



Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI



Die Lage der IT-Sicherheit in Deutschland 2020

Vorwort

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die Cyber-Sicherheitsbehörde des Bundes. Ihre Aufgabe ist es, Deutschland digital sicher zu machen. Der vorliegende Bericht zur Lage der IT-Sicherheit in Deutschland im Jahr 2020 macht erneut deutlich, wie wichtig die Aufgabe ist und dass die Herausforderungen vielfältig und komplex sind.

Cyber-Angriffe werden immer ausgefeilter. Gleichzeitig wird die IT-Abhängigkeit der Unternehmen, des Staates und der Bürger immer größer, wodurch das Schadenspotenzial zunimmt.

Die Corona-Pandemie hat uns nochmals deutlich vor Augen geführt, welche Bedeutung funktionierende und sichere IT-Infrastrukturen haben. IT-Sicherheit muss deshalb bei allen Digitalisierungsvorhaben einen Schwerpunkt bilden und von Anfang an mitgedacht und umgesetzt werden.

Im Berichtszeitraum ging eine große Bedrohung für Staat, Wirtschaft und Gesellschaft von der Schadsoftware Emotet aus. Die geschickte Kombination eines digitalen Werkzeugkastens mit Social Engineering lässt Infektionen auch bei professionellen Anwendern zu. Alle sind digital verwundbar. Ist ein System erst einmal infiziert, analysieren es die Täter und erpressen ihre Opfer mit der Verschlüsselung der Daten oder mit der Androhung ihrer Veröffentlichung. Je nach Ausmaß der Infektion kann es für Wirtschaftsunternehmen zu kurzfristigen Arbeits- und Produktionseinschränkungen bis hin zu einem kompletten Ausfall für mehrere Wochen oder Monate kommen.

Ich bin froh, dass wir mit dem BSI und den anderen Sicherheitsbehörden starke Partner haben, die jeden Tag ihr Bestes geben, um Privatanwender, Unternehmen und Behörden vor den Gefahren aus dem digitalen Raum zu schützen.

Neben seiner Rolle als „Sicherheitsdienstleister“ der Bundesverwaltung hat das BSI für Wirtschaft und Gesellschaft ein breites Portfolio an Dienstleistungen im Angebot. So fungiert es als zentrale Stelle und Informationsdrehscheibe für die IT-Sicherheit in Kritischen Infrastrukturen und entwickelt Sicherheitsanforderungen für die zukünftigen 5G-Netze. Außerdem stellt das BSI unter dem Motto „BSI für Bürger“ vielfältige Informationen zu Risiken und Schutzmaßnahmen bei der Nutzung des Internets bereit. Kurz nach Ausbruch der Corona-Pandemie hat das BSI Hinweise für sicheres mobiles Arbeiten zur Verfügung gestellt. Bei der

Entwicklung der Corona-Warn-App hat das BSI von Beginn an beraten, um ein Höchstmaß an IT-Sicherheit zu gewährleisten.

Wir müssen uns der stetig wechselnden Gefahrenlage anpassen. Deshalb möchte ich die Fähigkeiten des BSI weiter ausbauen und seine Rolle als Cyber-Sicherheitsbehörde des Bundes stärken. Hierfür werden wir noch in dieser Legislaturperiode das IT-Sicherheitsgesetz 2.0 auf den Weg bringen.

Zudem habe ich veranlasst, dass in den nächsten Monaten die Cyber-Sicherheitsstrategie der Bundesregierung fortgeschrieben wird. Die aus dem Jahr 2016 stammende Strategie benennt viele wichtige Ziele der nationalen und internationalen Cyber-Politik. Diese Ziele und die damit verbundenen Maßnahmen werden nun überprüft und zukunftsgerichtet neu formuliert.

Das Spektrum an Projekten im Bereich IT-Sicherheit ist mannigfaltig. Der Bericht zur Lage der IT-Sicherheit in Deutschland 2020, in dem das BSI die aktuelle Gefährdungslage sowie seine Tätigkeiten zur Eindämmung der Gefahren darstellt, spiegelt dies wider.



Horst Seehofer

Bundesminister des Innern, für Bau und Heimat

Vorwort

Deutschland – Digital – Sicher – BSI

Der bayerische Priester Sebastian Kneipp machte Mitte des 19. Jahrhunderts die später nach ihm benannte Wassertherapie bekannt und populär. Diese basiert auf dem Reizeffekt, den kaltes Wasser auf den menschlichen Körper hat und durch den im Körper Prozesse in Gang gesetzt oder befördert werden, die zur Heilung beitragen können. Einen ähnlichen Effekt haben wir in der ersten Jahreshälfte 2020 erlebt, als die Corona-Pandemie dazu führte, dass viele Menschen über Monate hinweg zu Hause bleiben und gewohnte Abläufe im privaten und geschäftlichen Bereich von heute auf morgen gestoppt und umgestellt werden mussten. Corona war für viele Menschen ein Schockmoment, und das in vielerlei Hinsicht.

Auch im Bereich der Informationssicherheit hat Corona für Veränderungen gesorgt. So hat sich einmal mehr gezeigt, wie flexibel die Online-Kriminalität auf neue Themen und Gegebenheiten reagiert und diese für ihre kriminellen Zwecke ausnutzt. Gleichzeitig hat aber auch das BSI gezeigt, dass es sich auf diese Krisensituation sehr schnell eingestellt und mit entsprechenden Empfehlungen und Gegenmaßnahmen im Bereich der Prävention, Detektion und Reaktion wirkungsvoll reagiert hat.

Haben wir „vor Corona“ noch sehr intensiv über Themen wie 5G, Künstliche Intelligenz, das Smart Home oder das vernetzte, autonome Fahren diskutiert, so traten diese Themen mit Beginn der Corona-Pandemie in den Hintergrund der öffentlichen Debatte. Das BSI jedoch hat diese Themen nie aus den Augen verloren. Vielmehr haben wir weiterhin sehr intensiv daran gearbeitet, die Informationssicherheit in diesen für den Standort Deutschland wichtigen Bereichen zu gestalten und voranzutreiben. Denn unser Job als Cyber-Sicherheitsbehörde des Bundes – als „Kernstück für die Sicherheit in der Digitalisierung“, wie Kanzleramtsminister Dr. Helge Braun das BSI einmal bezeichnete – ist es, den Anwendern in Staat, Wirtschaft und Gesellschaft dabei zu helfen, diese neuen Technologien sicher einsetzen zu können und die im vorliegenden „Bericht zur Lage der IT-Sicherheit in Deutschland“ beschriebene Gefährdungslage zu bewältigen. Dies tun wir, unter anderem indem wir Sicherheitsstandards definieren und für deren Umsetzung sorgen. Und indem wir Anwendern lebensnahe und praxisorientierte Empfehlungen an die Hand geben, mit denen sie sich sicher in der digitalen Welt bewegen können.

Abseits der teils tragischen medizinischen und epidemiologischen Entwicklungen hat die Corona-Pandemie gezeigt, wie bedeutend funktionierende, sichere Infor-

mationstechnik ist, im privaten Alltag ebenso wie im globalen, wirtschaftlichen Miteinander. Die positiven Entwicklungen und Prozesse, den Entwicklungsschub, den die Digitalisierung in Deutschland durch Corona erfahren hat, gilt es, in die Nach-Corona-Zeit mitzunehmen und weiter nachhaltig auszubauen. Dies wird nur gelingen, wenn wir weiterhin die Risiken von vornherein mitdenken und möglichst ausschließen. Dafür steht unser Motto „Deutschland – Digital – Sicher – BSI“, und daran arbeiten wir intensiv.



A handwritten signature in black ink that reads "Arne Schönbohm".

Arne Schönbohm

Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI)

Inhaltsverzeichnis

Vorworte

Vorwort Horst Seehofer, Bundesminister des Innern, für Bau und Heimat	3
Vorwort Arne Schönbohm, Präsident des BSI	4

1 Gefährdungslage

1.1 Schadprogramme	9
1.1.1 Zunahme der Anzahl neuer Schadprogramm-Varianten	9
1.1.2 Emotet: Neue Qualität fortschrittlicher Angriffe	11
1.1.3 Ransomware	11
1.1.4 Spam und Malware-Spam	15
1.1.5 Botnetze	16
1.2 Diebstahl und Missbrauch von Identitätsdaten	18
1.2.1 Phishing und weitere Betrugsformen	18
1.2.2 Schadprogramme für den Diebstahl von Identitätsdaten	20
1.2.3 Daten-Leaks	20
1.3 Schwachstellen	22
1.3.1 Schwachstellen in Software-Produkten	22
1.3.2 Schwachstellen in Hardware-Produkten	26
1.4 Advanced Persistent Threats	28
1.5 Distributed Denial of Service	29
1.6 Angriffe im Kontext Kryptografie	30
1.7 Hybride Bedrohungen	32
1.8 Gefährdungen der Cyber-Sicherheit durch die COVID-19-Pandemie	33
1.9 Zusammenfassung und Bewertung der Gefährdungslage	34

2 Zielgruppenspezifische Erkenntnisse und Lösungen

2.1 Gesellschaft	39
2.1.1 Erkenntnisse aus Umfragen zum Bild der Gefährdungslage in der Gesellschaft	39
2.1.2 Digitaler Verbraucherschutz	40
2.1.3 Das IT-Sicherheitskennzeichen – Transparenz für Verbraucherinnen und Verbraucher	41
2.1.4 Gesellschaftlicher Dialog für Cyber-Sicherheit	42
2.1.5 Information und Sensibilisierung von Bürgerinnen und Bürgern	42
2.1.6 Sicherheit von Wearables, Smart Home und dem Internet der Dinge	44
2.1.7 Sicherheit von Medizinprodukten	44
2.1.8 Corona-Warn-App	46
2.1.9 eHealth / elektronische Gesundheitskarte	46

2.1.10	Sicherheit von Bezahlverfahren	46
2.1.11	Zwei-Faktor-Authentisierung	47
2.1.12	Bewertung von elektronischen Identifizierungsverfahren	48
2.1.13	Sichere elektronische Identitäten auf dem Smartphone	49
2.1.14	Biometrie im Zeitalter der künstlichen Intelligenz	50
2.2	Wirtschaft / Kritische Infrastrukturen	51
2.2.1	Gefährdungslage Wirtschaft mit besonderer Betrachtung Kritischer Infrastrukturen	52
2.2.2	UP KRITIS	55
2.2.3	Zertifizierung intelligenter Messsysteme im Energiebereich	56
2.2.4	Moderne Telekommunikationsinfrastrukturen (5G)	57
2.2.5	IT-Sicherheit in intelligenten Verkehrssystemen (C-ITS)	58
2.2.6	Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme	59
2.2.7	Zertifizierung	60
2.2.8	IT-Grundschutzprofile und Testate	61
2.2.9	Unterstützung beim sicheren Umstieg ins Home-Office	62
2.2.10	Allianz für Cyber-Sicherheit	62
2.2.11	Dialog verschiedener Cyber-Sicherheitsinitiativen in Deutschland	63
2.2.12	Sonstige Lösungen / Angebote für die Wirtschaft	63
2.3	Staat / Verwaltung	64
2.3.1	Gefährdungslage der Bundesverwaltung	65
2.3.2	Nationales Cyber-Abwehrzentrum (Cyber-AZ)	66
2.3.3	Bundes Security Operations Center (BSOC)	66
2.3.4	Computer Emergency Response Team für Bundesbehörden	67
2.3.5	Nationales Verbindungswesen	68
2.3.6	Realisierung des Umsetzungsplans Bund (UP Bund)	68
2.3.7	Informationssicherheitsberatung	68
2.3.8	Smart Borders und hoheitliches Identitätsmanagement	69
2.3.9	Technologieverifikation in sogenannten Security Labs	69
2.3.10	App-Testing für mobile Lösungen	70
2.3.11	Abstrahlsicherheit	70
2.3.12	Lauschabwehr	71
2.3.13	VS-Zulassung und Herstellerqualifizierung	71
2.3.14	Umsetzung des Online-Zugangsgesetzes: Komponenten für die sichere Digitalisierung von Verwaltungsprozessen	72
2.4	Internationales	73
2.4.1	Internationales Engagement des BSI	73
2.4.2	eID: Europäische Anerkennung der Online-Ausweisfunktion	73
2.5	Sonstige Entwicklungen in der IT-Sicherheit	74
2.5.1	Künstliche Intelligenz	74
2.5.2	Kryptografie	75
2.5.3	Blockchain-Technologie	76
3	Fazit	78
4	Glossar	82
5	Quellenverzeichnis	85

1 Gefährdungslage



1 Gefährdungen der Cyber-Sicherheit in Deutschland

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beobachtet die Gefährdungslage der IT-Sicherheit in Deutschland kontinuierlich. Der vorliegende Bericht bezieht sich auf den Zeitraum vom 1. Juni 2019 bis 31. Mai 2020 (Berichtszeitraum), greift aber auch Ereignisse danach auf. Die Gefährdungslage der IT-Sicherheit bleibt in diesem Zeitraum angespannt. Dabei konnte eine Fortsetzung des Trends beobachtet werden, dass Angreifer Schadprogramme für cyber-kriminelle Massenangriffe auf Privatpersonen, Unternehmen und andere Institutionen nutzen. Auch Abflüsse von personenbezogenen Daten, in diesem Berichtszeitraum u. a. von Patientendaten, sowie kritische Schwachstellen in Software- und Hardwareprodukten konnten beobachtet werden.

1.1 Schadprogramme

Zu Schadprogrammen zählen alle Computerprogramme, die schädliche Operationen ausführen oder andere Programme hierzu befähigen können. Schadprogramme gelangen in der Regel über Anhänge oder Links in E-Mails auf einen Computer. Wenn Nutzerinnen oder Nutzer auf einen solchen Anhang oder auf einen Link klicken, der auf eine manipulierte Webseite führt, wird ein Schadprogramm installiert. Darüber hinaus zählen unbemerkte Downloads im Hintergrund (sogenannte *Drive-by-Downloads*¹) sowie malizöse Erweiterungen von legitimen Programmen zu den typischen *Angriffsvektoren*. Für die Infektion nutzen Schadprogramme in der Regel Schwachstellen aus. Diese können in Software- oder Hardware-Produkten, an Netzwerübergängen, zum Beispiel zwischen Büro- und Produktionsnetzwerken oder zum offenen Internet, sowie im Fall von *Social Engineering* durch menschliches Versagen auftreten.

Die einzelnen Schadprogramme unterscheiden sich im Hinblick auf ihre Funktionalität, wobei ein Schadprogramm auch mehrere Funktionalitäten aufweisen kann. Als *Ransomware* werden beispielsweise Schadprogramme bezeichnet, die etwa durch Verschlüsselung den Zugang zu Daten oder Systemen einschränken, um anschließend ein Lösegeld zu erpressen (vgl. Kapitel *Ransomware*, Seite 11). Schadprogramme, die sich als gutartige Software tarnen oder in legitimen Dateien verstecken, werden als Trojaner bezeichnet (vgl. Kapitel *Emotet: Neue Qualität fortschrittlicher*

Angriffe, Seite 11) und solche, die zum Beispiel mit Hilfe von Command-and-Control-Servern fernsteuerbar sind, als *Bot* (vgl. Kapitel *Botnetze*, Seite 16).

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

1.1.1 Zunahme der Anzahl neuer Schadprogramm-Varianten

Neue Varianten eines Schadprogramms entstehen, wenn im Programmcode Änderungen vorgenommen werden. Während für bekannte Schadprogramm-Varianten Detektionsmethoden existieren, sind neue Varianten unmittelbar nach ihrem Auftreten noch nicht als Schadprogramme erkennbar und daher besonders gefährlich.

Die Anzahl neuer Schadprogramm-Varianten hat im aktuellen Berichtszeitraum um rund 117,4 Millionen zugenommen (siehe Abbildung 1; Quelle dieser und der folgenden Daten: BSI-Auswertung von Rohdaten des Instituts AV-Test GmbH).

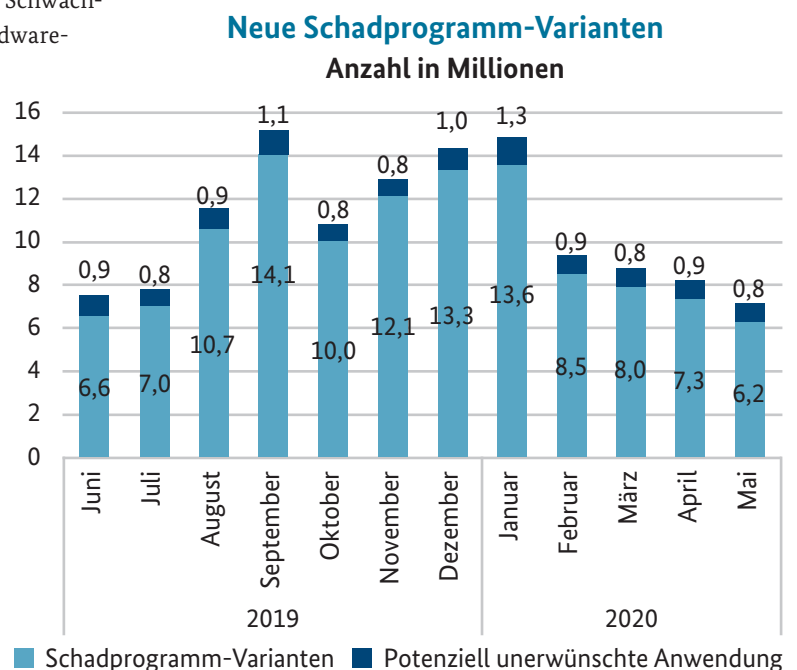


Abbildung 1 Neue Schadprogramm-Varianten,

Quelle: BSI-Auswertung von Rohdaten des Instituts AV-Test GmbH

¹ Kursiv gesetzte Begriffe werden im Glossar erläutert.

Täglicher Zuwachs neuer Schadprogramm-Varianten* Anzahl in 1000

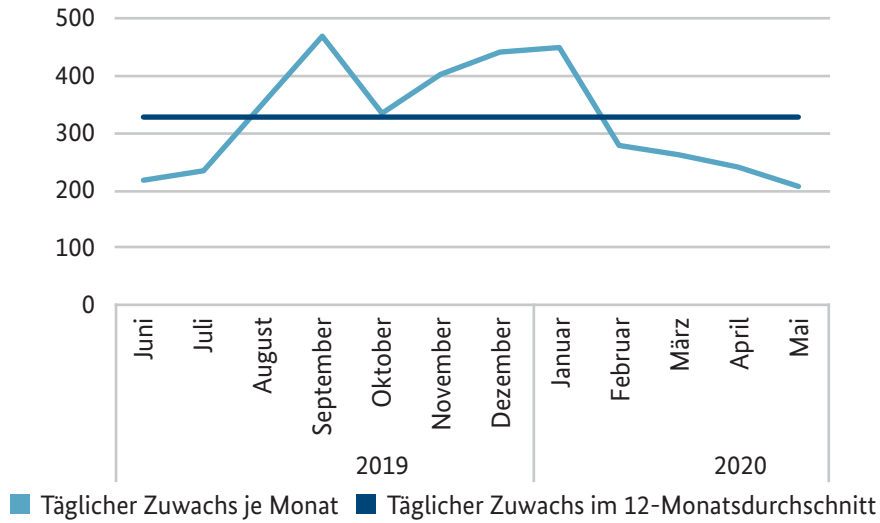


Abbildung 2 Täglicher Zuwachs neuer Schadprogramm-Varianten,
Quelle: BSI-Auswertung von Rohdaten des Instituts AV-Test GmbH
*ohne PUA

Besonders stark fiel der Zuwachs im September 2019 mit 14,1 Millionen neuen Schadprogramm-Varianten und 1,1 Millionen neuen Varianten potenziell unerwünschter Anwendungssoftware (PUA)² aus. Auch um den Jahreswechsel waren hohe Aufkommen zu verzeichnen.

Dies entsprach einem durchschnittlichen Zuwachs von rund 322.000 neuen Schadprogramm-Varianten pro Tag im Berichtszeitraum (siehe Abbildung 2). Allerdings waren erhebliche Schwankungen zu verzeichnen. So lag der Indikator Mitte 2019 noch bei 220.000 neuen Varianten pro Tag und damit 32 Prozent unter dem Durchschnittswert des Berichtszeitraums. Im September 2019 trat dann mit täglich durchschnittlich knapp 470.000 (46 Prozent über dem Durchschnittswert des Berichtszeitraums) neuen Varianten ein überdurchschnittlich hoher Zuwachs auf.

Im Februar 2020 brach die Welle neuer Schadsoftware-Varianten abrupt ein und stabilisierte sich anschließend auf unterdurchschnittlichem Niveau.

Wellen neuer Schadprogramm-Varianten, die im vierten Quartal beginnen und bis in das erste Quartal des neuen Jahres reichen, treten regelmäßig auf. Im Vergleich zu früheren Berichtszeiträumen fiel die Welle im aktuellen Zeitraum flacher, jedoch nicht weniger bedrohlich aus. Das lag insbesondere an den neuen Varianten der Schadsoftware Emotet, die seit September 2019 wieder verstärkt für Cyber-Angriffe verwendet wurde. Das Auftreten von Emotet markiert einen Methodenwechsel der Angreifer. Waren früher noch ungezielte Massenangriffe auf zufällig getroffene Ziele das Mittel der Wahl, so werden Schadsoftware-Angriffe mittlerweile immer intelligenter und – durch einen geschickt kombinierten Einsatz verschiedener Schadprogramme – gezielter.

1.1.2 Emotet: Neue Qualität fortschrittlicher Angriffe

Emotet dominierte im Berichtszeitraum die IT-Sicherheitsbedrohungen durch Schadprogramme. Der ehemalige Banking-Trojaner vereint vielfältige Schadfunktionen. So sind beispielsweise verschiedene Software-Module zum Ausspähen von Informationen (vgl. Kapitel *Diebstahl und Missbrauch von Identitätsdaten*, Seite 18), zum Spamversand (vgl. Kapitel *Spam und Malware-Spam*, Seite 15) sowie zum Nachladen weiterer Schadprogramme enthalten. Zudem besitzt Emotet Wurm- und Bot-Funktionalitäten (vgl. Kapitel *Botnetze*, Seite 16). Das Schadprogramm kann sich demnach nicht nur automatisiert in einem Netzwerk verbreiten, sondern auch Kontakt zu einem Command-and-Control-Server aufnehmen, um von dort Befehle der Angreifer entgegenzunehmen und im infizierten Netzwerk auszuführen.

