbraucherInnen/statementvideo-messenger-verschluesselung.html
33) https://datatracker.ietf.org/wg/mls/about/
34) https://www.europarl.europa.eu/factsheets/de/sheet/45/energiebinnenmarkt
35) https://www.bmwk.de/Redaktion/DE/Publikationen/Studien/it-dienstleister-als-akteure-zur-staerkung-der-it-sicherheit-bei-kmu-in-deutschland.html
36) https://www.bmwk.de/Redaktion/DE/Publikationen/Studien/it-dienstleister-als-akteure-zur-staerkung-der-it-sicherheit-bei-kmu-in-deutschland.html
37) auch BKA-Veröffentlichung: https://www.bka.de/SharedDocs/Downloads/DE/UnsereAufgaben/Deliktsbereiche/InternetKriminalitaet/CyberattackenUnternehmen.pdfl
38) https://ntia.gov/SBOM
39) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html
40) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Sichere_Nutzung_Cloud_Dienste.pdf
41) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html
42) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03160/tr03160_node.html
43) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03107/TR-03107_node.html
44) https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Elektronische-Identitaeten/Identitaetspruefung/identitaetspruefung_node.html
45) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03116/TR-03116_node.html

Verzeichnis der im Dokument abgebildeten QR-Codes

a) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.html
b) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Technische-Sicherheitshinweise-und-Warnungen/technische-sicherheitshinweise-und-warnungen_node.html
c) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-CC/itsicherheitszert.html
d) https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/Bewertung-2FA-Verfahren/bewertung-2fa-verfahren_node.html
e) https://www.bsi.bund.de/DE/Service-Navi/FAQ/IT-SicherheitskennzeichenVerbraucher/faq_it-sik-verbraucher_node.html
f) https://www.bsi.bund.de/DE/Themen/Kampagne-einfach-absichern/kampagne_node.html
g) https://www.dialog-cybersicherheit.de/
h) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartCity/Handlungsempfehlungen_Smart_City.pdf?__blob=publicationFile&v=3
i) https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Moderner-Staat/Online-Wahlen/online-wahlen_node.html
j) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Sicher_zahlen_im_E_Commerce.pdf
k) https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung_node.html
l) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html
m) https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/Stand-der-Technik-umsetzen/Uebersicht-der-B3S/uebersicht-der-b3s_node.html
n) https://www.bsi.bund.de/DE/Home/home_node.html
o) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/ohsza.html
p) https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/UP-KRITIS/up-kritis_node.html
q) https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Weitere_regulierte_Unternehmen/UBI/ubi_node.html
r) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/KMU/KMU_node.html
s) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03163/tr-03163.html
t) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-NESAS/NESAS-CCS-GI_node.html
u) https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html
v) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/5-G/KoPa45/Cyber-Sicherheit-digitale-Souveraenitaet-5G-6G_node.html
w) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Onlinekurs/Onlinekurs_node.html
x) https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Moderner-Staat/Online-Zugangsgesetz/IT-Sicherheitsverordnung_PVV/IT-Sicherheitsverordnung_PVV_node.html
y) https://www.bsi.bund.de/DE/Service-Navi/Publikationen/BSI-Magazine/bsi-magazine_node.html
z) https://cybersecurity-centre.europa.eu/index_de
aa) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Profil_Weltrauminfrastrukturen.html
bb) https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KI/Towards_Auditable_AI_Systems_2022.pdf
cc) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Kryptografie-quantensicher-gestalten.html
dd) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Eckpunkte_SSI_DLT.pdf
ee) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Kryptografie-quantensicher-gestalten.pdf?__blob=publicationFile&v=5

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
Oktober 2022

Druck
Appel & Klinger Druck und Medien GmbH, Schneckenlohe

Gestaltung
Faktor 3 AG

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

Illustrationen
Koivo c/o kombinatrotweiss.de
Instagram: koivo | kombinatrotweiss_illustration

Grafiken
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Artikelnummer
BSI-LB22/511