Diese vielfältigen Schadfunktionen bieten den Angreifern zahlreiche neue und fortschrittliche *Angriffsvektoren*. Dabei kommen Methoden in massenhafter Weise zum Einsatz, die zuvor nur bei gezielten, aufwändigen und fachlich anspruchsvollen Angriffen auf herausgehobene Ziele beobachtet wurden (z. B. bei einem APT-Angriff auf ein einzelnes Unternehmen, vgl. Kapitel *Advanced Persistent Threats*, Seite 28). Dies illustriert die dreistufige Angriffsstrategie mit Emotet, der Schadsoftware Trickbot und der Ransomware Ryuk:

1. Emotet-Infektion durch Social Engineering im Schneeballprinzip: Emotet wird per E-Mail verbreitet. Als E-Mail-Anhang wird es zum Beispiel als Bewerbungsschreiben oder in manipulierten Bilddateien getarnt. Als Link in E-Mails wird es auf Webseiten verborgen und nach dem Klick auf den Link installiert. Um Nutzerinnen und Nutzer zum Klick zu verleiten, kommen fortschrittliche *Social-Engineering*-Techniken zum Einsatz. Nach einer erfolgreichen Infektion späht Emotet die E-Mail-Kommunikation des Opfers aus (sogenanntes Outlook-Harvesting) und nutzt diese, um Kommunikationspartner wie beispielsweise Geschäftspartner des Opfers anzugreifen. Die Kommunikationspartner erhalten dann ihrerseits E-Mails mit schädlichen Anhängen, die beim Klick Emotet installieren. Mit Hilfe der zuvor erbeuteten E-Mail-Kommunikationsverläufe generiert Emotet automatisiert täuschend echt wirkende Antworten auf vermeintlich vom Opfer stammende E-Mails und verbreitet diese massenhaft weiter. Aufgrund der bekannten Betreffzeilen und zitierten E-Mail-Inhalte werden Empfänger häufig erfolgreich zum Klicken verleitet. Diese Angriffsmethode kann praktisch ohne weiteres Zutun der Angreifer automatisiert durch die Schadsoftware ausgeführt werden.

2. Spionage und Persistenz durch Trickbot: Nach erfolgreicher Infektion eines Systems lädt Emotet weitere Schadsoftware nach; im Berichtszeitraum handelte es sich häufig um Trickbot. Trickbot besitzt Spionage- und Sabotagekomponenten und kann automatisiert das Netzwerk des Betroffenen vollständig kompromittieren – bis hin zu zentralen Systemen wie dem Domain-Controller im Active Directory, der für die zentrale *Authentifizierung* von Nutzerinnen und Nutzern sowie die Zuweisung von Rechten und Rollen zuständig ist. Der Angreifer verfügt dadurch über alle Rechte, um beispielsweise Benutzerkonten mit Administratorrechten anzulegen, Daten einzusehen und abfließen zu lassen oder Hintertüren (sogenannte *Backdoors*) für einen längerfristigen Verbleib im infizierten System einzurichten. Zudem sammelt Trickbot eigenständig Informationen über Systeme, Benutzer und installierte Software des Opfers und übermittelt diese an die Angreifer.

3. Monetarisierung durch die Ryuk-Ransomware: Es ist davon auszugehen, dass die Angreifer auf Basis der von Trickbot beschafften Informationen entscheiden, ob sie anschließend über den Fernzugriff von Trickbot auch noch manuell auf das Netzwerk des Opfers zugreifen. Erscheint ihnen das Ziel zahlungsfähig, wird die *Ransomware* Ryuk gleichzeitig auf allen erreichbaren Servern und Systemen des Opfers verteilt. Aufgrund der von Trickbot beschafften weitreichenden Rechte werden oft auch *Backups* verschlüsselt. Anschließend erfolgt häufig eine Lösegeldforderung.

Die Schadwirkung dieser Vorgehensweise ist immens. Betroffene Unternehmen, Behörden, wissenschaftliche Einrichtungen und andere Institutionen müssen unter Umständen hohe Kosten für die Wiederherstellung von Systemen, für Produktionsausfälle und ausbleibende Umsätze in Kauf nehmen. Im Berichtszeitraum wurden zudem Lösegeldforderungen bis in den achtstelligen Bereich beobachtet.

1.1.3 Ransomware

Ransomware stellt bereits seit einigen Jahren eine der größten Bedrohungen für Nutzerinnen und Nutzer von IT-Systemen dar, denn der erfolgreiche Einsatz dieser Art von Schadsoftware verhindert den Zugriff auf lokale oder im Netzwerk erreichbare Daten und Systeme. Am häufigsten wird hierzu eine Verschlüsselung von Nutzerdaten (wie Office-, Bild-, Ton- und Videodateien) oder ganzer Datenbanken durchgeführt. Die Opfer erhalten anschließend eine Nachricht, dass die Beschränkung bei Zahlung eines Lösegelds (Ransom) wieder aufgehoben werde. Dabei werden häufig sehr kurze Fristen gesetzt und mit der sukzessiven Löschung oder Veröffentlichung der



Emotet als Türöffner: Ransomware-Angriff auf die Stadtverwaltung einer mittelgroßen deutschen Stadt

Sachverhalt

Am 6. September 2019 entdeckte die IT-Abteilung der Stadtverwaltung einer mittelgroßen deutschen Stadt, dass die örtlichen Systeme kompromittiert worden waren. Um eine weitere Ausbreitung der Infektion zu verhindern, setzten die Zuständigen die Server vorerst außer Betrieb. Bereits vorher waren jedoch große Teile der Datenbanken und Dokumente der Stadtverwaltung, einschließlich der *Backups*, verschlüsselt worden. Anschließend wurde ein Lösegeld gefordert.

Der Türöffner für den *Ransomware*-Angriff war Emotet. Vermutlich im Anhang einer durch *Social-Engineering*-Methoden authentisch wirkenden E-Mail hatte Emotet die Stadtverwaltung erreicht und infiziert. Virens Scanner konnten die Infektionen nicht verhindern.

Es gelang den Angreifern, die *Ransomware* Ryuk auf den infizierten Systemen auszurollen und rund 550.000 Dateien zu verschlüsseln, darunter Elterngeldanträge, Baupläne und vieles mehr. Die Verwaltungsgeschäfte kamen nahezu vollständig zum Erliegen. Es dauerte mehr als eine Woche, bis erste Systeme wieder in Betrieb genommen werden konnten. Einzelne Dienstleistungen konnten bis ins erste Quartal 2020 hinein nicht angeboten werden.

Reaktion

Da Emotet nicht nur Schadsoftware nachlädt, sondern auch die E-Mail-Kommunikation ausliest, um diese in weiteren Angriffen verwenden zu können, wurden externe Partner der Stadtverwaltung telefonisch aufgeklärt, keine E-Mails zu öffnen, die vermeintlich von der Stadtverwaltung stammten.

Für die Bereinigung der Systeme konnte ein sauberes, noch unverschlüsseltes *Backup* der Buchhaltungsdaten wieder eingespielt werden. Andere Dateien mussten neu erstellt werden; darunter die Planung eines Neubaugebiets. Auf Empfehlung des BSI wurden rund 300 Rechner neu aufgesetzt. Es fielen geschätzte Mehrausgaben für den IT-Neuaufbau von etwa 500 Euro je Rechner an.

Darüber hinaus wurden strengere Regeln für E-Mail-Anhänge eingeführt, sodass mehr Anhänge automatisch abgelehnt werden. Zudem wurde das Netzwerk stärker segmentiert, um die Ausbreitung von Schadsoftware bei einem eventuellen zukünftigen Angriff zu erschweren. Auch Bandsicherungen (*Offline-Backups*), die in Tresoren gelagert werden, wurden wieder eingeführt.

Empfehlung

Regelmäßige *Backups* sind die wichtigste Vorsorgemaßnahme, um nach einem *Ransomware*-Angriff schnell wieder handlungsfähig zu werden. Damit *Backups* im Fall eines Angriffs nicht mitverschlüsselt werden, müssen sie getrennt von den übrigen Systemen offline gesichert werden. Zudem sollte regelmäßig geprüft werden, ob sie sich im Notfall schnell wieder einspielen lassen.

verschlüsselten Daten gedroht (vgl. Kapitel *Diebstahl und Missbrauch von Identitätsdaten*, Seite 18). Die Lösegeldzahlungen werden üblicherweise in digitalen (virtuellen) Währungen (z. B. *Bitcoin*) abgewickelt, um die Strafverfolgung zu erschweren. Neben der echten Lösegelderpressung wurden aber auch Angriffe beobachtet, die den Anschein eines *Ransomware*-Angriffs erwecken, tatsächlich aber der Ablenkung von anderen Angriffen oder auch als reine Sabotageakte dienen.

Ransomware wird über die bei Schadprogrammen üblichen *Angriffsvektoren* als E-Mail-Anhang oder als Link

verbreitet, der auf eine infizierte Webseite führt (vgl. Kapitel *Schadprogramme*, Seite 9). Einen *Angriffsvektor*, der speziell für Unternehmen und andere Einrichtungen mit größerer IT-Infrastruktur gefährlich ist, stellen Schwachstellen in Fernwartungs- und *VPN*-Zugängen dar. Sie werden verwendet, um auf die zu wartenden Systeme zuzugreifen und/oder aus der Ferne auf ihnen zu arbeiten. Ihre Kompromittierung führt oft bereits im ersten Schritt dazu, dass der Angreifer anschließend mit weitgehenden Rechten ausgestattet ist. Weiterführende Informationen finden sich unter www.bsi.bund.de/ransomware (vgl. *Quellenverzeichnis*¹: www.bsi.bund.de).

Im aktuellen Berichtszeitraum setzte sich der Trend zu gezielten Angriffen auf komplette Netzwerke von Unternehmen oder anderen Institutionen fort. Zudem zeigte sich ein Trend zu gezielten Angriffen auf finanzstarke Opfer.

So wurden Automobilhersteller und ihre Zulieferer, verschiedene Flughäfen oder Fluggesellschaften, aber auch weniger bekannte Unternehmen mit hohen Umsätzen angegriffen. Auch kleinere Betriebe wurden angegriffen, die sich durch Alleinstellungsmerkmale wie zum Beispiel die Produktion spezieller Komponenten im Maschinenbau auszeichnen oder schlechte Schutzmechanismen aufwiesen.

Auch Einrichtungen der öffentlichen Verwaltung, insbesondere auf kommunaler Ebene, wurden zum Ziel von Angriffen durch *Ransomware*. Zudem waren auch Universitäten betroffen. Ebenso sind medizinische Einrichtungen, besonders Krankenhäuser, im Berichtszeitraum Opfer von Angriffen geworden.

Neben diesen gezielten Angriffen gab es auch im aktuellen Berichtszeitraum weiterhin *Ransomware*, die breit gestreut wurde (z. B. Sodinokibi). Die Angreifer versuchen dabei, ihre Gewinne über eine hohe Anzahl von Opfern zu maximieren. Mit Hilfe von *Social Engineering* in Spam-E-Mails werden viele Nutzerinnen und Nutzer zu Klicks auf schädliche E-Mail-Anhänge oder Links verleitet. Dabei wird die persönliche Vertrautheit von Namen oder die Neugier auf Neuigkeiten bei aktuellen Themen genutzt. Geschickt werden auch berufliche Zwänge missbraucht, etwa der Zwang von Mitarbeiterinnen und Mitarbeitern einer Personalverwaltung, Bewerbungsschreiben zu öffnen und damit eventuell schädliche Makros auszulösen. Eine *Ransomware* dieser Art ist Sodinokibi (bzw. Sodin oder REvil), die der vermutete Vorgänger GandCrab in einer besonderen Art als „Dienstleistungsmodell“ (*Ransomware-as-a-Service*) vertrieben wurde.

Der Ablauf bei dieser Art von Erpressung unterscheidet sich von dem bei netzwerkweiten Angriffen. In der Erpresserbotschaft werden die Opfer auf eine spezielle Webseite geleitet, welche im Tor-Netzwerk³ betrieben wird. Die Angreifer stellen hier häufig eine Infrastruktur bereit, über die ihre Opfer die Zahlung des Lösegelds abwickeln und anschließend ein entsprechendes Entschlüsselungsprogramm herunterladen können. Bei manuell ausgerollter *Ransomware* wie Ryuk enthält die Erpresserbotschaft dagegen üblicherweise nur eine oder mehrere E-Mail-Adressen, unter denen die Opfer zur Verhandlung des Lösegelds Kontakt mit den Angreifern aufnehmen können.

Die Schäden durch Lösegeldzahlungen und Wiederherstellungskosten steigen stetig, da ganze Netzwerke sabotiert und unter Umständen hunderttausende Menschen geschädigt werden, z. B. bei der Verschlüsselung von Patienten-

daten. Den Mitarbeiterinnen und Mitarbeitern von angegriffenen Einrichtungen drohen zudem teils drastische Folgen. Die durch *Ransomware* verursachten Schäden können existenzbedrohend sein.

Der entstandene Gesamtschaden bei den betroffenen Unternehmen und Institutionen ist zudem in der Regel weitaus größer als ein gegebenenfalls gezahltes Lösegeld, da durch einen Ausfall der IT neben den teils beträchtlichen Kosten zur Bereinigung und Wiederherstellung von Systemen unterschiedliche weitere Kosten entstehen. Umsatzausfälle führen zu direkten Verlusten. Die Kosten steigen aber auch durch die Installation alternativer Geschäftsprozesse (wenn etwa zusätzliches Personal eingestellt werden muss) oder die Beauftragung von Fremdfirmen. Bei der Wiederherstellung der IT-Infrastruktur nach einem Angriff wird oft auch die Hardware ausgetauscht, um notwendige, erneuerte Sicherheitskonzepte umsetzen zu können. Auch diese Migration bewirkt Störungen und Verzögerungen im Betriebsablauf und hat zum Beispiel Schulungsbedarf zur Folge.

Für viele Betroffene bedeutet ein *Ransomware*-Angriff zudem einen Reputationsverlust. Selbst bei großer Sorgfalt und vorhandenen *Backups* können Informationen verloren gehen (z. B. applikationsspezifische Zwischenspeicher). Güte und Häufigkeit der *Backups* entscheiden daher mit darüber, wieviel Aufwand oder Verlust diese verlorenen Daten verursachen.

Die wichtigste Maßnahme gegen die Folgen von *Ransomware*-Angriffen besteht in funktionierenden *Backups*. Die Rekonstruierbarkeit dieser *Backups* muss regelmäßig geprüft werden. Sie dürfen nicht aus dem Netzwerk heraus änderbar sein oder gelöscht werden können (*Offline-Backups*). Da Angreifer inzwischen aber häufig Daten nicht nur verschlüsseln, sondern auch ausleiten und mit Veröffentlichung drohen, um der Lösegeldforderung Nachdruck zu verleihen, ist auch ein systematisches, regelgeleitetes Monitoring des Datentransfers erforderlich. So kann etwa der Abfluss ungewöhnlich hoher Datenmengen erkannt und frühzeitig unterbunden werden.

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

Für Unternehmen und andere Institutionen sollte die umfassende und kontinuierliche Schulung aller Mitarbeiterinnen und Mitarbeiter zum Thema Informationssicherheit (Erhöhung der Aufmerksamkeit) und eine restriktive Auswahl der Personen mit (Remote-)Zugang zu den Systemen

³Netzwerk zur Anonymisierung von Verbindungsdaten

selbstverständlich sein. Bei den notwendigen Zugängen sind hohe Anforderungen an die Passwortsrichtlinien und die verwendeten Protokolle zu stellen.

Um im Falle eines Angriffs vorbereitet zu sein, müssen Reaktionsszenarien schriftlich festgehalten sein, 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.



Ransomware in Krankenhäusern

Sachverhalt

Am Samstag, den 13. Juli 2019 kam es auf zentralen Systemen der DRK-Trägersgesellschaft Süd-West zu einer Verschlüsselung durch eine *Ransomware*. Die angeschlossenen Krankenhäuser in Rheinland-Pfalz und im Saarland wurden dadurch erheblich in ihrer Versorgungsleistung beeinträchtigt.

Reaktion

Über das Nationale Cyber-Abwehrzentrum erfuhr das BSI von dem Vorfall und leitete die sogenannte Koordinierte Fallbearbeitung ein, an der verschiedene Bundes- und Landesbehörden beteiligt waren. Anhand des dem BSI von den Betroffenen übersandten Erpressertextes konnte die Schadsoftware Sodinokibi als wahrscheinlichster Verursacher festgestellt werden. Das BSI versorgte den betroffenen IT-Dienstleister der DRK-Trägersgesellschaft Süd-West als erste Sofort-Maßnahme mit einem fallspezifischen Unterstützungspaket. Dies enthielt aktuelle Warnungen und Hilfen sowie Informationen zur identifizierten Schadsoftware. Zusätzlich bestand das Angebot aus einem Einsatz des Mobile Incident Response-Teams (MIRT) zur Unterstützung vor Ort, welches am 18. Juli angenommen wurde. Am 19. Juli befand sich ein mehrköpfiges Team vor Ort. Das MIRT des BSI und der IT-Dienstleister arbeiteten gemeinsam erfolgreich daran, den Umfang des Angriffs festzustellen, das wahrscheinlichste Einfallstor zu ermitteln, den Angreifer aus dem Netz zu entfernen und auszusperrern und das IT-Netz wieder in einen arbeitsfähigen Zustand zu versetzen. Der Einsatz dauerte bis zum 26. Juli 2019.

Als Reaktion auf diesen Vorfall wurde im August 2019 auf Initiative des Ministeriums für Soziales, Arbeit, Gesundheit und Demografie des Landes Rheinland-Pfalz der Runde Tisch zur IT-Sicherheit der Krankenhäuser ins Leben gerufen, eine mit Fachexpertinnen und -experten besetzte Projektgruppe. Ihre Aufgabe war es, Empfehlungen zu formulieren und konkrete Maßnahmen auszuarbeiten, die insbesondere dazu dienen, die rheinland-pfälzischen Krankenhäuser zum Thema Informationssicherheit zu informieren und zu sensibilisieren. Teilnehmer der Projektgruppe waren neben Vertretern des Gesundheitsministeriums unter anderem Vertreter des BSI, der rheinland-pfälzische Landesbeauftragte für den Datenschutz und die Informationsfreiheit, Vertreter der Krankenhausgesellschaft Rheinland-Pfalz, Vertreter des Verbands der Krankenhausdirektoren sowie der Leiter IT-Management der DRK-Trägersgesellschaft Süd-West mbH. Im März 2020 verabschiedete der Runde Tisch einen Maßnahmenplan.

Bewertung

Der Sektor Gesundheit ist von zentraler Bedeutung für das Funktionieren des Gemeinwesens und gehört deshalb zur Kritischen Infrastruktur. Das BSI begrüßt die aus den Erfahrungen des Vorfalls entstandene Initiative des Landes Rheinland-Pfalz, die Zusammenarbeit zur Steigerung der Informationssicherheit in Kliniken zu institutionalisieren, und engagiert sich gerne auch zusammen mit anderen Bundesländern, Trägern und deren Verbänden für den Gesundheitssektor.

Empfehlung

Ein wichtiger Erfolgsfaktor für die Bewältigung von Cyber-Sicherheitsvorfällen ist ein funktionierendes und eingeübtes Notfallmanagement. In diesem Fall wesentlich war die übergreifende Krisenbehandlung im Krankenhaus, d. h. ein Zusammenwirken des Business Continuity Managements (BCM) im Bereich der Patientenversorgung, z. B. durch Umstellung der Behandlungsdokumentation mittels Stift und Papier, und des IT-Notfallmanagements. Für die IT-Vorfällebehandlung gilt: Problem eingrenzen, Ursache finden, erforderliche Maßnahmen auswählen.



Ransomware-Angriff auf eine Universität

Sachverhalt

Am 23. Dezember 2019 wurde eine Universität Opfer eines *Ransomware*-Angriffs. Unmittelbar nach der Feststellung des Angriffs erfolgte durch die Universität eine präventive Abschaltung aller Computersysteme, um die Ausbreitung der Schadsoftware im Netzwerk zu verhindern. Zur Analyse und Wiederherstellung der Systeme wurden anschließend die zuständigen Behörden und ein IT-Sicherheitsdienstleister hinzugezogen. Aufgrund der unmittelbaren Auswirkungen auf die Forschung und Lehre informierte die Universität über ihre Webseite zeitweise täglich über neue Entwicklungen, Handlungsempfehlungen und Kontaktmöglichkeiten.

Anfang Februar 2020 gab die Hochschule Details zum Angriff und aus der Bewältigung gezogene Rückschlüsse bekannt. Demnach drangen die Angreifer bereits im Oktober 2019 über E-Mails mit einem Schadprogramm in das Netzwerk der Universität ein. Bis zur Ausführung der *Ransomware* Clop im Dezember 2019 breiteten sie sich innerhalb des Netzwerks aus. Mithilfe weiterer Schadsoftware und unter Ausnutzung von Schwachstellen erlangten sie dabei einen umfassenden Zugriff, sodass durch den Angriff 1.647 Server sowie rund 7.307 Arbeitsplatz-Rechner eingeschränkt oder direkt betroffen waren. Dabei gelang es den Angreifern auch, die *Backup*-Server zu verschlüsseln.

Reaktion

Die Universität bestätigte später öffentlich, sich für die Zahlung des Lösegelds entschieden zu haben. Maßgebliche Faktoren bei der Entscheidung waren die ethischen Gesichtspunkte einer Zahlung als öffentliche Institution und die möglichen Auswirkungen auf die Wiederaufnahme der universitären Aufgaben und Pflichten. Weil auch kritische Systeme und ihre *Backups* durch die Angreifer verschlüsselt worden waren und davon auszugehen war, dass zum Beispiel Forschungsergebnisse unwiederbringlich verloren gehen würden, wurde ein Lösegeld gezahlt in Höhe von 30 *Bitcoin*, was zum damaligen Zeitpunkt ca. 200.000 Euro entsprach.

Die forensische Analyse erbrachte keine Hinweise darauf, dass während des Angriffs Forschungsergebnisse oder anderweitige Datenbestände aus den Netzen der Universität abgeflossen sind. Diese Möglichkeit wird von Seiten der Universität und des IT-Dienstleisters jedoch nicht gänzlich ausgeschlossen und weiter untersucht.

Empfehlung

Regelmäßige *Backups* sind die wichtigste Vorsorgemaßnahme, um nach einem *Ransomware*-Angriff schnell wieder handlungsfähig zu werden. Damit *Backups* im Fall eines Angriffs nicht mitverschlüsselt werden, müssen sie getrennt von den übrigen Systemen offline gesichert werden. Zudem sollte regelmäßig geprüft werden, ob sie sich im Notfall schnell wiederherstellen lassen.

Das BSI empfiehlt grundsätzlich, kein Lösegeld zu zahlen, um das „Geschäftsmodell“ *Ransomware* nicht zu unterstützen und nicht noch weitere Angriffe auf andere Ziele zu motivieren.

1.1.4 Spam und Malware-Spam

Allgemein werden unerwünscht zugesandte E-Mails als *Spam* bezeichnet. Neben Werbe-E-Mails kann es sich dabei auch um Cyber-Angriffe handeln, wie *Malware-Spam* oder *Phishing*-E-Mails. Der Spamversand erfolgt zum Beispiel über kompromittierte oder kommerziell angemietete Serverkapazitäten, über von Angreifern gestohlene legitime E-Mail-Accounts, deren Zugangsdaten zuvor ausgespäht wurden, oder über infizierte Systeme, die zu *Botnetzen* zusammengeschlossen sind und sodann für *Spam*-Dienstleistungen zur Verfügung gestellt werden (vgl. Kapitel *Botnetze*, Seite 16).

Der Versand unerwünschter Werbe-E-Mails ist auch im aktuellen Berichtszeitraum weiter zurückgegangen (vgl. *Quellenverzeichnis*²: www.bsi.bund.de). Ursache für den rückläufigen Trend dürfte insbesondere die weiter steigende Qualität vieler *Spam*-Filter sein. Ihre hohe Trefferquote macht Werbe-*Spams* als Geschäftsmodell zunehmend unattraktiv, da viele Werbe-E-Mails die Empfänger nicht mehr erreichen. Zudem existiert mittlerweile mit dem sogenannten Targeting eine effizientere Form des Online-Marketings. Beim Targeting wird das Nutzerver-

halten zum Beispiel auf Webseiten, in Online-Shops oder auf Social-Media-Plattformen analysiert, um anschließend zielgerichtet an die jeweiligen Nutzerbedarfe angepasste Werbung einblenden zu können.

Bei *Malware-Spam* handelt es sich um *Spam*-E-Mails, die Schadprogramme ungezielt und breit verteilen. Während der *Spam*-Versand zurückgegangen ist, ist die Effektivität von *Malware-Spam* im Berichtszeitraum weiter gestiegen. So wurde insbesondere die *Spam*-Komponente von Emotet im Berichtszeitraum weiterhin erfolgreich für die Verteilung des Schadprogramms genutzt. Das Schadenspotenzial basiert dabei insbesondere auf ausgefeilten *Social-Engineering*-Techniken, durch die die Nutzerin oder der Nutzer zum Ausführen des Schadprogramms verleitet wird. Das Infektionsrisiko ist daher als hoch einzuschätzen (vgl. Kapitel *Emotet: Neue Qualität fortschrittlicher Angriffe*, Seite 11).

1.1.5 Botnetze

Als *Bot* wird ein Schadprogramm bezeichnet, das einem Angreifer den Fernzugriff auf ein infiziertes System ermöglicht. Jedes Schadprogramm, das eine Verbindung zu einem Command-and-Control-Server des Angreifers aufbauen kann, um von dort Befehle entgegen zu nehmen und auf dem infizierten System auszuführen, ist insofern ein *Bot*. Durch die großflächige Verbreitung von *Bot*-Software haben Angreifer Zugriff auf eine große Anzahl fremder Systeme (Computer, Smartphones, Router, *IoT*-Geräte etc.) und können diese für eigene Zwecke missbrauchen. Den Zusammenschluss mehrerer *Bots*, die von einer zentralen Stelle gesteuert werden, bezeichnet man als *Botnetz*.

Aufgrund des modularen Aufbaus aktueller *Bot*-Software ist es dem Angreifer möglich, die Funktionalität eines *Bots* flexibel auf die jeweiligen Einsatzzwecke und Angriffsziele anzupassen. Neben der Verursachung von Schäden auf dem infizierten System selbst (Abgreifen persönlicher Informationen, Online-Banking-Betrug, Datenverschlüsselung etc.), können die infizierten Systeme auch zum Angriff Dritter genutzt werden. So können Angreifer die enormen Rechen- und Netzwerkkapazitäten der zusammengeschlossenen infizierten Systeme zum Beispiel für bandbreitenstarke *DDoS-Angriffe* (vgl. Kapitel *Distributed Denial of Service*, Seite 29) oder für den Versand von *Spam*-E-Mails verwenden.

Im aktuellen Berichtszeitraum wurden *Botnetze* in erster Linie zum Informationsdiebstahl sowie zum Nachladen und Verteilen weiterer Schadprogramme (Banking-Trojaner oder *Ransomware*) genutzt. Im Vergleich zum vergangenen Berichtszeitraum ging die Anzahl bekannter *DDoS-Botnetze* signifikant zurück. Zwar erschienen auch

weiterhin beispielsweise neue Varianten des *Botnetzes* Mirai mit zusätzlichen Infektionsmechanismen, um das Spektrum der Opfersysteme auf zusätzliche Geräteklassen wie *IoT*-Geräte und weniger stark verbreitete Hardware-Plattformen (z. B. ARM, ARC, oder PowerPC) zu erweitern. Diese traten jedoch nicht mit hohen Infektionszahlen oder erfolgreichen *DDoS-Angriffen* in Erscheinung.

Der Trend zur stärkeren Ausrichtung der Angreifer auf mobile Endgeräte wie beispielsweise Smartphones und Tablets war auch im aktuellen Berichtszeitraum wieder zu beobachten. Im Bereich der Windows-basierten *Botnetze* haben insbesondere Emotet und Trickbot größere Infektionswellen in Deutschland verursacht. Beide Schadprogramm-Familien sind bereits seit mehreren Jahren in Deutschland aktiv und haben neben Privatanwenderinnen und -anwendern auch mehrere größere Institutionen und Unternehmen infiziert. Durch die *Ransomware* Ryuk, die ausgewählte, von Trickbot zuvor ausgespähte Opfer angreift, wurden große finanzielle Schäden verursacht (vgl. Kapitel *Emotet: Neue Qualität fortschrittlicher Angriffe*, Seite 11).

Im Berichtszeitraum wurden täglich bis zu 20.000 *Bot*-Infektionen deutscher Systeme registriert und über das BSI an die deutschen Internet-*Provider* gemeldet. Diese benachrichtigen ihrerseits die betroffenen Kundinnen und Kunden über die Infektion und stellen teilweise weiterführende Informationen zur Bereinigung der Systeme bereit. Zur Erkennung von *Botnetz*-Infektionen werden sogenannte *Sinkhole*-Systeme verwendet, die anstelle der regulären Command-and-Control-Server der Angreifer die Kontaktanfragen von *Bots* entgegennehmen. Eine Beschreibung des Sinkholing-Verfahrens findet sich unter www.bsi-fuer-buerger.de (vgl. *Quellenverzeichnis*³: www.bsi-fuer-buerger.de).

Die Bedrohungslage durch *Botnetze* ist wie auch in den Vorjahren anhaltend hoch. Die aus dem Sinkholing ermittelten Infektionszahlen bilden stets eine Untergrenze, da eine vollständige Erfassung aller *Botnetz*-Infektionen nicht möglich ist. Abhängig von der Auswahl der beobachteten *Botnetze* und der zugehörigen Domänen der Steuerungsserver schwanken die Zahlen der sichtbaren Infektionen sehr stark. Die bisherigen Erfahrungen aus *Botnetz*-Abschaltungen zeigen aber, dass die Dunkelziffer deutlich höher liegt und sich mindestens in einem siebenstelligen Bereich bewegt.

Aufgrund der stetig breiter werdenden Angriffsfläche potenzieller Opfersysteme durch unzureichend gesicherte *IoT*-Geräte und mobile Systeme ist mit einer kontinuierlichen Zunahme von Infektionen zu rechnen und davon auszugehen, dass die Anzahl und Größe von *Botnetzen* weiterhin zunehmen werden.

i Avalanche: Verlängerung der Schutzmaßnahmen

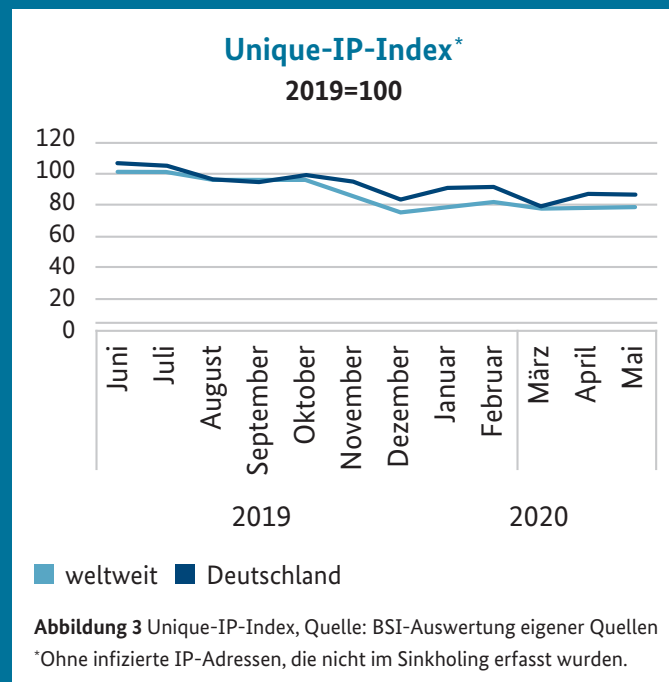
Sachverhalt

Am 30. November 2016 haben die Zentrale Kriminalinspektion Lüneburg und die Staatsanwaltschaft Verden in einer internationalen Operation erfolgreich die *Botnetz*-Infrastruktur *Avalanche* ausgehoben. Dabei unterstützte das BSI maßgeblich. Die Server der *Botnetz*-Infrastruktur wurden abgeschaltet, die Angreifer wurden verhaftet und die Nutzerinnen und Nutzer infizierter Systeme über die *Internet-Provider* informiert. Zur fortlaufenden Erkennung infizierter Systeme wurden *Sinkhole*-Server eingerichtet, die die Kontaktversuche der weiterhin aktiven *Bots* verzeichnen und deren IP-Adressen identifizieren. Mithilfe der IP-Adressen sowie des Zugriffszeitpunkts können *Internet-Provider* die betroffenen Anwenderinnen und Anwender informieren und warnen.

Reaktion

Die ursprünglich auf ein Jahr ausgelegten Schutz- und Informationsmaßnahmen wurden in den Folgejahren kontinuierlich verlängert, um infizierte Systeme weiterhin zu schützen. Im November 2019 wurde eine erneute Verlängerung um zwölf Monate umgesetzt. Hierbei wurden ca. 830.000 Domänen überprüft und vor fremden Zugriff gesichert, um eine Übernahme der *Botnetze* durch Kriminelle zu unterbinden. Hierzu ist die kooperative Mitwirkung der Domaininhaber erforderlich. Die Weitergabe der Infektionsdaten durch das BSI an *Internet-Provider* und andere, auch internationale Partner ermöglicht eine rasche Bereinigung der betroffenen Systeme.

Aufkommen und Entwicklung der Infektionszahlen werden anhand des Unique-IP-Index gemessen. Gezählt werden die eindeutigen IP-Adressen pro Tag in Deutschland und in der Welt. Auch im aktuellen Berichtszeitraum war der Trend weiter rückläufig, sodass der Index sich überwiegend unter dem Durchschnittswert von 2019 bewegte.



Empfehlung

Die Infektionszahlen verdeutlichen, dass selbst nach dreieinhalb Jahren viele betroffene Anwenderinnen und Anwender ihre infizierten Systeme noch nicht bereinigt haben. Das BSI empfiehlt, dies dringend nachzuholen.

1.2 Diebstahl und Missbrauch von Identitätsdaten

Unter einer Identität wird im Kontext der Informationssicherheit die Menge von Merkmalen verstanden, die die Echtheit einer Person oder Sache nachweist. Die Identität einer Person oder Sache kann sowohl durch ein einzelnes Merkmal oder aber durch die Kombination diverser Merkmale bestimmt werden. Im Internet wird auf die Identität einer Person meist aus Identifikations- und Authentisierungsdaten geschlossen wie zum Beispiel aus der Kombination von Benutzername und Passwort. Als Identitätsdiebstahl wird folglich die rechtswidrige Aneignung solcher Daten bezeichnet. Wird zudem die Identität nach dem Diebstahl unautorisiert für eigene oder fremde Zwecke verwendet, wird dies auch als Identitätsmissbrauch bezeichnet.

Meldungen zum Abfluss von Identitätsdaten wurden, wie auch im vergangenen Berichtszeitraum, regelmäßig beobachtet. Unabhängig von den Vorteilen, die große Digitalisierungsprojekte erwarten lassen, werden sie daher nur dann gelingen und eine entsprechende Akzeptanz erfahren, wenn sie von Anfang an sicher gestaltet und auch langfristig mit den hierfür notwendigen Ressourcen hinterlegt werden. Hierbei ist seitens der Anbieter von Internetdiensten insbesondere auch die Integration von Verfahren zur sicheren Identifizierung für den erstmaligen Kundenkontakt vorzusehen. Erst durch eine dem Schutzbedarf angemessene Identifizierung eines Nutzers kann ein Dienst sicherstellen, dass sensible Daten nur durch berechtigte Personen und nicht durch Dritte verwendbar sind.

Die aktuellen Fälle von Identitätsdiebstahl zeigen jedoch auch, dass die digitale Eigenverantwortung jedes Einzelnen einen wesentlichen Bestandteil der nachhaltigen Informations- und IT-Sicherheit darstellt. Die Fülle kompromittierter Nutzerinformationen und deren Missbrauchsmöglichkeiten macht private Informationen zu einem weithin verfügbaren und wertvollen Handelsgut, wodurch Sicherheit und Vertrauen in die gesamte digitale Infrastruktur gefährdet sind. Denn diese Daten steigern in den Händen von Angreifern die Aussichten enorm, dass Manipulations- und Erpressungsbestrebungen sowie automatisierte Authentisierungsversuche (sogenanntes Credential Stuffing) bis hin zum Direktzugriff auf fremde Konten von Erfolg gekennzeichnet sind.

Das BSI empfiehlt deswegen, Sorgfalt im Umgang mit den eigenen, persönlichen Informationen walten zu lassen und die Verwendung einer *Zwei-Faktor-Authentisierung* in Anspruch zu nehmen, sobald ein Online-Dienst dies ermöglicht. So wurde etwa mit dem Standard FIDO2 (Fast Identity Online 2) ein Protokoll für die *Authentifizierung*

definiert, das die Verwendung von Schlüsselspeichern in Mobilgeräten oder externen Hardware-Token als Authentifizierungsfaktor erlaubt, und das bereits in den meisten Browsern implementiert worden ist. Das Protokoll basiert auf *Public-Key-Kryptografie*, bei der Nutzerinnen und Nutzer ihre privaten Schlüssel nie mit dem Dienst teilen müssen, sondern dessen Besitz mit einer digitalen Signatur über einen Zufallswert nachweist. Der Standard wird bereits durch viele Diensteanbieter wie zum Beispiel Google, Facebook und Microsoft unterstützt. Durch die Verwendung von Authentifizierungsfaktoren aus getrennten Kategorien (Wissen, Besitz oder biometrische Merkmale) wird die Möglichkeit eines Identitätsdiebstahls bzw. -missbrauchs deutlich erschwert.

Eine prominente Form des Identitätsdiebstahls ist das sogenannte *Phishing*. Mit Hilfe hoch entwickelter Techniken des *Social Engineering* versucht ein Angreifer, das Opfer zur Herausgabe sensibler Informationen zu bewegen (vgl. Kapitel *Phishing und weitere Betrugsformen*, Seite 18). Eine weitere Möglichkeit, Identitätsdaten zu entwenden, besteht im Einsatz spezieller Schadprogramme (vgl. Kapitel *Schadprogramme für den Diebstahl von Identitätsdaten*, Seite 20). Aber auch ohne direkte Beteiligung des Opfers können Identitätsdaten entwendet werden, zum Beispiel direkt bei einem Diensteanbieter (vgl. Kapitel *Daten-Leaks*, Seite 20).

1.2.1 Phishing und weitere Betrugsformen

Beim Thema *Phishing* stehen in Deutschland neben Bankkundinnen und -kunden insbesondere auch Kundinnen und Kunden von Online-Versandhändlern wie Amazon oder Bezahlssystemen wie PayPal im Fokus der Angreifer. Nach wie vor orientieren sich aktuelle *Phishing*-Kampagnen an gesellschaftlichen Ereignissen und aktuellen Themen wie etwa Steuerrückzahlungen oder Rabatt-Aktionen zum Black Friday. Während sich Angreifer im vergangenen Berichtszeitraum die Unsicherheit rund um das Thema Datenschutzgrundverordnung (DSGVO) zunutze machten, stand im aktuellen Berichtszeitraum größtenteils die Umsetzung der zweiten Zahlungsdiensterichtlinie (Payment Service Directive 2, PSD2) im Vordergrund. Aber auch die Auswirkungen der COVID-19-Pandemie spiegelten sich in der digitalen Welt wider. Die Unsicherheit im Umfeld der Maßnahmen gegen die COVID-19-Pandemie, der reale und empfundene Zeitdruck und die gesellschaftliche und mediale Dominanz des Themas wurden von Angreifern ausgenutzt. Vor diesem Hintergrund wurden dem BSI deutschsprachige *Phishing*-E-Mails gemeldet, die sich dadurch auszeichnen, dass sie in gutem Deutsch formuliert sind, gezielt mit Emotionen spielen und das bestimmende Thema COVID-19 adressieren: Die vorübergehende Schließung

von Bankfilialen, verbunden mit der Übermittlung von Erreichbarkeiten sowie die Beantragung von Soforthilfe und Kurzarbeitergeld sind nur einige Beispiele.

Unter der Ausnutzung menschlicher Eigenschaften, wie Hilfsbereitschaft, Vertrauen, Angst, Dringlichkeitsempfinden oder Respekt vor Autorität, wurden Opfer immer wieder auf *Phishing*-Seiten geleitet, die von den Originalseiten kaum zu unterscheiden waren.

Der Einsatz von HTTPS-Links in *Phishing*-Nachrichten entwickelt sich hierbei immer mehr zum Standard. Hypertext Transfer Protocol Secure (HTTPS) steht für eine verschlüsselte sowie gegen Manipulation geschützte Datenübertragung und verstärkt insofern den Eindruck von Vertrauenswürdigkeit und Seriosität von *Phishing*-Seiten.

Gemeinsame Analysen der Verbraucherzentrale NRW sowie des BSI auf Basis der Meldungen an das *Phishing-Radar* (vgl. *Quellenverzeichnis*⁴: www.verbraucherzentrale.de) haben ergeben, dass im aktuellen Berichtszeitraum in Deutschland mittlerweile mehr als jeder zweite Link einer *Phishing*-Nachricht HTTPS verwendet (60 %). Im vergangenen Berichtszeitraum hatte der Wert noch bei 45 Prozent gelegen. Diese Entwicklung dürfte insbesondere darauf zurückzuführen sein, dass gängige Internet-Browser inzwischen einfache HTTP-Seiten negativ kennzeichnen und so das Misstrauen der Opfer erregen. Die für eine verschlüsselte Verbindung notwendigen Zertifikate können kostenfrei im Internet bezogen werden und gewährleisten in der Regel nicht, dass die Besitzer des Zertifikats vertrauenswürdig sind.

Links in Phishing-E-Mails nach verwendetem Protokoll

Anteile in % an allen Links

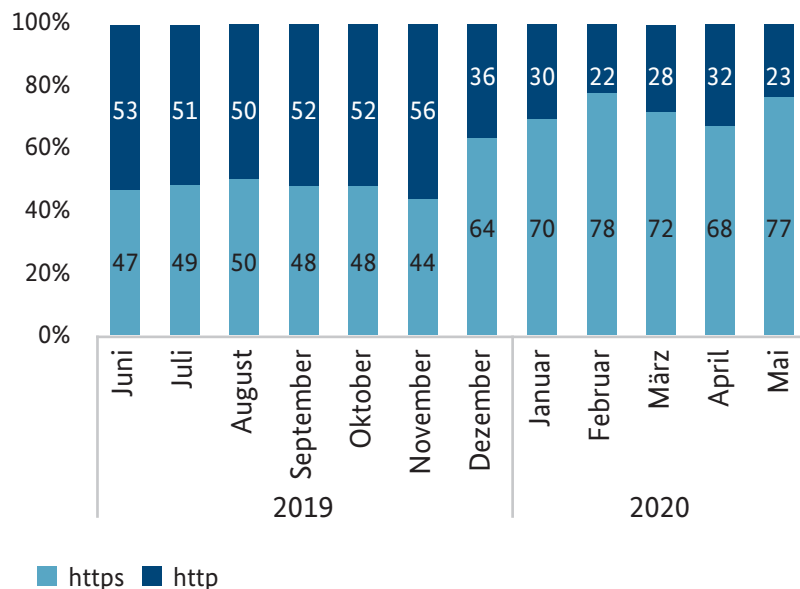


Abbildung 4 Links in Phishing-E-Mails nach verwendetem Protokoll
Quelle: BSI-Auswertung von Rohdaten der Verbraucherzentrale NRW

Neben klassischen *Phishing*-E-Mails wurden auch im aktuellen Berichtszeitraum wieder Erpressungsversuche beobachtet. Hierbei schickten Angreifer in den fingierten E-Mails beispielsweise (korrekte oder vermeintliche) Passwörter der Opfer mit oder gaben vor, das Opfer bei dem Besuch von Internetseiten mit pornografischen Inhalten beobachtet und aufgezeichnet zu haben (Sextortion). Die Angreifer zeigten hierbei eine hohe Kreativität in der Verfassung solcher Erpressungsversuche. Ob durch Androhung der Offenlegung aller Geheimnisse des Opfers, die Androhung von Gewalt oder die Androhung einer Infektion der gesamten Familie mit COVID-19: Ziel ist in der Regel, dem Opfer einen finanziellen Schaden zuzufügen. Neben dem Ausnutzen

von Ängsten wurde aber auch an die Hilfsbereitschaft der Menschen appelliert, indem die Angreifer beispielsweise vorgaben, dass ein vermeintlicher Freund im Urlaub in Not geraten sei und nun dringend finanzielle Unterstützung benötige. Auch wurde um zweifelhafte Spenden für die Entwicklung eines Impfstoffes gegen COVID-19 gebeten – zu bezahlen in der Kryptowährung *Bitcoin*.

Zusammenfassend zeigte sich im aktuellen Berichtszeitraum erneut die flexible Orientierung der Angreifer an gesellschaftlichen Ereignissen und aktuellen Themen. Die COVID-19-Pandemie und die mit ihr einhergehende gesellschaftliche Unsicherheit wurde dafür besonders genutzt.

1.2.2 Schadprogramme für den Diebstahl von Identitätsdaten

Neben *Phishing* kommen ebenfalls Schadprogramme für den Diebstahl und den Missbrauch von Identitätsdaten zum Einsatz. Das Schadprogramm Emotet unterstreicht hierbei eindrucksvoll, welchen enormen Mehrwert gesammelte Identitätsdaten als Grundlage für nachfolgende Angriffe haben. Emotet liest die Kontaktbeziehungen und E-Mail-Inhalte aus den Postfächern infizierter Systeme aus. Diese Informationen verwenden die Angreifer im Anschluss daran zur weiteren Verbreitung des Schadprogramms. Der große Erfolg von Emotet beruht darauf, dass die E-Mails besonders authentisch wirken und so die Opfer erfolgreich zum Öffnen verleiten (vgl. Kapitel *Emotet: Neue Qualität fortschrittlicher Angriffe*, Seite 11).

Auch bei Erpressungsversuchen spielt der Diebstahl privater Informationen im Einzelfall eine große Rolle. Dem BSI wurden einige Fälle bekannt, bei denen – neben der Forderung nach Lösegeld für die Entschlüsselung von Daten – zusätzlich damit gedroht wurde, die abgeflossenen privaten Informationen im Internet zu publizieren. Beispiele für dieses Vorgehen sind die Angreifergruppierungen hinter den *Ransomwares* Sodinokibi und Maze (vgl. Kapitel *Ransomware*, Seite 11).

Aber nicht nur der Einsatz komplexer Schadprogramme stellt eine Gefahr dar. Auch scheinbar einfache Programme wie Browser-Erweiterungen können für Nutzerinnen und Nutzer risikobehaftet sein und den Verlust persönlicher Daten bewirken. Browser-Erweiterungen sind optionale Programme, die den bestehenden, standardmäßigen Funktionsumfang der Browser um zusätzliche Funktionalitäten ergänzen können. Im Berichtszeitraum wurde eine Vielzahl dieser Erweiterungen von Browser-Herstellern gesperrt, weil sie schädliche Eigenschaften aufwiesen. So entfernte beispielsweise der Entwickler des Browsers Firefox, Mozilla, Ende 2019 unter anderem die Browser-Erweiterung eines bekannten Herstellers für IT-Sicherheitssoftware. Diese hatte umfangreiche Daten über das Surf-Verhalten seiner Nutzerinnen und Nutzer erfasst und anschließend für Marketingzwecke verwendet.

Insgesamt zeigte sich im Berichtszeitraum erneut, dass die stetig wachsende Anzahl frei verfügbarer Identitätsdaten eine bedrohliche Basis für weitere Angriffe darstellt. Auch scheinbar unbedeutende Programme wie beispielsweise Browser-Erweiterungen können großen Schaden anrichten.

1.2.3 Daten-Leaks

Meldungen zum Diebstahl von Kundendaten wurden auch im aktuellen Berichtszeitraum wieder häufig beobachtet.

Unter den von einem Daten-Leak betroffenen Unternehmen befanden sich unter anderem namhafte Banken und Zahlungsdienstleister, Technologieunternehmen, Arztpraxen und Krankenhäuser, Hochschulen sowie ein Unternehmen im Elektronik-Versandhandel und ein weiteres in der Autovermietung (vgl. Vorfall *Daten-Leak bei einer deutschen Autovermietung*, Seite 21). Im Berichtszeitraum stachen neben dem Vorfall bei der Autovermietung besonders die Veröffentlichung großer Mengen privater Krankendaten heraus. Solch hochsensible personenbezogene Daten, insbesondere aus dem medizinischen Sektor, haben einen besonders hohen Schutzbedarf.

Die Vielfalt und Häufigkeit von Vorfällen, bei denen immer wieder sensible Daten unfreiwillig veröffentlicht werden, sind besorgniserregend. Auch größere Unternehmen bleiben hiervon nicht verschont. Sicherheitsforscher entdeckten Ende 2019 mehrere ungesicherte Datenbanken eines Technologieunternehmens mit Kunden- und Supportinformationen, die aufgrund von Fehlkonfigurationen öffentlich im Internet verfügbar waren (vgl. *Quellenverzeichnis*⁵: www.heise.de). Solche Daten bieten eine hervorragende Grundlage für vorgetäuschte Support-Anfragen. Bei dieser Form des *Social Engineering* geben sich Angreifer beispielsweise als Mitarbeiter des Unternehmens aus und versuchen, per Anruf oder über im Computer eingeblendete, gefälschte Warnhinweise unter falschem Vorwand, Sicherheitsfunktionen auszuhebeln oder Zugriff auf das System des Opfers zu erlangen. Insbesondere vor dem Hintergrund der COVID-19-Pandemie stellen solche Angriffe eine erneut wachsende Bedrohung dar: Derartige Angriffsmöglichkeiten treffen in dieser Sondersituation unter Umständen vermehrt auf unvorbereitete oder unaufmerksame Personen, die sich gezwungen sehen, schnell zu handeln, ohne die gebotene Sorgfalt walten zu lassen (vgl. Kapitel *Gefährdungen der Cyber-Sicherheit durch die COVID-19-Pandemie*, Seite 33; vgl. Vorfall *COVID-19 Soforthilfe-Maßnahmen durch Cyber-Kriminelle missbraucht*, Seite 34).

Um im Internet offen erreichbare, exponierte Datenbanken und Systeme zu identifizieren, sind frei erhältliche Tools und Dienste verfügbar. Angreifer können sie beispielsweise nutzen, um unbefugten Zugriff auf solche Datenbanken und Systeme zu erhalten.

Die regelmäßigen Meldungen zu Datenabflüssen lassen Diensteanbietern eine große Verantwortung zuteilwerden. Besonders im Gesundheitssektor kann das Öffentlichwerden sensibler Daten auch gleichzeitig negative Auswirkungen auf die jeweils individuelle Gesundheit der Patientinnen und Patienten haben - mit möglicherweise lebenslangen Folgen. Die aktuellen Fälle von Identitätsdiebstahl zeigen jedoch auch, dass die digitale Eigenverantwortung jedes Einzelnen einen wesentlichen Bestandteil der nachhaltigen IT-Sicherheit darstellt.



Daten-Leak bei einer deutschen Autovermietung

Sachverhalt

Auf Hinweis der Deutschen Gesellschaft für Cybersicherheit sowie durch eine gemeinsame Recherche der Journalisten von c't und ZEIT wurde der breiten Öffentlichkeit im Januar 2020 erstmalig bekannt, dass sensible Daten von drei Millionen Kundinnen und Kunden einer deutschen Autovermietung frei im Internet abrufbar gewesen waren.

Demnach hatte es einen Konfigurationsfehler bei einem *Backup*-Server des Anbieters gegeben, sodass kein Passwort für den Zugriff über das Netzwerkprotokoll Server Message Block (SMB) erforderlich war. Über den offenstehenden SMB-Port 445 war jeder Internetnutzer in der Lage, den Datenbestand von insgesamt 10 Terabyte herunterzuladen.

Der Datenbestand umfasste laut den Analysen der Journalisten über neun Millionen Mietverträge, die zum Teil bis in das Jahr 2003 zurückreichten. Neben den Mietern seien auch die Fahrer mit Namen, Adresse, Geburtsdatum, Führerscheinnummer und Ausstellungsdatum aufgeführt gewesen. Viele Mieter hätten zudem Mobilfunknummern und E-Mail-Adressen angegeben. Darüber hinaus seien detaillierte Informationen über bei der Anmietung entstandene Schäden und Unfälle enthalten und mehr als 3.000 Passwörter von Angestellten und Kunden im Klartext ersichtlich gewesen. Kreditkartennummern hätten sich nicht in der Datenbank befunden, wohl aber Zahlungsinformationen und Bankverbindungen auf eingescannten Rechnungen.

Da der Autovermieter seine Fahrzeuge auch über Vermittler anbietet, könnten auch Personen betroffen gewesen sein, die gar kein Auto unmittelbar bei dem Anbieter gemietet hatten. Die enthaltenen Angaben zu Unfällen könnten zudem dazu geführt haben, dass auch Daten von Personen erfasst wurden, die in keinem Kundenverhältnis zum Unternehmen standen.

Die veröffentlichten Daten waren als äußerst sensibel einzuschätzen. Aufgrund der hohen Validität der abrufbaren Daten verfügten diese über ein hohes Potenzial, für kriminelle Zwecke Verwendung zu finden: Vom *Phishing* bis hin zur Erpressung oder Bedrohung wären zahlreiche Handlungen krimineller Akteure denkbar. Potenzielle kriminelle Handlungen könnten auch mit einem erheblichen zeitlichen Versatz eintreten, wenn der Vorfall bereits in Vergessenheit geraten ist.

Reaktion

Der ungeschützte Zugriff auf den Server war bis zur Schließung des Ports am 20. Januar 2020 möglich. Der Autovermieter hat das zuständige Landesamt für Datenschutz hierüber unterrichtet. Am 25. Januar 2020 veröffentlichte das Unternehmen eine Stellungnahme mit Angaben nach Art. 34 DS-GVO und bestätigte den Vorfall.

Empfehlung

Der Vorfall macht deutlich, welche schwerwiegenden Konsequenzen ein einzelner Konfigurationsfehler haben kann. Im Sinne der BSI-Standards zur Internet-Sicherheit (ISi-Reihe) sollte bei Servern möglichst nach einem Minimalsystem gearbeitet werden: Es sollten nur die Dienste, Programme und Funktionen bereitgestellt werden, die auch tatsächlich benötigt werden. Nach der Konfiguration des Servers sollte zudem eine Analyse der laufenden Prozesse, der im Netz erreichbaren Schnittstellen und anderer auf dem Server installierter Programme erfolgen, um etwaige Fehlkonfigurationen auszuschließen. Abhängig vom Einsatzzweck eines Servers sollte die Konfiguration zusätzlich von einer Management-Komponente auf etwaige Änderungen geprüft werden.



Patientendaten und medizinische Bilddaten öffentlich verfügbar

Sachverhalt

Im September 2019 wurde das BSI von IT-Sicherheitsforschern informiert, dass ungesicherte Datenbanken mit hochsensiblen medizinischen Daten im Internet entdeckt worden waren. Bei den Informationen handelte es sich um personenbezogene Daten wie Vor- und Nachname, Geburtsdatum, Untersuchungstermin, Informationen über den behandelnden Arzt oder die Behandlung selbst sowie hochauflösende Röntgenaufnahmen u. ä.. Die Informationen lagen auf sogenannten PACS-Servern (Picture Archiving and Communication Systems), die im Gesundheitssektor genutzt werden, um Bilder, die durch radiologische Verfahren entstanden sind, zu archivieren und behandelnden Ärzten zur Betrachtung bereit zu stellen.

Alleine in Deutschland waren im Zeitraum von Juli 2019 bis September 2019 etwa 15.000 Datensätze öffentlich zugänglich, wobei diesen Datensätzen mehrere Millionen Bilder zugeordnet waren (vgl. *Quellenverzeichnis*⁶: www.greenbone.net). Davon war ein Großteil ohne Passwort oder *Authentifizierung* abrufbar. Auch international war eine Vielzahl von Staaten betroffen. Insgesamt waren Schätzungen zufolge 24,3 Millionen Patientendatensätze und mehrere hundert Millionen verknüpfte Bilddateien frei im Internet zugänglich.

Reaktion

Die medizinischen Einrichtungen wurden durch das BSI in Kenntnis gesetzt. In drei Fällen konnten die Einrichtungen direkt kontaktiert werden, in 14 weiteren Fällen wurden die jeweiligen *Internet-Provider* gebeten, ihre Kundinnen und Kunden anhand der IP-Adressen zu identifizieren und zu informieren. Zudem hat das BSI 46 internationale Partnerorganisationen über den Sachverhalt in Kenntnis gesetzt.

Viele Staaten haben ebenfalls auf die Situation reagiert und zeitnah entsprechende Maßnahmen eingeleitet, um die Daten zu schützen. So haben elf Länder alle beim ursprünglichen Scan gefundenen PACS-Systeme vom öffentlichen Netz genommen (unter anderem Deutschland). Es sind auch neue Staaten hinzugekommen, bei denen offen zugängliche PACS-Systeme entdeckt wurden.

Empfehlung

Das BSI empfiehlt, Patientendaten nur dann cloudbasierten oder anderen über das Internet erreichbaren Services zur Verfügung zu stellen, wenn sicher ist, dass alle verfügbaren Schutzmechanismen, zum Beispiel verschlüsselte Übertragung der Daten und verschlüsselte Speicherung, für eine adäquate Sicherung und sichere *Authentisierung* der Vertraulichkeit der Patientendaten angemessen sind. Die IT-Sicherheit von PACS-Systemen, die zur Gruppe der Medizinprodukte gehören, wurde noch nicht durch das BSI bewertet. Alle zuvor genannten Anforderungen zum Schutz sensibler Patientendaten gelten, aus Sicht des BSI, auch für PACS-Systeme.

1.3 Schwachstellen

1.3.1 Schwachstellen in Software-Produkten

Software-Produkte unterstützen heutzutage zahlreiche Prozesse und Lebensbereiche. Sie können zum Beispiel helfen, komplexe Probleme zu lösen oder Vorgänge zu vereinfachen. Um diesen mit der Zeit gewachsenen Herausforderungen zu begegnen, sind die Software-Produkte selbst immer komplexer geworden. Sie bestehen mittlerweile oftmals aus mehreren Millionen Zeilen Programmcode. Dies macht eine Prüfung aller Eventualitäten, mit denen ein Software-Produkt konfrontiert werden könnte, momentan faktisch

unmöglich (wohlwissend, dass es zahlreiche Ansätze gibt, die Soft-Qualität automatisiert zu erhöhen). Software-Produkte weisen insofern unerkannte Fehler oder ungewünschte Fehlfunktionen auf, die dazu führen können, dass sie nicht mehr richtig funktionieren. Wenn diese Fehler oder Fehlfunktionen von unbefugten Dritten ausgenutzt werden können, um schädliche Operationen auf einem Computersystem auszuführen, wird von Schwachstellen oder Sicherheitslücken in Software-Produkten gesprochen.

Bei der Ausnutzung einer Schwachstelle veranlasst ein Angreifer ein Software-Produkt dazu, vom Entwickler nicht vorgesehene Aktionen durchzuführen. So können zum Beispiel sensible Informationen offengelegt werden (vgl. Kapitel *Diebstahl und Missbrauch von Identitätsdaten*, Seite 18), eingeschleuste Schadprogramme zur Ausführung veranlasst werden (vgl. Kapitel *Schadprogramme*, Seite 9), oder Software zum Absturz gebracht werden. Schwachstellen in Software-Produkten sind unerwünscht und häufig auch bedrohlich. Sobald sie bekannt werden, sollten sie daher zeitnah beseitigt werden.

Schwachstellen unterscheiden sich in ihrer Kritikalität, ihrem individuellen Bedrohungspotenzial und darin, ob bereits Gegenmaßnahmen, zum Beispiel in Form von Updates, zur Verfügung stehen. Die Kritikalität einer Schwachstelle ergibt sich vereinfacht aus drei Aspekten: der Relevanz des betroffenen Software-Produkts für Anwenderinnen und Anwender, dem Aufwand oder den Voraussetzungen zur erfolgreichen Ausnutzung der Schwachstelle sowie den möglichen Auswirkungen auf die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit. Zusammengefasst ergeben diese Aspekte das individuelle Risiko einer Schwachstelle für Anwenderinnen und Anwender. Im Allgemeinen kann davon ausgegangen werden, dass das korrekte Funktionieren einer Software ebenso wichtig ist wie der Zweck, den sie erfüllen soll. Eine derartige Risikobewertung kann beispielsweise unter Anwendung des BSI IT-Grundschatzes erstellt werden.

Spätestens wenn eine Schwachstelle öffentlich wird, muss davon ausgegangen werden, dass Angreifer aktiv nach Wegen suchen, diese Schwachstelle für Angriffe auszunutzen. Es ist daher im besonderen Interesse von Nutzerinnen und Nutzern eines Software-Produkts, dass der Hersteller die Schwachstelle durch ein Sicherheitsupdate schnellstmöglich schließt.

Um Schwachstellen zu finden und schließen zu können, noch bevor sie ausgenutzt werden, setzen einige Unternehmen mittlerweile auf sogenannte Bug-Bounty-Programme. Hierbei werden Entwickler und IT-Sicherheitsforscher gegen eine Belohnung dazu aufgerufen, aktiv nach Schwachstellen zu suchen. Das Suchen nach Schwachstellen ohne Erlaubnis des Herstellers ist in der Regel rechtlich untersagt, da die bei der Suche angewendeten Methoden zum Beispiel gegen die Allgemeinen Geschäftsbedingungen (AGB) bei Erwerb und Einsatz der Software verstoßen. Die Suche kann für IT-Sicherheitsforscher daher zu juristischen Konsequenzen führen, wenn sie nicht ausdrücklich beauftragt wurde.

Die Anzahl von kritischen Schwachstellen kann durch eine entsprechende Designphilosophie bereits während

der Software-Entwicklung reduziert werden. Um Software-Produkte sicherer zu gestalten, müssen *Security by Design* und *Security by Default* umgesetzt werden. Die *Security-by-Design*-Philosophie setzt bereits zu Beginn einer Software-Entwicklung an und wird im kompletten Produktlebenszyklus berücksichtigt. Dabei nimmt die Sicherheit eines Software-Produkts einen vergleichbaren Stellenwert ein, wie beispielsweise die Nutzerfreundlichkeit. Besonders bei Software, die in sensiblen Bereichen eingesetzt wird, ist der Stellenwert sogar deutlich höher.

Das *Security-by-Default*-Konzept stellt die Konfiguration einer Software bei der Auslieferung in den Fokus. So erlaubt eine Vielzahl von Software-Produkten den Nutzerinnen und Nutzern unterschiedliche Konfigurationen vorzunehmen, um dem jeweiligen Anwendungszweck zu entsprechen oder zwischen Nutzbarkeit und Sicherheit abzuwägen. Bei einer Auslieferung im Sinne des *Security by Default* ist die Standardeinstellung (Default) die sicherste Konfiguration, in der die Software betrieben werden kann. Dieses Konzept ist relevant, da immer häufiger Fälle bekannt werden, in denen die initiale Konfiguration nicht angepasst und schließlich durch Angreifer ausgenutzt wurde.

Der Umgang mit Schwachstellen in Software-Produkten ist ein wesentlicher Faktor für die sichere Digitalisierung in Deutschland. Der breitere und intensivere Einsatz von Bug-Bounty-Programmen, CVD-Prozessen (vgl. Kapitel *Computer Emergency Response Team für Bundesbehörden*, Seite 67), *Security by Design* und *Security by Default* zeigt, dass dieses Verständnis von immer mehr Software-Herstellern, IT-Sicherheitsforschern und staatlichen Organisationen geteilt wird.

Gerade beim Umgang mit Schwachstellen zeigte sich auch im aktuellen Berichtszeitraum die digitale Eigenverantwortung der Anwenderinnen und Anwender. Ihnen obliegt es, ihre Software angemessen zu pflegen. Hierzu zählen das Einspielen von Aktualisierungen und das Reagieren auf Herstellerhinweise, falls noch kein *Patch* zur Verfügung steht. Aber selbst bei kritisch zu wertenden Schwachstellen hat das BSI immer wieder beobachtet, dass zur Verfügung stehende Aktualisierungen verzögert oder gar nicht eingespielt werden.

Die Mitwirkung der Anwenderinnen und Anwender war auch im Berichtszeitraum gefordert, denn am 14. Januar 2020 endete der Support für die Microsoft-Produkte Windows 7 und Windows Server 2008 (R2). Seitdem werden kritische oder wichtige Sicherheitsupdates für diese Betriebssysteme nur noch für Kundinnen und Kunden des kostenpflichtigen Extended-Security-Updates-Programms zur Verfügung gestellt. Andere Nutzer erhalten keine Sicherheitsupdates mehr. Die Betriebssystemversi-

on Windows 7 ist inzwischen ein Jahrzehnt alt und noch weit verbreitet. Nach dem Support-Ende bleibt Windows 7 voll funktionsfähig und installationsfähig, jedoch ungeschützt vor neuen Risiken.

Das BSI empfiehlt Privatanwenderinnen und -anwendern sowie Unternehmen, die betroffenen Windows-Betriebssysteme nicht mehr zu verwenden und zu einem Betriebssystem zu wechseln, für das weiterhin Sicherheitsupdates bereitgestellt werden. Vor einem Upgrade oder Wechsel des Betriebssystems sollte geprüft werden,

ob die technischen Systemanforderungen für das neue Betriebssystem erfüllt sind. Auch eingesetzte Programme oder Fachanwendungen sowie Peripheriegeräte wie zum Beispiel Drucker sollten unterstützt werden. Schließlich sind Datensicherungen durchzuführen, um einem möglichen Datenverlust vorzubeugen. Da die Migration eines Betriebssystems, insbesondere in größeren Organisationen, mit einem beträchtlichen zeitlichen und personellen Aufwand verbunden sein kann, sollte zeitnah gehandelt werden.



Kritische Schwachstelle in Citrix-Produkten

Sachverhalt

Am 17. Dezember 2019 veröffentlichte das US-Softwareunternehmen Citrix Informationen über kritische Schwachstellen in mehreren seiner Produkte und empfahl Gegenmaßnahmen, um gegen eine Ausnutzung abgesichert zu sein. Die betroffenen Software-Produkte dienen unter anderem als VPN-Gateway für den entfernten Zugriff auf organisationsinterne Anwendungen und wurden weltweit von über 80.000 Unternehmen in 158 Ländern eingesetzt. In ihrer Funktion als Gateway stellen sie einen der neuralgischen Netzwerkübergänge dar, die ein Unternehmensnetzwerk vom Internet trennen und regulieren. Durch die Schwachstellen waren Angreifer in der Lage, einen beliebigen Code – auch Schadprogramme – auf ebenjenen Netzwerkübergängen zur Ausführung zu bringen. Abhängig von weiteren Schutzmaßnahmen in den Unternehmensnetzwerken standen den Angreifern dadurch ggf. weitreichende Möglichkeiten für weitere Angriffe offen.

Ab dem 8. Januar 2020 wurden *Exploits* öffentlich, die sich durch ihre einfache Handhabbarkeit auszeichneten. Dies ermöglichte unterschiedlichen Angreifern, die *Exploits* zeitnah für ihre jeweiligen Zwecke anzupassen und auszunutzen (vgl. *Quellenverzeichnis*⁷: www.trustedsec.com). In der Folge konnte eine massive Ausnutzung der Schwachstellen beobachtet werden (vgl. *Quellenverzeichnis*⁸: <https://deyda.net>, vgl. *Quellenverzeichnis*⁹: <https://blog.dco.de>, vgl. *Quellenverzeichnis*¹⁰: www.fireeye.com).

Reaktion

Das BSI hat seit dem Bekanntwerden des *Exploit*-Codes ca. 5.000 verschiedene durch die Schwachstellen verwundbare Systeme allein in Deutschland identifiziert und an die zuständigen Netzbetreiber und Internet-*Provider* gemeldet, um über die Gefährdung zu informieren. Es ist jedoch anzunehmen, dass zeitweise mehr als die 5.000 identifizierten Systeme in Deutschland gefährdet waren.

Bis zum 24. Januar 2020 stellte der Hersteller sukzessive Sicherheitsupdates bereit, welche die Schwachstellen in den betroffenen Produktversionen schlossen. Nach der Bereitstellung der Updates nahm die Anzahl an verwundbaren Systemen deutlich ab und lag zuletzt bei etwa 230. Zudem hat das BSI mehrere Dutzend Systeme an die zuständigen Netzbetreiber und Internet-*Provider* gemeldet, auf denen die Angreifer sogenannte *Backdoors* installiert hatten. Solche *Backdoors* ermöglichen den Angreifern den Zugriff auf das System, auch wenn die Schwachstelle geschlossen wurde.

Empfehlung

Anwenderinnen und Anwendern der betroffenen Produkte, die die Handlungsempfehlungen des Herstellers zur vorübergehenden Schließung der Schwachstellen bis zur Bereitstellung eines *Patches* nicht vor der beobachteten großflächigen Ausnutzung umgesetzt hatten, wird empfohlen, ihre direkt mit dem Internet verbundenen Citrix-Systeme auf eine wahrscheinliche Kompromittierung hin zu prüfen.

Bereits vor dem Bekanntwerden von Schwachstellen sollten nach Möglichkeit nur Programme auf einem System installiert sein und betrieben werden, die auch notwendig sind. Diese Verkleinerung der Angriffsfläche reduziert das Risiko, Opfer eines Cyber-Angriffs zu werden („Härtung“).

Wenn Sicherheitsupdates für Software zur Verfügung stehen, die eine Schwachstelle schließen, sollten diese in der Regel umgehend installiert werden. In Fällen, wo dies zum Beispiel aus Kompatibilitätsgründen nicht möglich ist, sollte der Einsatz von Workarounds geprüft werden, die die Ausnutzung einer Schwachstelle verhindern. In Situationen, in denen weder *Patches* noch funktionierende vorübergehende Lösungen vorhanden sind, sollte eine befristete Abschaltung der betroffenen Software erwogen werden.

Inwieweit die oben genannten Maßnahmen im Einzelfall umsetzbar sind, hängt von den individuellen Einsatzbedingungen einer Software und den damit einhergehenden Risiken ab. In jedem Fall sollte aber auf eine Schwachstelle reagiert werden, da eine unveränderte Beibehaltung zu hohen Risiken führt.



Kritische Schwachstellen in Windows' Remote Desktop Protokoll

Sachverhalt

Das Remote Desktop Protocol (RDP) ist ein Dienst in Microsofts Betriebssystem Windows und ermöglicht unter anderem die Fernwartung des Systems. Im Mai 2019 wurde die kritische Schwachstelle BlueKeep in diesem Dienst bekannt, die es entfernten Angreifern ermöglicht, beliebige Programme – auch Schadprogramme – auf dem angreifbaren System auszuführen (vgl. *Quellenverzeichnis*¹¹: www.microsoft.com). Von BlueKeep sind die älteren Systeme Windows XP, Windows Server 2003, Windows 7, Windows Server 2008 und Windows Server 2008 R2 betroffen. Seit Juni 2019 sind öffentliche *Exploits* für BlueKeep verfügbar. Diese Schadprogramme suchen nach offen erreichbaren RDP-Diensten im Internet, um sich über die Schwachstelle automatisiert weiterzuverbreiten. BlueKeep wird deshalb auch als „wurmfähig“ bezeichnet. Szenarien wie 2017, als die *Ransomware* WannaCry innerhalb kurzer Zeit mehrere 100.000 Windows-Systeme infizierte und Daten in großem Umfang verschlüsselte, sind denkbar.

Darüber hinaus wurden im August 2019 unter dem Namen DejaBlue zwei weitere Schwachstellen mit ähnlichem Bedrohungspotenzial bekannt. Diese betrafen auch neuere Windows-Systeme bis einschließlich Windows 10 und Windows Server 2019. Auch über DejaBlue können Angreifer ohne *Authentifizierung* oder Interaktion eines Nutzers einen beliebigen Code aus der Ferne ausführen.

Die Schwachstellen sind als kritisch anzusehen. Zwar ist der RDP-Dienst in der Standardeinstellung nicht aktiv, für eine hohe Anzahl von Servern wird der Dienst aber für die Fernwartung verwendet, und dies teilweise relativ ungeschützt über das Internet.

Reaktion

Microsoft hat in der Konsequenz Sicherheitsupdates für die betroffenen Systeme bereitgestellt, und zwar auch für die sonst nicht mehr unterstützten WindowsXP und Windows-Server-2003-Systeme. Zudem wiesen Microsoft sowie verschiedene deutsche und internationale Sicherheitsbehörden und –dienstleister auf die Schwachstellen und die zur Verfügung stehenden Sicherheitsupdates hin.

Das BSI hat zu BlueKeep und DejaBlue Cyber-Sicherheitswarnungen und Pressemitteilungen veröffentlicht (vgl. *Quellenverzeichnis*¹²: www.bsi.bund.de).

Empfehlung

Bereits bei der Einrichtung von Systemen sollten nur die Programme installiert und betrieben werden, die auch notwendig sind. Eine verkleinerte Angriffsfläche senkt das Risiko, Opfer eines Angriffs zu werden.

Wenn ein Sicherheitsupdate zur Verfügung steht, um eine Schwachstelle zu schließen, sollte dies umgehend installiert werden. In Fällen, in denen dies nicht möglich ist, sollten vorübergehende Lösungen geprüft werden, die die Ausnutzung der Schwachstelle verhindern. Mögliche vorübergehende Lösungen sind stark abhängig von der Art der Schwachstelle und dem betroffenen Dienst. Sie können beispielsweise in einer zeitweisen Abschaltung des jeweiligen Dienstes oder einer zeitweisen Nutzung einer alternativen Softwarekomponente liegen.

1.3.2 Schwachstellen in Hardware-Produkten

Neben rein softwarebasierten Angriffen auf die Vertraulichkeit von Daten oder die Integrität und Verfügbarkeit von Diensten und Dienstleistungen, rücken Angriffe auf die Hardware in stetig wachsendem Maße in den Fokus von Sicherheitsexpertinnen und -experten und auch der Öffentlichkeit. Die Lücken Spectre und Meltdown in Prozessoren sowie die Meldungen um vermeintliche versteckte Spionagechips auf Hauptplatinen, beides Vorfälle aus dem Jahr 2018, sind nur zwei Beispiele, die die Aufmerksamkeit auf sich gezogen haben und den Stellenwert sicherer Hardware in besonderem Maße verdeutlichen.

Angriffen auf Hardware ist gemein, dass diese in der Regel sehr tief in der jeweiligen Architektur oder dem

organisatorischen Prozess ansetzen, wie etwa an der Physik von Transistoren in hochintegrierten Schaltungen, der Mikroarchitektur eines hochkomplexen Prozessors oder auch den Schritten Produktion und Lieferkette bei Betrachtung des Lebenszyklus eines IT-Produkts. Dem vergleichsweise hohen Schwierigkeitsgrad und der Komplexität solcher Angriffe steht ein potenziell sehr hoher Gewinn entgegen. Ist die grundlegende Hardware kompromittiert oder bieten darin enthaltene Schwächen ein hinreichend großes Einfallstor, verlieren auf ihr aufsetzende Sicherheitsmechanismen grundsätzlich ihre Wirkung.



Angriffe auf Authentisierungstoken

Passwörter sind heutzutage immer noch die übliche Methode, sich bei Internetdiensten zu authentisieren. Allerdings haben Passwörter einige Nachteile (vgl. Kapitel *Zwei-Faktor-Authentisierung*, Seite 47). Daher bieten immer mehr Dienste eine zusätzliche Absicherung der Anmeldung durch die Benutzung spezieller Hardware an, mit denen zusätzlich zum Passwort (Wissen) ein weiteres Merkmal (Besitz) der Anwenderinnen und Anwender geprüft wird.

Allerdings können auch solche Sicherheitstoken Schwachstellen aufweisen. Im Rahmen eines BSI-Projekts wurde ein nicht nach Common Criteria zertifiziertes, kommerziell vertriebenes FIDO-U2F-Token, das als Schlüsselspeicher für Webanwendungen eingesetzt wird, durch das Fraunhofer-Institut AISEC auf Sicherheitslücken untersucht. Der Hersteller wurde über die Ergebnisse informiert. (Der entsprechende CVE-Eintrag hat die Nummer CVE-2020-12061.)

Bei diesem Token war es möglich, das Gehäuse zu öffnen, ohne äußere Spuren zu hinterlassen. In der Folge konnten mithilfe eines Oszilloskops sicherheitsrelevante gerätespezifische Daten aus dem Gerät ausgelesen werden. Anschließend wurde eine neue *Firmware* aufgespielt, die Schlüssel mit einer sehr geringen Entropie erzeugt und bereits vorhandene Schlüssel, die noch mit hoher Entropie erzeugt wurden, über eine *Phishing*-Webseite ausleitet. Außerdem bestand die Möglichkeit, die Kopie eines Tokens zu erstellen. Die zusätzliche Sicherheitsannahme durch das Merkmal Besitz war somit nicht mehr gültig.

Dieses Vorgehen entspricht einem sogenannten Evil-Maid-Szenario, in dem ein Angreifer gezielt kurzzeitig die Kontrolle über ein Token erlangt und dieses manipuliert. Außerdem besteht die Möglichkeit, ein sogenanntes Supply-Chain-Szenario durchzuführen, wobei ein nicht vertrauenswürdiger Hersteller, Lieferant oder Händler einen beliebig großen Anteil der Token vor der Auslieferung an die Kundinnen und Kunden manipuliert.

Bei diesem Angriff wurden zwei prinzipiell unabhängige Schwachstellen kombiniert:

- Die sicherheitsrelevanten Daten können unverschlüsselt mitgelesen werden (Schwäche im Design).
- Der Mikrocontroller ist als Maßnahme gegen Manipulationen zwar mit einem Leseschutz versehen, das Schreiben wird dadurch aber nicht verhindert (Schwäche des verwendeten Mikrocontrollers).

Die Untersuchung belegt erneut, dass es unabdingbar ist, Sicherheits-Hardware gründlich zu untersuchen und dabei in ihrer Gesamtheit zu betrachten. Bei einer getrennten Analyse von Hard- und Software können Schwachstellen eventuell unentdeckt bleiben.



Schwachstellen in SmartCards

SmartCards sind Plastikkarten, in die eine elektronische Verarbeitungseinheit, der sogenannten Mikrochip, eingebettet ist. Diese Mikrochips beinhalten unter anderem spezielle Bausteine für die Verschlüsselung von Nachrichten. Der bereits ältere Datenverschlüsselungsstandard (Data Encryption Standard, DES) wird heute noch benutzt, meist in der Form der dreifachen Verschlüsselung (3DES). Forscher haben in der Umsetzung des Standards auf SmartCards vor kurzem Schwachstellen gefunden und veröffentlicht. Da diese Veröffentlichungen kompliziert sind und es so wirkt, dass die Schwachstellen nur mit speziellen Geräten im Labor ausgenutzt werden können, war unklar, ob die Schwachstellen die Verschlüsselung unsicher machen. Da diese Schwachstellen von anderen Experten nicht nachgestellt werden konnten, hat das BSI gemeinsam mit dem Fraunhofer Institut für Angewandte und Integrierte Sicherheit (AISEC) versucht, den für die Durchführung des Angriffs notwendigen Laboraufbau nachzustellen und den Angriff zu bewerten. Bei diesen Untersuchungen hat sich gezeigt, dass die Stärke der Verschlüsselung wesentlich abgeschwächt werden konnte, auch bei der heute eingesetzten Dreifachverschlüsselung. Diese Reduzierung der Schlüsselstärke führt dazu, dass der Datenverschlüsselungsstandard nicht mehr den Sicherheitsanforderungen entspricht. Deswegen sollten SmartCards, die noch auf dem älteren Datenverschlüsselungsstandard mit Dreifachverschlüsselung basieren, ausgetauscht und durch solche ersetzt werden, die den fortgeschrittenen Verschlüsselungsstandard (Advanced Encryption Standard, AES) einsetzen.



Angriffe auf die Ausführung von Programmen

Die in modernen Computern verbauten Verarbeitungseinheiten führen die Befehle von Programmen nicht ausschließlich in der vorgegebenen Reihenfolge aus. Zur Leistungssteigerung werden die Befehle eines Programms umsortiert, um sämtliche Rechenwerke der Verarbeitungseinheit möglichst optimal und gleichzeitig auszulasten. Durch diese Optimierung kann es passieren, dass Befehle fehlerhaft ausgeführt werden. Zum Beispiel werden die Befehle mit zum Zeitpunkt der Ausführung noch nicht vollständig berechneten Zwischenergebnissen ausgeführt. Dadurch werden auch Verzweigungen durch Wenn-Dann-Bedingungen falsch ausgewertet und Befehle ausgeführt, die in dieser Form bei einer sequentiellen Abarbeitung nicht ausgeführt worden wären. Erkennt die Verarbeitungseinheit später einen solchen Ausführungsfehler, werden die durchgeführten Operationen rückgängig gemacht. Dadurch wird der entstandene Fehler korrigiert. Obwohl diese Fehler außerhalb der Verarbeitungseinheit nicht sichtbar sein sollten, haben Forscher Anfang 2018 gezeigt, dass in Zwischenspeichern noch Auswirkungen der fehlerhaft ausgeführten Befehle zu finden sind und wie diese dazu genutzt werden können, um die verarbeiteten Daten eines anderen Programms auszuspähen. Obwohl diese Angriffe auf die Ausführung von Programmen sehr komplex sind und für die jeweilige Architektur und die spezifischen internen Optimierungsmaßnahmen der Verarbeitungseinheit angepasst werden müssen, stellen sie eine ernsthafte Bedrohung dar und müssen beseitigt werden. Dazu stellen die Hersteller Verbesserungen der Betriebssoftware der Verarbeitungseinheiten zur Verfügung, die allerdings teilweise zu erheblichen Einbußen in der Leistung der Verarbeitungseinheit führen. Gleichzeitig werden von Forschern weltweit neue Angriffsmethoden entwickelt, die auf ähnlichen Methoden aber anderen Optimierungen und Zwischenspeichern verschiedener Verarbeitungseinheiten basieren.

Rückblickend zeigt sich, dass die erwartete Entwicklung der Ausführungsangriffe eingetreten ist. Entsprechend sind die im letztjährigen Lagebericht vorgeschlagenen Handlungsempfehlungen nach wie vor aktuell: Mittel- und langfristig sollten Rechner derart konzipiert werden, dass besonders vertrauenswürdige Daten, insbesondere Schlüsselmaterial, lediglich auf vollständig separierten Verarbeitungseinheiten verarbeitet werden. Zu schützen sind im Kontext der Ausführungsangriffe insbesondere virtualisierte *Cloud*-Systeme. Aufgrund der hohen Komplexität auch in der Ausnutzung der bestehenden Lücken erscheinen Angriffe in der Fläche nicht effizient und sind daher wenig wahrscheinlich.

1.4 Advanced Persistent Threats

Advanced Persistent Threats (APTs) unterscheiden sich von anderen Bedrohungen der IT-Sicherheit durch die Motivation und die Vorgehensweise der Angreifer. Während die meisten Schadprogramme in der Regel von finanziell motivierten Angreifern massenhaft und ungezielt verteilt werden, sind APTs oft langfristig und mit großem Aufwand geplante Angriffe auf einzeln ausgewählte, herausgehobene Ziele. APT-Angriffe dienen normalerweise nicht der kriminellen Gewinnerzielung, sondern der Beschaffung von Informationen über das Ziel und ggf. der Sabotage.

Die technischen Unterschiede zwischen kriminellen Aktivitäten und gezielten Angriffen verschwimmen zunehmend. Dies zeigt sich unter anderem daran, dass auch *Ransomware*-Angriffen wochenlanges Ausbreiten in internen Netzwerken vorangehen kann (vgl. Kapitel *Emotet: Neue Qualität fortschrittlicher Angriffe*, Seite 11), was früher nur von APT-Angriffen bekannt war. Dadurch gewinnt als Unterscheidungskriterium der Umstand Bedeutung, dass gezielte Angriffe stets einen strategischen Hintergrund haben. Eine Betrachtung der Sicherheitslage im Bereich von APT-Angriffen muss daher diese Dimension berücksichtigen, wofür sich derzeit der Begriff der strategischen Threat Intelligence etabliert. Die strategische Sicht erleichtert eine Einordnung, aus welchen Gründen, beispielsweise Branche und Produkte oder geografischer Standort, die eigene Organisation ein potenzielles Ziel für APT-Angriffe sein kann.

Derzeit ist eine dreistellige Zahl von APT-Gruppen weltweit aktiv. In Deutschland sind davon im Berichtszeitraum Aktivitäten von knapp über einem Dutzend beobachtet worden, wobei die Art der Aktivität von einfachen Angriffsversuchen und *Phishing*-E-Mails bis zu erfolgreichen Kompromittierungen reicht. Ziel der Angriffsversuche auf die Regierungsnetze in Deutschland waren vor allem Ministerien mit außenpolitischen Aufgaben. Auch Botschaften waren Ziel von APT-Gruppen, die einen Fokus auf das vertretene Land hatten. Weitere Angriffe bzw. Angriffsversuche richteten sich gegen international agierende Nicht-Regierungs-Organisationen und Unternehmen im Chemie-, Automobil- und Maschinenbausektor. Dies verdeutlicht, dass APT-Gruppen gezielt eingesetzt werden und einer strategischen Ausrichtung folgen, die oftmals mit einer Fokussierung auf bestimmte Weltregionen oder Branchen einhergeht.

Besonders viel Aktivität zeigte sich im aktuellen Berichtszeitraum in Südostasien, Zentralasien und im Mittleren Osten. Ein deutlicher Anstieg der APT-Aktivität ist in diesen Regionen im Telekommunikationssektor zu beobachten. Dieser Sektor bietet den Angreifern sowohl Daten zum Ausspähen von Individuen als auch Daten zu Technologien oder Geschäftsgeheimnissen. Viele öffentliche Berichte

dokumentieren zudem, dass in vielen Staaten Spionageprogramme genutzt werden, um Kritiker in der eigenen Bevölkerung auszuspähen.

Der überwiegende Teil von APT-Aktivitäten dient nach wie vor der Informationsbeschaffung in Regierungsbehörden, Militärorganisationen, Wirtschaftsunternehmen oder bei Regimekritikern. Sabotageangriffe sind deutlich seltener und auf einzelne Sektoren und Regionen beschränkt. Allerdings sind Fälle bekannt, in denen Informationen gesammelt wurden, die bei Bedarf Sabotageangriffe unterstützen könnten.

Auf der technischen Seite findet eine Diversifizierung von Angriffsmethoden statt. Während APT-Angriffe früher vor allem über E-Mail-Anhänge oder Links auf Schadcode-Webseiten erfolgten, variieren die Angreifer die *Angriffsvektoren* mittlerweile. Dazu gehören die Kompromittierung von legitimen Software-Produkten, das Ausnutzen von Schwachstellen in Fernwartungsdiensten und das Wiederverwenden ausgespähter Zugangsdaten. Zudem nutzt eine zunehmende Zahl an APT-Gruppen die Infrastrukturen und Zugangsdaten von Zulieferern, um ihre eigentlichen Ziele zu kompromittieren. In einem ersten Schritt werden dabei schlechter geschützte Netzwerke von Zulieferern angegriffen. Im zweiten Schritt werden die dort erlangten Informationen und Zugänge verwendet, um in das Netzwerk des tatsächlichen Angriffsziels einzudringen. Dadurch können auch solche Unternehmen, die eigentlich ein hohes IT-Sicherheitsniveau und professionelle Sicherheitsteams besitzen, kompromittiert werden, wenn sie einem schlecht gesicherten Zulieferer vertrauen und diesen an das eigene Netzwerk anschließen.

Zudem entwickeln und testen mehrere APT-Gruppen aktuell Methoden, um Unternehmensrouter zu kompromittieren. Dies ist bedenklich, da für diese Router bisher nur wenige Sicherheitsprodukte existieren, die ein Monitoring ermöglichen oder gar Angriffe detektieren könnten.

Obwohl die meisten APT-Gruppen frei verfügbare Werkzeuge wie Cobalt Strike oder Empire verwenden, deren Aufbau und Spezifikationen bekannt sind, entwickeln viele Gruppen dennoch zusätzlich eigene Tools weiter. Insbesondere wird viel Aufwand investiert, um zusätzliche Teilschritte in der initialen Phase von Angriffen vorzunehmen. Schadprogramme werden nicht direkt auf das Zielsystem übertragen, sondern erst nach und nach über mehrere Stufen nachgeladen – teilweise erst nach einer Prüfung durch die Angreifer, ob das kompromittierte System als interessantes Ziel erachtet wird. Dieser Aufwand verdeutlicht, dass die Angreifer die Detektionsmethoden und Analyseprozesse von Sicherheitsteams verstanden haben und versuchen, die eigenen Schadprogramme der Analyse zu entziehen.

1.5 Distributed Denial of Service

Als Distributed-Denial-of-Service-Angriffe (*DDoS-Angriffe*) werden Überlastungsangriffe auf Internetdienste bezeichnet. Wenn eine Webseite wie zum Beispiel ein Online-Shop oder eine Internetplattform nicht mehr erreichbar ist, Netzwerkdienste ausfallen oder kritische Geschäftsprozesse wegen Überlastung blockiert werden, ist eventuell ein *DDoS-Angriff* die Ursache. *DDoS-Angriffe* werden meist genutzt, um gezielt Schaden anzurichten, die Opfer zu erpressen oder Aufmerksamkeit für eine eigene Sache zu erregen, beispielsweise eine politische Forderung. Ein weiteres Motiv liegt darin, andere Angriffe zu verschleiern oder erst zu ermöglichen. *DDoS-Angriffe* werden häufig mittels einer großen Anzahl von Computern, ggf. Servern, parallel durchgeführt (vgl. Kapitel *Botnetze*, Seite 16). *DDoS-Angriffe* werden bereits seit zwei Jahrzehnten beobachtet, und so feierte *DDoS* im Berichtszeitraum einen runden Geburtstag: Als erster beobachteter *DDoS* gilt ein Angriff auf die Universität von Minnesota am 22. Juli 1999 (vgl. *Quellenverzeichnis*¹³: www.link11.com).

Die Auswirkungen von *DDoS-Angriffen* können beträchtlich sein. Sie können bei den betroffenen Institutionen einen großen wirtschaftlichen Schaden verursachen und auch einen Reputationsverlust nach sich ziehen. Für die digitale Geschäftswelt stellen sie eine der größten Cyber-Bedrohungen überhaupt dar, da sie sich unmittelbar gegen die Verfügbarkeit der angebotenen Dienstleistungen richten.

Wie bereits im vergangenen Berichtszeitraum war die Lage im Bereich von *DDoS-Angriffen* durch mehrere, sich überschneidende Entwicklungen gekennzeichnet. Nach wie vor setzte sich die stetige Spezialisierung der Angreifer durch Entwicklung und Anwendung neuer *Angriffsvektoren* fort. Aktuelle Beispiele dafür sind WS-Discovery, Apple Remote Management Service und TCP-Amplification. Gleichwohl standen für fachlich weniger spezialisierte Angreifer auch weiterhin sogenannte *DDoS-Boooterdienste* zur Verfügung. Sie machen es Angreifern ohne technische Kenntnisse und ohne kriminelle Biographie (z. B. Schülern (vgl. *Quellenverzeichnis*¹⁴: www.cl.cam.ac.uk) immer leichter, Angriffe mit hohem Schadenspotenzial durchzuführen (vgl. *Quellenverzeichnis*²: www.bsi.bund.de).

Darüber hinaus waren im Berichtszeitraum erhöhte *DDoS*-Aktivitäten zu anlassbezogenen Ereignissen im E-Commerce-Umfeld (Vorweihnachtsgeschäft, Black Friday, Cyber Monday) oder im Gaming-Umfeld zu beobachten.

Neu dagegen sind im aktuellen Berichtszeitraum beobachtete Angriffe mit erhöhter Qualität, welche weit über das Maß der erwarteten Entwicklungen durch Spezialisie-

rung auf bestimmte Zielgruppen hinausgehen: Gemeint sind technisch laborierte Angriffe, die im Gegensatz zu früheren bandbreitenstarken Angriffen nunmehr intelligente und effiziente Strategien anwenden. Diese Angriffe können selbst bislang als wirksam geltende Schutzmaßnahmen überwinden und dadurch die Entwicklung grundlegend neuer Schutzkonzepte und Schutzmaßnahmen erforderlich machen.

So vermehren sich Meldungen über aktiv gesteuerte Angriffe, bei denen der Angreifer aktiv auf Gegenmaßnahmen des Opfers reagiert, um die Wirkung des Angriffs trotz Gegenwehr aufrechterhalten zu können. Dafür verwendet der Angreifer Informationen über den Verlauf des Angriffs, die er zum Beispiel aus öffentlichen Quellen bezieht. Ein Beispiel dafür ist der Angriff auf eine große Direktbank mit rund vier Millionen Kundinnen und Kunden im Januar 2020, der über mehrere Tage angehalten hat. Der Angreifer nutzte dabei die öffentliche Seite allestörungen.de, um Informationen über den Verlauf und die Wirkung des Angriffs auf das Opfer zu gewinnen. Die Seite sammelt Statusberichte und Störungsmeldungen zum Beispiel von Kundinnen und Kunden und erkennt dadurch frühzeitig Serviceunterbrechungen und -störungen bei Dienstleistern aus verschiedenen Bereichen (z. B. Banking, Online-Handel, Internet-Provider). Dem Angreifer standen auf diese Weise zeitnah die benötigten Informationen zur Verfügung, um auf die getroffenen Gegenmaßnahmen aktiv reagieren zu können. Bei einem Angriff auf einen südafrikanischen Internet-Provider beobachtete der Angreifer die Gegenmaßnahmen ebenfalls, um seine Angriffsstrategie daran anzupassen. Da gegen diese noch keine Schutzmaßnahmen bestanden, blieb der Internet-Provider weiterhin nicht verfügbar.

Im zweiten Halbjahr 2019 trat zudem verstärkt eine Strategie auf, die bereits seit Ende 2017 bekannt ist und als Carpet Bombing (Flächenbombardement) bezeichnet wird (vgl. *Quellenverzeichnis*¹⁵: www.datensicherheit.de; vgl. *Quellenverzeichnis*¹³: www.link11.com). Dabei umgeht der Angreifer den klassischen *DDoS*-Schutz an der Netzwerkgrenze, indem er den Angriff gegen eine große Anzahl von IP-Adressen innerhalb dieses Netzwerks richtet. Die Datenmenge des Angriffs pro IP-Adresse ist dadurch jeweils so klein, dass sie sich unter den Detektions-Schwellwerten der meisten *DDoS*-Schutzlösungen bewegt, der Angriff daher nicht detektiert und somit nicht abgewehrt wird. In der Summe entspricht die Angriffsbandbreite aller Einzelangriffe zwar der eines großen *DDoS-Angriffs* von mehreren dutzenden oder hunderten Gbit/s, der Angriff wird jedoch nicht detektiert. Dieser Angriffstyp stellt besonders für Internet-Provider eine erhebliche Gefahr dar und wurde auch bei dem erwähnten Angriff auf den südafrikanischen Internet-Provider über zwei Tage angewendet.

Nicht unmittelbar zu den neuen elaborierten Angriffen zählen die sogenannten Multivektor-Angriffe, die bereits im BSI-Lagebericht 2019 thematisiert wurden. Sie erreichten im vierten Quartal 2019 einen Anteil von 65 Prozent und setzten somit ihre Entwicklung weiter fort (vgl. *Quellenverzeichnis*¹³: www.link11.com). Im Gegensatz zu herkömmlichen *DDoS-Angriffen* zeichnen sich Multivektor-Angriffe durch eine zielgerichtete Zusammensetzung der verwendeten *Angriffsvektoren* aus. Dies bedeutet für die Opfer eine deutlich komplexere Bedrohungslage, für deren Abwehr ein ebenso komplexes Fachwissen über die verschiedenen *DDoS-Angriffsarten* nötig ist. Auch diese Angriffsform hat das Potenzial, gegen bestehende Schutzmaßnahmen ihre Wirkung entfalten zu können. Die Reaktionszeiten von statischen Schutzlösungen auf Basis statischer Schwellwerte erweisen sich angesichts von Angriffen mit Vektorenwechseln im Minutentakt als zu langsam und zu ineffizient.

Insgesamt betrachtet hat sich der Trend aus dem vergangenen Berichtszeitraum hin zu fortschrittlichen *DDoS-Angriffen* weiter verstetigt, auch wenn fortschrittliche Angriffe – mit Ausnahme der bereits verbreiteten Multivektor-Angriffe – momentan noch einen vergleichsweise geringen Anteil am gesamten Angriffsaufkommen ausmachen. Auch anhand vergleichbarer Erfahrungen bei anderen Bedrohungen (z. B. bei Schadsoftware) erscheint es plausibel, dass diese Entwicklung anhält und fortschrittliche *DDoS-Angriffe* in der Zukunft zunehmen werden.

Der Trend hin zu fortschrittlichen Angriffen macht es erforderlich, die Schutzlösungen entsprechend anzupassen. Die Wirksamkeit von statischen Schutzlösungen ist dabei allerdings begrenzt. Um den fortschrittlichen Angriffen in diesem Sinne begegnen zu können, sind dynamische Konzepte für Gegenmaßnahmen erforderlich wie zum Beispiel die automatische Ableitung von Filterdefinitionen aus dem Angriffsmuster. Qualifizierte *DDoS-Mitigation-Dienstleister* im Sinne von § 3 Abs. 3 BSI-G erfüllen die letztgenannte Anforderung. Eine Liste mit qualifizierten Dienstleistern einschließlich der verwendeten Auswahlkriterien ist auf www.bsi.bund.de (vgl. *Quellenverzeichnis*¹⁶: www.bsi.bund.de) verfügbar.

1.6 Angriffe im Kontext Kryptografie

Kryptografische Mechanismen stellen wichtige Grundbausteine für die Umsetzung von Sicherheitsfunktionen in IT-Produkten dar. Dem Stand der Technik entsprechende Kryptoalgorithmen liefern hierfür grundsätzlich ausgezeichnete Sicherheitsgarantien. Das BSI empfiehlt in der Technischen Richtlinie TR-02102 eine Reihe kryptografischer Algorithmen und Protokolle, die aufgrund

eingehender mathematischer Kryptoanalyse allgemein als sicher angesehen werden.

Bevor ein kryptografisches Verfahren implementiert werden kann, wird es zunächst mathematisch bzw. auf dem Papier geplant. Dabei ist die Sicherheit eines solchen Verfahrens in der Regel an gewisse Voraussetzungen geknüpft. Zum Beispiel müssen die verwendeten Schlüssel unvorhersagbar sein und dürfen nicht durch Zwischenergebnisse der Prozessberechnungen oder *Seitenkanalangriffe* abfließen. Falls in der praktischen Umsetzung eines Verfahrens nicht alle Voraussetzungen erfüllt sind, müssen zusätzliche Absicherungsmaßnahmen getroffen werden. Folgende Aspekte können dazu beitragen, dass ein Kryptosystem in der Praxis nicht den vorgesehenen Zweck erfüllt:

- Schwächen in kryptografischen Mechanismen (vgl. Kasten *Kollisionsangriffe gegen SHA-1*, Seite 31)
- Implementierungsfehler
- Unzureichend abgesicherte Seitenkanäle
- Hardware-Schwachstellen (vgl. Kapitel *Schwachstellen in Hardware-Produkten*, Seite 26)
- Schwache Zufallszahlen, die zu vorhersagbaren und damit weniger sicheren kryptografischen Schlüsseln führen können.

In einem typischen Einsatzszenario wie die Kommunikation über ein unsicheres Netzwerk, in dem zumindest die Endpunkte geschützt sind, werden IT-Produkte in einer sicheren Umgebung betrieben und kommunizieren mit anderen Geräten über ein offenes Netzwerk. Für die vertrauliche und integritätsgeschützte Kommunikation stehen verschiedene kryptografische Protokolle zur Verfügung, für die gemeinhin angenommen wird, dass ein Angreifer mit Netzwerkzugriff weder die geheimen Schlüssel in Erfahrung bringen noch Nachrichten entschlüsseln oder unbemerkt manipulieren kann. Für die Wirksamkeit der kryptografischen Protokolle muss zum einen die korrekte Implementierung sichergestellt sein. Zum anderen muss verhindert werden, dass das an der Netzwerkschnittstelle beobachtbare Verhalten der Geräte (z. B. Fehlermeldungen, Antwortzeit) Informationen über verarbeitete Geheimnisse preisgibt (vgl. Kasten *Laufzeitangriffe gegen ECDSA*, Seite 32).

Bei der Absicherung von Kryptosystemen, die selbst Angreifern in räumlicher Nähe standhalten sollen, müssen neben der Laufzeit noch weitere Informationen wie Stromverbrauch oder elektromagnetische Abstrahlung der Geräte berücksichtigt werden, weil diese für *Seitenkanalangriffe* verwendet werden können. Intensive Forschung auf diesem Gebiet hat neben Gegenmaßnahmen auch neue *Angriffsvektoren* hervorgebracht. Die Künstliche Intelligenz (KI) spielt auch in der Kryptografie

eine wichtige Rolle, und zwar in der Seitenkanalanalyse, also der Analyse auf Anfälligkeit für *Seitenkanalangriffe*, und als Werkzeug in der mathematischen Kryptoanalyse (vgl. Kapitel *Kryptografie*, Seite 75).

Eine wesentliche Voraussetzung für den sicheren Einsatz von Kryptografie ist die Erzeugung von Zufallszahlen, die gewisse Gütekriterien erfüllen. Zufallszahlen werden in der Kryptografie unter anderem für die Erzeugung kryptografischer Schlüssel benötigt. Wie der Name schon sagt, dürfen sie nicht vorhersagbar sein. Je stärker die Zufallszahlen sind, desto schwieriger ist es, sie für Angriffe auszunutzen. Um dieser Ausnutzung vorzubeugen, definiert das BSI in den Anwendungshinweisen und Interpretationen zum Schema AIS 20 und AIS 31 Funktionalitätsklassen von Zufallszahlengeneratoren für verschiedene Einsatzzwecke. Zudem hat das BSI aktiv an der Entwicklung des Standards ISO/IEC 20543:2019 zur Evaluierung von Zufallszahlengeneratoren mitgewirkt, der im Oktober 2019 in Kraft getreten ist.

Positiv hervorzuheben ist, dass mittlerweile viele Produkte über einen nach dem deutschen Common-Criteria-Schema (vgl. Kapitel *Zertifizierung*, Seite 60) zertifizierten physikalischen Zufallszahlengenerator verfügen. Aufgrund der effizienteren Ausnutzung von Halbleiterprodukten und der immer größeren Leistungsfähigkeit bei geringem Stromverbrauch verfügen neuere Produkte zudem über eine integrierte kryptografische Nachbearbeitung der Zufallszahlen. Diese verringert die bereits sehr geringe Wahrscheinlichkeit, dass die bereits sehr kleinen verbleibenden Schwächen physikalischer Rauschquellen ausgenutzt werden können, und verhindert sie vollends.

Die Sicherheitsgarantien der heute eingesetzten kryptografischen Mechanismen gelten allerdings nicht mehr, sobald ein hinreichend leistungsstarker Quantencomputer zur Verfügung steht. Das Kapitel *Kryptografie* (vgl. Kapitel *Kryptografie*, Seite 75) zeigt Möglichkeiten auf, dieser Bedrohung zu begegnen, und stellt die Aktivitäten des BSI in diesem Bereich dar.



Kollisionsangriffe gegen die Hashfunktion SHA-1

Kryptografische Hashfunktionen bilden Nachrichten beliebiger Länge auf Hashwerte fester Länge ab und werden unter anderem zur Integritätssicherung eingesetzt. Eine wichtige Sicherheitseigenschaft, die von einer kryptografischen Hashfunktion erfüllt werden muss, ist die Kollisionsresistenz. Das ist dann der Fall, wenn es praktisch unmöglich ist, eine Kollision, d. h. zwei unterschiedliche Nachrichten mit identischem Hashwert, zu finden.

Die Kollisionsresistenz der weit verbreiteten Hashfunktion SHA-1 (Secure Hash Algorithm 1) wurde bereits im Jahr 2005 von den Forschern Xiaoyun Wang, Yiqun Lisa Yin und Hongbo Yu theoretisch widerlegt (X. Wang, Y.L. Yin, H. Yu: Finding Collisions in the Full SHA-1). Die erste Kollision wurde von einem Forscherteam um Marc Stevens praktisch berechnet und im Februar 2017 veröffentlicht (vgl. *Quellenverzeichnis*¹⁷: <https://shattered.io>). Im aktuellen Berichtszeitraum wurden die bekannten Kollisionsangriffe gegen SHA-1 weiter verbessert. Im Januar 2020 wurde von den Forschern Gaëtan Leurent und Thomas Peyrin die erste sogenannte Chosen-Prefix-Kollision von SHA-1 veröffentlicht (vgl. *Quellenverzeichnis*¹⁸: <https://sha-mbles.github.io>). Die Nachrichten einer Chosen-Prefix-Kollision enthalten nicht mehr wie zuvor ein identisches, vorab gewähltes Anfangssegment, sondern zwei verschiedene vorab gewählte Anfangssegmente. Diese höhere Flexibilität ermöglicht neue Angriffsszenarien.

Darüber hinaus konnten die Forscher den Rechenaufwand für Kollisionsangriffe gegen SHA-1 ungefähr auf ein Zehntel reduzieren. Auch wurden die Kosten für die Erzeugung einer Kollision oder Chosen-Prefix-Kollision von SHA-1 mit gemieteter Hardware nach Einschätzung der Forscher stark reduziert.

Für den allgemeinen Anwendungsfall wird die Hashfunktion SHA-1 vom BSI schon seit vielen Jahren nicht mehr empfohlen. Gegen eine Verwendung in Konstruktionen, die keine Kollisionsresistenz benötigen (z. B. bei einem der bekanntesten und wichtigsten Anwendungsfällen von SHA-1, dem Hash-based Message Authentication Code, kurz HMAC), bestehen aber aus sicherheitstechnischer Sicht nach gegenwärtigem Kenntnisstand keine Einwände. Dennoch wird empfohlen, auch in diesen Anwendungen als grundsätzliche Sicherungsmaßnahme eine Hashfunktion der SHA-2- oder SHA-3-Familie einzusetzen.



Laufzeitangriffe gegen das Signaturverfahren ECDSA

Bei einem Laufzeitangriff nutzt der Angreifer die Rechenzeit einer kryptografischen Implementierung als Seitenkanalinformation. So kann bei ungeschützten Implementierungen die Laufzeit Rückschlüsse auf verarbeitete Geheimnisse (z. B. geheime Schlüssel) zulassen.

Im Berichtszeitraum haben zwei Forscherteams Untersuchungen zu Laufzeitangriffen gegen das Signaturverfahren ECDSA (Elliptic Curve Digital Signature Algorithm) durchgeführt, die unter den Bezeichnungen Minerva (vgl. *Quellenverzeichnis*¹⁹: <https://minerva.crocs.fi.muni.cz>) und TPM-Fail (vgl. *Quellenverzeichnis*²⁰: <https://tpm.fail>) veröffentlicht wurden. Bei Minerva wurden ECDSA-Implementierungen von Smartcards und Software-Kryptobibliotheken betrachtet, bei TPM-Fail wurden Sicherheitselemente für Computer, sogenannte Trusted Platform Modules (TPMs) untersucht.

Die Grundidee der Angriffe ist bereits seit 1999 bekannt. Zunächst wird die Erzeugung mehrerer Signaturen angestoßen. Dabei werden die jeweils für eine Signaturerstellung benötigten Laufzeiten gemessen. Im Anschluss werden die einzelnen Informationen mit Hilfe eines mathematischen Verfahrens zusammengeführt, wodurch der geheime Signaturschlüssel berechnet werden kann. Der Signaturschlüssel ermöglicht es dem Angreifer, Signaturen des Opfers zu fälschen.

Es sind verschiedene Gegenmaßnahmen bekannt, die Laufzeitangriffe gegen ECDSA-Implementierungen effektiv verhindern. Als Teil der AIS 46 veröffentlicht das BSI Leitfäden zur Evaluierung und Zertifizierung von Implementierungen bezüglich ihrer Widerstandsfähigkeit gegen *Seitenkanalangriffe*.

1.7 Hybride Bedrohungen

Hybride Bedrohungen und deren Abwehr gewinnen sowohl im nationalen als auch internationalen Kontext stetig an Relevanz. Staatliche aber auch nichtstaatliche Akteure greifen vermehrt auf hybride Methoden und Ansätze zurück, um destabilisierenden Einfluss auf Staaten auszuüben.

Hierzu bedienen sie sich typischerweise verschiedenster Werkzeuge, wie beispielsweise Cyber-Angriffe, verdeckte militärische Operationen, wirtschaftlicher Druck oder Desinformation, die in mehreren Domänen Wirkung entfalten und sich gegenseitig begünstigen können. Dies geschieht oft unter Verschleierung der Absichten und Urheberchaft bzw. gezielt unterhalb der Schwelle bestehender rechtsstaatlicher Interventionsmöglichkeiten.

Die weltweit fortschreitende Digitalisierung ist ein entscheidender Treiber der Dynamik hybrider Bedrohungen, da sich neue potenzielle Verwundbarkeiten von Staat, Wirtschaft und Gesellschaft eröffnen. Der Dimension Cyber kommt deshalb in der Zusammensetzung hybrider Kampagnen eine herausgehobene Stellung zu. Zusätzlich hat sie eine besondere Querschnittsfunktion, da auch Maßnahmen in anderen Dimensionen oftmals von ihr abhängen. In einer hybriden Kampagne können je nach individueller Ausprägung die physische (z. B. Hardware und *Firmware*), die logische (z. B. Virtualisierungen und Betriebssysteme) und die informationelle

(z. B. Anwendungen und Daten) Schicht des Cyberspace durch einen Aggressor genutzt werden.

Im Berichtszeitraum zeigte auch die COVID-19-Pandemie zu Beginn des Jahres 2020, wie Akteure versuchen, mittels Desinformation, die auch ein hybrides Mittel sein kann, Einfluss auf andere Staaten auszuüben. Es wird davon ausgegangen, dass bestehende Ängste und Unsicherheiten innerhalb der Bevölkerung der Zielstaaten ausgenutzt werden sollten, um durch gezielte Desinformation das Vertrauen der Bevölkerung in die nationalen Systeme und die demokratischen Institutionen zu schwächen.

In zunehmendem Maße stützen sich Desinformationen auf technische Hilfsmittel, die der Manipulation authentischer Informationen dienen. Beispiele dafür sind das Verfälschen von Foto-, Video- und Tonaufnahmen sowie das Vortäuschen einer bestimmten Urheberchaft einer Informationsübermittlung (z. B. einer E-Mail oder eines Beitrags in Sozialen Netzwerken). Solche technischen Manipulationen hinterlassen oftmals Spuren, bei deren Identifizierung das BSI mit seiner technischen Expertise unterstützen kann. Darüber hinaus unterstützt das BSI unter anderem die Betreiber kritischer Infrastrukturen, die IT-Sicherheit im Rahmen von Wahlen, steht im Austausch mit den Betreibern Sozialer Netzwerke, z. B. im Rahmen einer Initiative zur Entwicklung von Sicherheitsempfehlungen, und sensibilisiert mit seinen Angeboten die Bevölkerung in Fragen der IT-Sicherheit.

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

Aufgrund der hochvernetzten globalen Beziehungen in Wirtschaft, Staat und Gesellschaft hat die COVID-19-Pandemie umfassende Auswirkungen auf nahezu jeden Lebensbereich. Dies gilt auch für die digitale Welt, die mittlerweile oftmals einen zentralen Baustein für das Aufrechterhalten der notwendigsten Grundversorgung der Bevölkerung bildet, aber auch für die Bekämpfung der Pandemie selbst. So stellen digitale Systeme beispielsweise den essenziellen Informationsaustausch von Forschern zur Bekämpfung der Pandemie, die Lieferketten für lebenswichtige Güter und die Arbeitsgrundlagen für unzählige Unternehmen sicher. Vor diesem Hintergrund könnte ein erfolgreicher Cyber-Angriff zum Beispiel auf eine für die Bewältigung der Pandemie relevante Organisation massive Konsequenzen haben, sowohl für jeden Einzelnen, als auch für die Eindämmung der Pandemie und ihrer gesamtgesellschaftlichen Folgen.

Social-Engineering-Angriffe unter Ausnutzung der COVID-19-Pandemie

Zu *Social-Engineering*-Angriffen zählen Betrugs- und Manipulationsversuche, die unter Vorspiegelung falscher Tatsachen und unter Ausnutzung von menschlichen Reaktionen wie Angst oder Hilfsbereitschaft Opfer dazu verleiten, sich selbstschädigend zu verhalten; beispielsweise durch den Klick auf einen Link, der ein Schadprogramm installiert (vgl. Kapitel *Diebstahl und Missbrauch von Identitätsdaten*, Seite 18). Angreifer, die sich solcher Methoden bedienen, reagieren in der Regel schnell auf medienrelevante, öffentlichkeitswirksame Themen und passen ihre Angriffskampagnen entsprechend an. So beobachtete das BSI auch im Zuge der COVID-19-Pandemie unterschiedliche Kampagnen, die sich die komplexe Gesamtsituation rund um COVID-19 zunutze machten. Hierzu zählen beispielsweise *Phishing*- und Schadprogramm-Kampagnen, *CEO-Fraud*, und Betrugsversuche mit IT-Mitteln, auch allgemein Scam genannt. Die von Ängsten, Sorgen und Unsicherheit geprägte Stimmung in weiten Teilen der Bevölkerung kann die Erfolgsaussichten solcher Angriffe zwar begünstigen, unerwartet große Häufungen traten jedoch nicht auf.

IT-Sicherheit unter erschwerten Bedingungen

Unter normalen Umständen ergibt sich aus den in Organisationen umgesetzten IT-Sicherheitsmaßnahmen, der lokalen Verfügbarkeit von IT-Fachpersonal und Dienstleistern sowie finanziellen und infrastrukturellen Sicherheitsvorkehrungen eine vielschichtige

Abwehr- und Reaktionsstruktur. Die häufig erforderliche Verlagerung von Beschäftigten und Geschäftsprozessen ins Home-Office bringt die Gefahr mit sich, dass die IT-Sicherheit zugunsten eines ad hoc funktionierenden Home-Office vernachlässigt wird. Außerdem wurde die Verfügbarkeit und Einsatzfähigkeit von IT-Fachpersonal und IT-Sicherheitsdienstleistern durch die erforderlichen Beschränkungen erschwert.

Digitalisierungsschub vergrößert Angriffsfläche

Ausgangsbeschränkungen, Schul- und Geschäftsschließungen, Abstandsregeln – die politischen Maßnahmen gegen die COVID-19-Pandemie führten zu weitreichenden Einschränkungen der alltäglichen Lebensführung. In vielen Fällen waren digitale Lösungen das Mittel der Wahl, um elementare Geschäftsprozesse und zwischenmenschliche Beziehungen aufrecht erhalten zu können. Arbeiten im Home-Office, Online-Unterricht, Einkäufen im Internet und der Video-Chat mit Freunden und Verwandten führten zu einer beispiellosen Welle der Digitalisierung vieler Lebensbereiche. Die umfassende, plötzliche Mehrnutzung von Digitalisierungsprodukten eröffnete Angreifern eine stark vergrößerte Angriffsfläche für ihre kriminellen Aktivitäten.

Nutzung unsicherer oder nicht ausreichend datenschutzkonformer Lösungen

In den Sektoren Bildung, Medizin, Verwaltung und generell bei der Nutzung von Heimarbeitsplätzen wurden schlagartig Kommunikationsplattformen, VPN, Chats sowie Videokonferenzen etabliert. Insbesondere in der privaten Nutzung wurde auf die schon bekannten und gewohnten Messenger sowie sozialen Netzwerke im verstärkten Maße zurückgegriffen. Hingegen wurden im beruflichen Umfeld VPN-Lösungen, Team-Lösungen sowie Software für Videokonferenzen usw. nachgefragt.

Bewertungen

Aus Sicherheitsgründen ist der Einsatz einer VPN-Lösung für den Zugriff auf berufliche Dokumente anderen Lösungen wie Dateiversand und öffentlichen Cloud-Diensten vorzuziehen. Auch in einer Krisensituation sollten wichtige Überlegungen zur Sicherheit und Datenschutz wie in der Datenschutzgrundverordnung (DSGVO) zusammengefasst nicht ignoriert werden. Sofern Cloud-Dienste zum Betrieb der Anwendungen erforderlich sind, ist aus Gründen der Sicherheit zu erwägen, ob eine Datenhaltung innerhalb einer privaten Cloud eingerichtet werden kann.



COVID-19 Soforthilfe-Maßnahmen durch Cyber-Kriminelle missbraucht

Sachverhalt

Nahezu unmittelbar nach Bekanntgabe und Umsetzung der finanziellen Soforthilfe-Maßnahmen auf Bundes- und Länderebene Ende März 2020 wurden *Phishing*-Kampagnen beobachtet, die versuchten, diese Maßnahmen auszunutzen. Betrüger registrierten dafür *Phishing*-Domains und gestalteten die darunter erreichbaren Webseiten teilweise identisch zu den offiziellen Soforthilfe-Seiten. Anschließend wurden diese Seiten mit unterschiedlichen Mitteln wie *Spam*-E-Mails oder Platzierungen in Suchmaschinen in Umlauf gebracht. Es ist davon auszugehen, dass das grundlegende Ziel dieser *Phishing*-Versuche die Sammlung von Informationen über finanziell notleidende Unternehmen und Privatpersonen war. Diese Informationen konnten die Angreifer anschließend verwenden, um bei den offiziellen Soforthilfe-Stellen Zahlungen im Namen der Opfer abzurufen, wodurch dem eigentlich berechtigten Antragssteller etwaige Hilfeleistungen zumindest vorübergehend verwehrt wurden und dem Staat erheblicher Schaden entstanden ist. Langfristig ist auch die Verwendung der durch das *Phishing* gewonnenen Informationen für Folgeangriffe auf die Opfer nicht auszuschließen.

Phishing-Angriffe im Kontext finanzieller Unterstützungsleistungen waren allerdings nicht allein auf Deutschland beschränkt. Auch in anderen Staaten, die vergleichbare finanzielle Soforthilfe-Maßnahmen aufgesetzt hatten, konnten derartige Angriffsversuche beobachtet werden.

Reaktion

Um zu verhindern, dass Cyber-Kriminelle die amtlichen Soforthilfe-Seiten mit den erbeuteten Identitätsdaten missbrauchen, wurden einige Soforthilfe-Seiten vorübergehend vom Netz genommen und in der Folge auch einige Auszahlungen zwischenzeitlich ausgesetzt. Nach einer Überarbeitung und Überprüfung der betroffenen Prozesse wurde die Antragsstellung über die amtlichen Webseiten sowie die Auszahlungen wieder aufgenommen. Die zuständigen Polizeien der Länder ermitteln.

Identifizierte betrügerische Webauftritte wurden im Rahmen der Ermittlungen vom Netz genommen. Das BSI hat die Ermittlungsbehörden bei der Abschaltung betrügerischer Webseiten mit Bezug zu COVID-19 unterstützt. Mehrere offizielle Stellen der Länder und des Bundes so auch das BSI warnten öffentlich vor diesen Betrugsversuchen.

Empfehlung

Um sich vor *Phishing*- und ähnlichen Betrugs-Kampagnen zu schützen, ist bei E-Mails, Telefonaten und Webseiten, die personenbezogene Daten abfragen, besondere Vorsicht geboten. Die Authentizität des Absenders einer E-Mail sollte im Zweifel telefonisch überprüft werden.

1.9 Zusammenfassung und Bewertung der Gefährdungslage

Die Lage der IT-Sicherheit in Deutschland bleibt im Berichtszeitraum angespannt. Angreifer nutzten Schadprogramme für cyber-kriminelle Massenangriffe auf Privatpersonen, Unternehmen, Behörden und andere Institutionen, aber auch für gezielte Angriffe auf ausgewählte Opfer. Zugleich hat die Bedrohung durch Daten-Leaks mit der Offenlegung von Millionen von Patientendatensätzen im Internet eine neue Qualität erreicht. Im Berichtszeitraum traten, wie in den vorangegangenen Kapiteln dargestellt, zudem mehrere, teils kritische Schwachstellen in Software-Produkten auf, die Angreifer für Schadprogramm-Angriffe oder Datendiebstahl ausnutzen konnten.

Dabei nutzten die Angreifer auch verstärkt den Faktor „Mensch“ als Einfallstor für Angriffe, die mit *Social-Engineering*-Methoden arbeiten und gleichsam als Türöffner für weitere Angriffe dienen.

Nachstehend noch einmal zusammenfassend einige herausgehobene Beispiele aus dem Berichtszeitraum:

- **Neue Schadprogramm-Welle im Herbst und Winter: Emotet dominiert die Lage**
Dominiert wurde die Lage durch das Schadprogramm Emotet, das sich schon im vergangenen Berichtszeitraum als besonders gefährlich erwiesen hatte. Es ermöglicht eine Kaskade weiterer Schadsoftware-Angriffe bis hin zu gezielten *Ransomware*-

- Angriffen auf ausgewählte, zahlungskräftige Opfer. Insgesamt war das Aufkommen neuer Schadprogramm-Varianten im Herbst und Winter überdurchschnittlich hoch (der Tageszuwachs lag zeitweise bei knapp 470.000 Varianten).
- **Cyber-Kriminelle kommunizieren verschlüsselt**
Das Hypertext Transfer Protocol Secure (HTTPS) steht für sichere, verschlüsselte Datenübertragung im Internet. Im Berichtszeitraum hat sich jedoch der Trend zur Nutzung von HTTPS-Seiten durch Cyber-Kriminelle verstärkt. Wie das BSI in Zusammenarbeit mit der Verbraucherzentrale NRW herausfand, führt inzwischen mehr als jeder zweite Link in einer *Phishing*-E-Mail auf eine HTTPS-Webseite (60 %), die im Gegensatz zu einfachen HTTP-Webseiten besonders seriös und sicher erscheinen, tatsächlich aber betrügerischen Zwecken dienen.
 - **Millionen Patientendaten im Internet öffentlich zugänglich**
Meldungen zu Diebstählen von Kundendaten wurden im Berichtszeitraum erneut regelmäßig beobachtet. Aber nicht nur Diebstahl führte zum Datenabfluss. Im Berichtszeitraum wurden auch Datenbanken mit hochsensiblen medizinischen Daten frei zugänglich im Internet entdeckt. Anders als bei Datendiebstählen war hier also kein technisch aufwändiger Angriff notwendig, sondern unzureichend gesicherte oder falsch konfigurierten Datenbanken Ursache für den Datenabfluss. Allein in Deutschland waren zwischen Juli und September 2019 etwa 15.000 Datensätze von Bundesbürgerinnen und Bundesbürgern mit insgesamt mehreren Millionen Bildern frei im Internet verfügbar.
 - **Kritische Schwachstellen in Remote-Zugängen**
Im Berichtszeitraum sind mehrere kritische Schwachstellen aufgetreten. Die neuen Schwachstellen BlueKeep und DejaBlue in Windows' Remote Desktop Protocol machen viele Windows-Systeme bis hin zu Windows 10 angreifbar. Durch die Schwachstellen können Angreifer einen beliebigen Code – auch Schadprogramme – auf den angreifbaren Systemen ausführen. Die Schwachstellen ermöglichen Schadprogrammen außerdem, sich automatisiert weiterzuverbreiten, und werden daher auch als „wurmfähig“ bezeichnet. Microsoft hat Sicherheitsupdates für alle betroffenen Systeme bereitgestellt.
 - **Neue APT-Gruppen**
Im Zusammenhang mit *Advanced Persistent Threats* waren im Berichtszeitraum in Deutschland etwas mehr als ein Dutzend Gruppen aktiv. Weltweit lag die Anzahl im dreistelligen Bereich. Immer mehr Staaten haben inzwischen öffentlich bekannt gegeben, Cyber-Fähigkeiten zu entwickeln, sodass die Zahl der aktiven APT-Gruppen weltweit künftig weiter ansteigen dürfte. Im Gegensatz zu anderen Angreifern verfolgen APT-Gruppen in der Regel keine cyber-kriminellen Ziele, sondern taktische und strategische Absichten wie Spionage oder Sabotage.
 - **Distributed-Denial-of-Service-Angriffe (DDoS-Angriffe) mit intelligenten Strategien**
DDoS-Angreifer setzten im Berichtszeitraum vermehrt auf technisch hoch entwickelte und strategisch intelligente Angriffe. So konnte insbesondere beobachtet werden, dass Angreifer öffentlich verfügbare Informationen, wie etwa Störungsmeldungen, nutzten, um während eines Angriffs die Abwehrmaßnahmen des Opfers zu beobachten und ihre Angriffsstrategien ad hoc flexibel anzupassen.
 - **Social-Engineering-Angriffe unter Ausnutzung der COVID-19-Pandemie**
Cyber-Kriminelle, die sich auf Betrug im Internet spezialisiert haben, reagieren in der Regel schnell auf gesellschaftlich relevante Themen und Trends, um diese für Kampagnen auszunutzen. Im Zuge der COVID-19-Pandemie wurden beispielsweise *Phishing*-Kampagnen, *CEO-Fraud* und Betrugsversuche mit IT-Mitteln beobachtet. So gelang es Betrügern beispielsweise, Soforthilfe-Maßnahmen zu missbrauchen, indem sie die Antragswebseiten amtlicher Stellen täuschend echt nachahmten. Die unternehmensbezogenen Daten, die die Antragsteller auf den gefälschten Seiten eingegeben hatten, nutzten die Cyber-Kriminellen anschließend, um sich als Antragsteller auszugeben und Hilfgelder missbräuchlich zu beantragen.

Cyber-Sicherheitslage für Deutschland 2020

Aktion und Reaktion

117,4 MIO.

neue Schadprogramm-Varianten



2019:

114 MIO.

durchschnittlich

322.000

neue

Schadprogramm-Varianten pro Tag

in Spitzenwerten

470.000

76%
 ist der Anteil unerwünschter SPAM-MAILS an allen in den Netzen des Bundes eingegangenen Mails
 ▶ 2019: 69% ◀

24,3 MIO.

Patientendatensätze

waren Schätzungen zufolge international frei im Internet zugänglich

täglich
 bis zu **20.000**
 BOT-INFEKTIONEN deutscher Systeme

419

KRITIS-Meldungen

▶ 2019: 252

▶ 2018: 145

52.000
W E B S E I T E N

wurden wegen enthaltener Schadprogramme durch die Webfilter der Regierungsnetze gesperrt

35.000

Mails mit Schadprogrammen wurden durchschnittlich pro Monat in deutschen Regierungsnetzen abgefangen

109.000

Abonnenten Bürger-CERT

▶ 2019 : 105.000

▶ 2018 : 100.000

rund **100**

Produkte und Standorte hat das BSI im Bereich Common Criteria zertifiziert

mehr als **4.400**

Mitglieder der Allianz für Cyber-Sicherheit

▶ 2019 : 3.700

▶ 2018 : 2.700

rund **1.700**

registrierte **KRITIS-Anlagen**

knapp

7 MIO.

Meldungen zu **Schadprogramm-INFEKTIONEN**

übermittelte das BSI an deutsche Netzbetreiber

2 Zielgruppenspezifische Erkenntnisse und Lösungen



2 Zielgruppenspezifische Erkenntnisse und Lösungen

Fragen der Informationssicherheit sind für alle gesellschaftlichen Belange von großer Bedeutung. Das erklärt die Vielfalt von Aufgaben, mit denen sich das BSI beschäftigt. Das BSI informiert und berät Bevölkerung, Wirtschaft sowie Politik, tauscht sich mit der Wissenschaft aus und unterstützt den gesamtgesellschaftlichen Austausch zu Fragen der Informationssicherheit. So sammelt und erhebt das BSI umfangreiche Daten zur Lage der IT-Sicherheit in Deutschland, die durch hauseigene Experten unterschiedlicher Fachgebiete analysiert werden. Aus den Ergebnissen werden Schutzmaßnahmen und Lösungen für alle Gefährdungslagen im digitalen Zeitalter entwickelt – vom Verbraucherprodukt über die Kritischen Infrastrukturen im öffentlichen Raum bis hin zu Regierungsnetzen. Je nach Zielgruppe steht das BSI dabei unterschiedlichen Herausforderungen gegenüber, mit jeweils eigenen Antworten.

2.1 Gesellschaft

Online-Shopping, *Wearables*⁴ sowie neue Bezahl- und Identifikationsverfahren: Die Digitalisierung prägt den Alltag der Bevölkerung. Doch mit ihr gehen auch zahlreiche Risiken und Gefahren einher. Laut dem Digitalbarometer 2020⁵ war bereits jeder Vierte Opfer von Kriminalität im Internet. Das BSI setzt sich daher in vielfältiger Weise für mehr Schutz der Verbraucherinnen und Verbraucher in der digitalen Welt ein. Informationsangebote, Veranstaltungen und Warnmeldungen zu kritischen Produkten und Angeboten zählen ebenso zu den Leistungen des BSI wie der gesamtgesellschaftliche Dialog zur Informationssicherheit. Dabei sucht das BSI den Austausch mit Bürgerinnen und Bürgern sowie mit Wissenschaft, Politik und Wirtschaft gleichermaßen, um auch die Entwicklung des digitalen Verbraucherschutzes voranzutreiben.

2.1.1 Erkenntnisse aus Umfragen zum Bild der Gefährdungslage in der Gesellschaft

Um Aussagen über die Gefährdungslage der IT-Sicherheit für die Gesellschaft zu treffen, arbeitet das BSI mit unterschiedlichen Behörden, Institutionen und Organisationen zusammen. Im Rahmen dieser Kooperationen werden Befragungen und Studien durchgeführt, deren Ergebnisse ein deutliches Abbild der Lage zeichnen.

Ergebnisse und Erkenntnisse aus dem Digitalbarometer 2020
Das BSI und die Polizeiliche Kriminalprävention der Länder

und des Bundes (ProPK) kooperieren, um Bürgerinnen und Bürger umfassend über die Risiken und die Schutzmöglichkeiten im Internet aufzuklären. Grundlage dieser Arbeit ist das Digitalbarometer, eine gemeinsame, repräsentative Online-Befragung. In dieser wird erhoben, welche Bedeutung Sicherheit im Internet bei Privatanwenderinnen und -anwendern hat, wie sie sich über Schwachstellen und Risiken informieren und inwiefern sie sich vor den Gefahren der digitalen Welt schützen.

Jeder Vierte ist Opfer

Die generelle Betroffenheit bei Bürgerinnen und Bürgern bleibt konstant: Jeder Vierte war bereits Opfer von Kriminalität im Internet, 25 Prozent von ihnen in den letzten 12 Monaten. Dabei sind den Betroffenen vor allem Betrug beim Online-Shopping (44 %) und der Fremdzugriff auf einen Online-Account (30 %) widerfahren. Die Schutzmaßnahmen bleiben weiterhin ausbaufähig. Zwar sind beispielsweise Antivirenprogramme (57 %) und sichere Passwörter (48 %) verbreitet, werden aber längst nicht umfassend eingesetzt. Zudem nutzt nur ein Viertel der Befragten automatische Updates und etwa ein Drittel eine *Zwei-Faktor-Authentisierung* (siehe Kapitel *Zwei-Faktor-Authentisierung*, Seite 47).

Sicherheitsempfehlungen direkt umsetzen zahlt sich aus

Knapp über die Hälfte der Befragten kennt die aktuellen Sicherheitsempfehlungen zum Schutz vor Kriminalität im Internet. Umgesetzt werden diese in den meisten Fällen, wenn es gerade passt (41 %) oder auch direkt, nachdem eine Empfehlung zur Kenntnis genommen wurde (39 %). Auffallend ist, dass Menschen, die bereits mehrfach Opfer waren, häufiger die Sicherheitsempfehlungen erst im Problemfall umsetzen (33 %), obwohl sie diese vorab schon kannten.

Der größte Teil der Befragten informiert sich hin und wieder über Internetsicherheit (37 %), jeder Vierte nie. Besonders wichtig ist den Befragten die Sicherheit beim Online-Banking (60 %) und Online-Shopping (40 %). Etwa jeder vierte Befragte erhält die Sicherheitsempfehlungen durch das BSI und kennt die Webseite von „BSI für Bürger“ (27 %).

Wunsch nach Orientierung für den Notfall

Die Gruppe mit dem größten Anteil (36 %) hat sich nach einer Straftat selbst geholfen. Das entspricht auch dem Wunsch nach Informationen: Mehr als die Hälfte der Betroffenen halten eine Checkliste für

⁴Intelligente elektronische Geräte die am Körper getragen werden, wie z. B. Fitness-Tracker in Form von Armbändern oder Smart watches, digitale Brillen u. ä.

⁵Bürgerbefragung zur Cyber-Sicherheit von BSI und der Polizeilichen Kriminalprävention der Länder und des Bundes

den Notfall für hilfreich. Zudem wünschen sich die Befragten in Zukunft verstärkt mehr Hinweise, wie sie Kriminalität im Internet erkennen können (58 %) und was man als Opfer tun kann (46 %). ProPK und BSI haben auf diese Bedürfnisse bereits reagiert und eine Checklisten-Reihe ins Leben gerufen, die auf den jeweiligen Webseiten zum Download zur Verfügung steht (vgl. *Quellenverzeichnis*²¹: www.bsi-fuer-buerger.de). Diese wird kontinuierlich erweitert.

Ergebnisse und Erkenntnisse aus einem Projekt zum Schutz von Online-Konten

Die Entwicklung wirksamer Schutzmaßnahmen von Online-Konten für Bürgerinnen und Bürger ist Ziel eines gemeinsamen Projektes, das das BSI gemeinsam mit dem Bundeskanzleramt im Juli 2019 begonnen hat. Die erste Phase des Projekts verfolgte das Ziel, Erkenntnisse zum Umgang mit Passwörtern, zu Handlungsbarrieren und Risikowahrnehmung zu gewinnen sowie zu erfahren, auf welchen Wegen Anwenderinnen und Anwender zu diesen Themen informiert und aufgeklärt werden möchten.

Aus zehn Gruppendiskussionen mit insgesamt 100 Teilnehmerinnen und Teilnehmern, aufgeteilt in fünf Altersgruppen und nach Geschlecht, erhielt das Projektteam erste Einblicke und Anhaltspunkte zu diesen Themenfeldern. Diese flossen in den Fragebogen einer repräsentativen Online-Befragung ein (n=995, 16 Jahre und älter, Durchführungszeitraum: 26. Oktober bis 3. November 2019). Die in der Folge dargestellten Erkenntnisse zum Schutz von Online-Konten bei Privatanwenderinnen und -anwendern basieren auf diesen beiden Befragungen.

Risikowahrnehmung

Im Durchschnitt wird die Gefahr, dass Datendiebe an Passwörter gelangen könnten, als mittelhoch betrachtet (Mittelwert=2,9 auf einer Skala von 1=sehr gering bis 5=sehr hoch). Dabei halten es die Befragten für am wahrscheinlichsten, dass Hacker über Datendiebstähle bei Unternehmen an ihre Passwörter gelangen könnten (Mittelwert=3,3 auf einer Skala von 1=überhaupt nicht wahrscheinlich bis 5=sehr wahrscheinlich). Sie glauben eher nicht, dass sie sich selbst durch Passwörter wirksam vor Hackern schützen können. Gleichzeitig wissen sie eher nicht, ab wann ein Passwort nicht mehr von Hackern geknackt werden kann.

Umgang mit Passwörtern und verfügbarer Technik

Gerade die Anzahl an Passwörtern, die in verschiedenen Kontexten, ob zu Hause oder unterwegs, abrufbar sein müssen, stellt für die Befragten eine Herausforderung dar. Knapp vier Fünftel der Befragten (78 %) nutzen bis zu 20 Online-Accounts, die mit einem Passwort geschützt werden müssen. Dem begegnen

drei Viertel der Befragten (74 %) mit dem Ansatz, sich Passwörter selber zu merken. Rund ein Drittel (34 %) notiert sich Passwörter auf Papier, 15 % speichern sie in einem Passwortmanager (Mehrfachnennungen waren möglich).

Zwei Drittel der Befragten (67 %) geben an, dass sie völlig unterschiedliche Passwörter vergeben. Auf eine eigene Regel, nach der Passwörter erstellt werden, greifen 10 Prozent der Befragten zurück, 6 Prozent von ihnen verfolgen die Strategie, aus einem willkürlich gebildeten Satz ein Passwort aus den Anfangsbuchstaben abzuleiten.

Von den 39 Prozent der Befragten, die Passwortmanager kennen, setzt letztlich nur knapp ein Drittel (27 %) derartige technische Hilfsmittel ein, um starke Passwörter zu erstellen und sich bei Online-Accounts anzumelden. Hauptgrund für die Nichtnutzung solcher Software sind Vorbehalte (67 %). Besonders stark wiegt dabei die Sorge, dass ein Hacker mit einem Schlag an alle verwendeten Passwörter gelangen könnte (78 %), ebenfalls verbreitet ist eine Skepsis gegenüber der Seriosität von Anbietern solcher Programme (58 %, Mehrfachnennungen möglich).

Informationsbedarf

Zwei Drittel der Befragten wünschen sich mehr Informationen, wie sie sich vor Datendiebstahl schützen können (66 %). Praktische Tipps, wie man bei sehr vielen Konten seine Passwörter sicher handhabt, stehen dabei im Mittelpunkt des Informationsinteresses (59 %), gefolgt von Empfehlungen, welche Software zum Schutz der eigenen Online-Konten geeignet ist (52 %), und Informationen über die Vor- und Nachteile von Passwortmanagern (49 %, Mehrfachnennungen möglich).

Ein ausführlicher Zwischenbericht mit weiteren Informationen zu den Befragungen und ihren Ergebnissen ist unter www.bundesregierung.de (vgl. *Quellenverzeichnis*²²: www.bundesregierung.de) abrufbar.

2.1.2 Digitaler Verbraucherschutz

Nicht nur die zahlreichen Fälle von Identitätsdiebstahl im aktuellen Berichtszeitraum zeigen: In unserem zunehmend digitalen Alltag sind wir als Verbraucherinnen und Verbraucher permanent Gefahren und Risiken ausgesetzt. Durch die Aktivitäten des BSI werden Bürgerinnen und Bürger in der digitalen Welt besser für diese Cyber-Gefahren sensibilisiert und damit die Widerstandsfähigkeit der Gesellschaft erhöht. Das BSI arbeitet für die Verbraucherinnen und Verbraucher insbesondere daran, ihr Risiko-

bewusstsein zu erhöhen, ihre Beurteilungsfähigkeit zu steigern und ihre Lösungskompetenz zu stärken.

Digitalen Verbraucherschutz vorantreiben

Mit der Einrichtung eines eigenen Organisationsbereichs am neuen Standort Freital intensiviert das BSI seine Arbeit im digitalen Verbraucherschutz. Expertinnen und Experten werden sich hier unter anderem damit beschäftigen, wie der staatliche Rahmen für Cyber-Sicherheit verbraucherfreundlich gestaltet, sichere Verbraucherprodukte und -dienste angeboten und Anliegen der Verbraucherinnen und Verbraucher zu Themen der Cyber-Sicherheit serviceorientiert bearbeitet werden können.

Durch Kooperationen neue Perspektive gewinnen

Um den Verbraucherschutz wirksam zu gestalten, ist das Zusammenwirken von Staat, Wirtschaft und Gesellschaft notwendig. So hat das BSI mit der Verbraucherzentrale NRW im Jahr 2017 und dem Verbraucherzentrale Bundesverband e.V. im Jahr 2020 ein Memorandum of Understanding mit dem Ziel einer vertieften Zusammenarbeit geschlossen. Der kooperative Ansatz umfasst zudem den Austausch mit der Wissenschaft, um Perspektiven unterschiedlicher Fachdisziplinen in die Arbeit einfließen zu lassen und gemeinsam an innovativen Lösungskonzepten zu arbeiten. So veranstaltete das BSI gemeinsam mit dem Netzwerk Verbraucherforschung im September 2019 ein interdisziplinäres Verbraucherforschungsforum zum Thema *Digital Nudging*. Bei der Veranstaltung wurden Erkenntnisse aus der Verhaltensökonomik auf Fragestellungen der Informationssicherheit angewandt. Im Mittelpunkt der Diskussion stand stets das gemeinsame Ziel: die Stärkung des digitalen Verbraucherschutzes in Deutschland.

2.1.3 Das IT-Sicherheitskennzeichen – Transparenz für Verbraucherinnen und Verbraucher

Auf Grundlage der Cyber-Sicherheitsstrategie 2016 für Deutschland und aufbauend auf das sich derzeit in Abstimmung befindliche IT-Sicherheitsgesetz 2.0 plant das BSI in Zusammenarbeit mit dem Bundesministerium des Innern, für Bau und Heimat (BMI) die Einführung einer Kennzeichnung von Verbraucherprodukten.

Das IT-Sicherheitskennzeichen soll zu einer Sensibilisierung der Verbraucherinnen und Verbraucher und damit zu einem verstärkten Bewusstsein für IT-Sicherheit allgemein beitragen. Dazu sollen produktspezifische Eigenschaften der Informationssicherheit transparent dargestellt werden. Die Verbraucherinnen und Verbrau-

cher sollen somit dazu befähigt werden, vor dem Kauf eine Bewertung der Sicherheitseigenschaften von Produkten und Diensten vornehmen zu können. Dazu sollten die Anforderungsdokumente transparent und verständlich im Rahmen des Informationsangebots zum IT-Sicherheitskennzeichen erklärt werden. Der Einfluss von IT-Sicherheitsmerkmalen auf die Kaufentscheidung der Verbraucherinnen und Verbraucher soll so einen Beitrag dazu leisten, das Sicherheitsniveau für Produkte am Verbrauchermarkt signifikant zu steigern.

Mit dem IT-Sicherheitskennzeichen sollen die Hersteller von *Internet of Things (IoT, Internet der Dinge)*-Produkten für Verbraucherinnen und Verbraucher außerdem ein Instrument erhalten, um die Sicherheitsfunktionalitäten ihrer Produkte herauszustellen und dabei die Transparenz bezüglich der Informationssicherheit der gekennzeichneten Produkte für Verbraucherinnen und Verbraucher zu erhöhen. Das IT-Sicherheitskennzeichen soll dazu mit einem dynamischen Informationsangebot für Verbraucherinnen und Verbraucher verknüpft werden, welches neben der Transparenz über die Sicherheitseigenschaften auf ggf. aktuell bestehende Sicherheitsprobleme hinweist und entsprechende Lösungsmöglichkeiten des Herstellers für die Anwenderinnen und Anwender aufzeigt.

Das IT-Sicherheitskennzeichen soll für *IoT*-Produkte erteilt werden, die die Sicherheitseigenschaften nach dem aktuellen Stand der Technik für die jeweilige Produktklasse erfüllen. Dieser Stand der Technik soll in Zusammenarbeit mit den Herstellern in Anforderungsdokumenten für bestimmte Produktklassen festgelegt werden. Das können zum Beispiel TR des BSI oder vom BSI anerkannte Anforderungsdokumente (z. B. DIN-Normen, VDE⁶-Anwendungsregeln oder andere branchenspezifische Standards) sein. Nach derzeitiger Planung sollen Hersteller mit einer Erklärung über die Einhaltung dieser produktspezifischen Anforderungen informieren. Die Anforderungsdokumente sollen auch Prüfvorschriften enthalten, die vom Hersteller verpflichtend anzuwenden sind und deren Ergebnisse zu dokumentieren und als Nachweis dem BSI vorzulegen sind.

Die Anforderungsdokumente sollen dabei insbesondere *Security by Design* und *Security by Default* in der Produktentwicklung fördern und etablieren sowie die Einhaltung der allgemeinen Schutzziele der Informationssicherheit beim Produkt sicherstellen.

Mit dieser Zielsetzung in Richtung der Hersteller auf der einen und den Verbraucherinnen und Verbrauchern auf der anderen Seite soll das IT-Sicherheitskennzeichen einen essenziellen Beitrag zum digitalen Verbraucherschutz leisten. Herstellern soll damit künftig ein Rahmen zur Verfügung gestellt werden, um Sicherheitseigenschaften in

⁶Verband der Elektrotechnik, Elektronik und Informationstechnik

ihre Produkte zu implementieren und diese für Verbraucherinnen und Verbraucher transparent zu machen. Der Hersteller soll dadurch unterstützt werden, die Resilienz eines Produkts über den vollständigen Lebenszyklus des Geräts sicherzustellen. Ein wesentliches Merkmal ist dabei die unverzügliche Behebung auftretender kritischer Sicherheitslücken.

Die erste Produktklasse für das IT-Sicherheitskennzeichen sollen Breitband-Router sein, zu denen das BSI bereits im vergangenen Jahr eine Technische Richtlinie veröffentlicht hat. Die zugehörige Prüfspezifikation zum Nachweis der Erfüllung der Anforderungen steht ebenfalls kurz vor der Veröffentlichung.

2.1.4 Gesellschaftlicher Dialog für Cyber-Sicherheit

Der gesamtgesellschaftliche Dialog ist für das BSI ein zentrales Instrument, um den Austausch unterschiedlicher Perspektiven auf Informationssicherheit und so den Stellenwert des Themas in der Gesellschaft insgesamt zu fördern. Er bricht die sonst eher geschlossenen Diskursgruppen auf und ermöglicht so den gemeinsamen Austausch aller gesellschaftlichen Akteure darüber, wie eine sichere Informationsgesellschaft gestaltet werden kann. Dabei möchte das BSI vor allem den Dialog mit der organisierten Zivilgesellschaft stärken und Impulse für die eigene Arbeit aufnehmen. Als organisierte Zivilgesellschaft wird ein gesellschaftlicher Bereich zwischen dem staatlichen, dem wirtschaftlichen und dem privaten Sektor verstanden. Der Bereich umfasst die Gesamtheit des gesellschaftlichen Engagements – zum Beispiel in

Vereinen, Verbänden und anderen Formen von Initiativen und Bewegungen - und zeichnet sich dadurch aus, dass ihre Aktivitäten weder profitorientiert noch abhängig von parteipolitischen Interessen sind.

Auf Grundlage eines partizipativ ausgerichteten Multi-Stakeholder-Ansatzes, der Akteure aus den Bereichen Wissenschaft, Wirtschaft, Staat, Kultur und Medien sowie organisierte Zivilgesellschaft umfasst, wurde im Berichtszeitraum das seit Anfang 2018 laufende Projekt „Institutionalisierung des gesellschaftlichen Dialogs“ fortgeführt und inzwischen abgeschlossen. Bis Ende des Jahres 2019 arbeiteten 15 Expertinnen und Experten aus den o. g. unterschiedlichen Bereichen in Form einer Kerngruppe in verschiedenen Workshops und Arbeitstreffen zusammen, u. a. an der Institutionalisierung des gesellschaftlichen Dialogs.

Die Teilnehmerinnen und Teilnehmer des Dialogs haben ein Modell (vgl. Abbildung 5) erarbeitet, wie der vom BSI initiierte Multi-Stakeholder-Dialog künftig vertieft und verstetigt werden kann. Das Modell, das auf partizipativen Elementen beruht, beinhaltet die jährlich stattfindende Denkwerkstatt als inhaltlichen Knotenpunkt. In die Denkwerkstatt können die Teilnehmerinnen und Teilnehmer selbst Themenvorschläge einbringen, die anschließend in sogenannten Workstreams in einer agilen Arbeitsweise über maximal neun Monate bearbeitet werden können.

Weitere Aufgabenschwerpunkte waren die Identifizierung der relevanten zivilgesellschaftlichen Akteure im Feld Cyber-Sicherheit, ihrer wesentlichen Aktivitäten, Zielsetzungen und Vernetzungsstrukturen sowie die Initialisierung einer Veranstaltung, die zur Vernetzung der Akteure im Feld Wissensvermittlung und Cyber-Sicherheit beitragen soll.

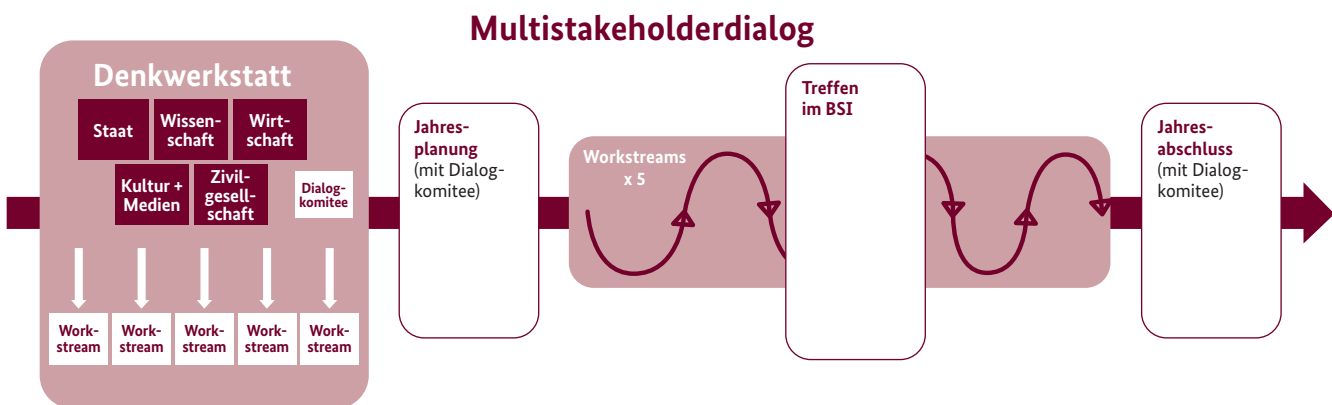


Abbildung 5 Jahreszyklus des Dialogprozesses (vereinfachte Darstellung). Quelle: BSI

Weitere Informationen zum Projekt und den Ergebnissen gibt es unter: www.bsi.bund.de/gesellschaftlicherDialog (vgl. *Quellenverzeichnis*²³; www.bsi.bund.de/gesellschaftlicherDialog)

2.1.5 Information und Sensibilisierung von Bürgerinnen und Bürgern

Da Cyber-Kriminelle immer häufiger den Faktor „Mensch“ als Einfallstor für ihre Angriffe mit *Social-Engineering*-

Methoden nutzen (vgl. *Kapitel Zusammenfassung und Bewertung der Gefährdungslage*, Seite 34), ist es eine wichtige Aufgabe des BSI, Bürgerinnen und Bürger zu sensibilisieren. Das BSI bietet dazu ein breites Informations- und Beratungsangebot für Privatanwenderinnen und -anwender unter dem Namen „BSI für Bürger“ an. Im Mittelpunkt dieses Angebots steht die Webseite www.bsi-fuer-buerger.de (vgl. *Quellenverzeichnis*²⁴: www.bsi-fuer-buerger.de), auf der Informationen zu Risiken und Schutzmaßnahmen bei der vielseitigen Nutzung des Internets bereitgestellt werden. Dabei liegt der Fokus auf Empfehlungen für ein sicheres und selbstbestimmtes Handeln im digitalen Raum. Auf aktuelle Vorfälle wird direkt reagiert, beispielsweise mit Handlungsempfehlungen zu eklatanten Sicherheitslücken oder Schadsoftware-Wellen. Die oftmals komplexen Themen sind als Checklisten, informative Grafiken und interaktive Quizze sowie in Experteninterviews, animierten Erklärvideos und Podcasts einfach verständlich aufgearbeitet.

Mit dem kostenlosen Warn- und Informationsdienst Bürger-CERT informiert das BSI in Form von Technischen Warnungen oder mit dem vierzehntägigen Newsletter „Sicher ° Informiert“ über Schwachstellen und gibt entsprechende Hilfestellungen. Derzeit nutzen rund 109.000 Abonnentinnen und Abonnenten dieses Angebot.

Eine fünfteilige Broschürenreihe befasst sich mit dem digitalen Basisschutz und gibt praxistaugliche Tipps zu den Themen: Surfen, Sicher mobil unterwegs, Soziale Medien, IoT und Cloud-Computing. Die Broschüren stehen über die Mediathek der Webseite zum Download zur Verfügung und können dort auch kostenfrei als Printexemplar bestellt werden. Ein Mal- und Rätselheft für den computerbegeisterten Nachwuchs ergänzt seit dem Sommer 2019 das Printangebot als Format speziell für Kinder.

Flankierend zur Webseite präsentiert sich das BSI bürgernah auf den Social-Media-Plattformen Facebook und YouTube. Darüber hinaus steht ein Service-Center telefonisch unter 0800 2741000 oder per E-Mail unter mail@bsi-fuer-buerger.de für Anwenderfragen zu Themen der IT- und Internetsicherheit zur Verfügung.

Darüber hinaus planen das Bundesministerium des Innern, für Bau und Heimat (BMI) und das BSI eine gemeinsame Sensibilisierungs- und Informationskampagne zur IT-Sicherheit für Verbraucherinnen und Verbraucher, die Anfang des Jahres 2021 starten soll. Damit möchten das BMI und das BSI Risikobewusstsein schaffen, die Beurteilungsfähigkeit stärken und Lösungskompetenzen vermitteln. Dazu soll sich die Kampagne auch konkreten Themen widmen, zu denen sich die Bürgerinnen und Bürger gemäß

Umfragen des BSI am meisten Informationen und Unterstützung wünschen.

Kooperationen

Um Synergien zu nutzen, arbeitet „BSI für Bürger“ mit zahlreichen Organisationen und Initiativen zusammen, die sich ebenfalls mit dem Thema Cyber-Sicherheit beschäftigen. So besteht eine rege Zusammenarbeit mit den Verbraucherzentralen, zum Beispiel eine gemeinsame Kommunikation von Themen bei anstehenden Warnungen oder die Videoreihe „Cyber-Sicherheit hoch 2“, in der sich Expertinnen und Experten der Verbraucherzentrale NRW und des BSI zu unterschiedlichen Aspekten der Smartphone-Sicherheit austauschen. Mit dem Ziel der Hilfe zur Selbsthilfe legten ProPK und BSI als Reaktion auf das Digitalbarometer 2019 gemeinsam eine Reihe von Checklisten auf, mit der sie sich gezielt an die Opfer von Kriminalität im Internet wenden. *Phishing*, Betrug beim Online-Banking und Infektion mit Schadprogrammen sind die bisherigen Themen der Reihe. Zusammen mit dem Verein Deutschland sicher im Netz (DsiN) wurde eine Cyber-Fibel erarbeitet, die Multiplikatoren eine Orientierung in der Aufklärungsarbeit geben soll. Mit der Bundesarbeitsgemeinschaft der Seniorenorganisationen (BAGSO) wurde eine Kooperation in Form erster gemeinsamer Aktivitäten initiiert. Dieser Ansatz ist ein Beispiel für die zielgruppenspezifische Erarbeitung von Aufklärungs- und Sensibilisierungsmaßnahmen.

Europäischer Aktionsmonat

Erneut beteiligte sich das BSI als nationaler Koordinator am European Cyber Security Month (ECSM). Der ECSM verfolgt das Ziel, Cyber-Sicherheit in den Fokus von Bürgerinnen und Bürgern, Unternehmen und Organisationen zu rücken und für den verantwortungsbewussten Umgang im Cyber-Raum zu sensibilisieren. Mit 183 Aktionen und Veranstaltungen von 123 Partnern konnte die Bedeutung der Cyber-Sicherheit in Deutschland weiter in die Öffentlichkeit getragen werden. Zu den teilnehmenden Partnern gehörten Unternehmen, Ministerien und Behörden, IHK und Wirtschaftsverbände, Hochschulen und Universitäten sowie die unter dem Dach der Allianz für Cyber-Sicherheit kooperierenden Cyber-Sicherheitsinitiativen. Der offizielle Startschuss zum ECSM in Deutschland fiel im Rahmen des 29. Cyber-Sicherheits-Tages unter dem Motto „Netzwerke schützen Netzwerke“ mit über 300 Vertreterinnen und Vertretern aus Staat, Wirtschaft und Gesellschaft.

Zudem hat sich „BSI für Bürger“ mit eigenen Aktionen beteiligt: Auf Webseite, Facebook und Twitter stand die Hilfe zur Selbsthilfe als Reaktion auf Gefahren im Internet im Mittelpunkt.

2.1.6 Sicherheit von Wearables, Smart Home und dem Internet der Dinge

Wearables sind intelligente elektronische Geräte, die am Körper getragen werden, und aus dem Leben vieler Menschen nicht mehr wegzudenken. Vor allem Fitness-Tracker sind sehr beliebt. Armbanduhren zeigten früher nur die Uhrzeit oder das aktuelle Datum an, können heutzutage jedoch, sofern sie smart sind, bei alltäglichen Dingen des Lebens unterstützen, zum Beispiel beim Lesen oder Schreiben von Nachrichten, beim Erhalt und der Steigerung von körperlicher Fitness oder beim Zurechtfinden in fremden Umgebungen. Kurz gesagt: Smart Watches bieten viele nützliche Funktionen bis hin zur Erweiterung des eigenen Smartphones am Handgelenk.

Insbesondere Smart Watches mit GPS-Tracking sind beliebt, auch um den Standort von Kindern oder hilfsbedürftigen Personen nachvollziehen zu können. Eine ständige Internetanbindung und GPS-Tracking eröffnen allerdings auch Möglichkeiten für kriminelle Absichten. So existieren zum Beispiel Medienberichte über kritische Schwachstellen in Smart Watches, die die Privatsphäre von Nutzerinnen und Nutzern verletzen.

Bei einer Smart Watch für Kinder stellte ein Sicherheitsforscher beispielsweise gravierende Sicherheitsmängel fest und informierte hierüber Ende 2019 sowohl das *Computer Emergency Response Team (CERT)* des BSI als auch die Presse. Daraufhin wurden die Schwachstellen in einer sicherheitstechnischen Prüfung verifiziert und der Hersteller zu einer Stellungnahme nach § 7a BSIG zu den festgestellten Schwachstellen aufgefordert.

Aufgrund einer fehlenden Verschlüsselung bei der Kommunikation zwischen der Smartphone-App und dem Server des Herstellers sowie einer fehlerhaft durchgeführten Authentifizierung war es möglich, die übertragenen Daten mitzulesen und persönliche Daten von Nutzerinnen und Nutzern abzufragen.

Durch das Ändern der Geräte-ID in einer Konfigurationsdatei der App auf dem Smartphone wurde darüber hinaus die Möglichkeit eröffnet, die App mit der Smart Watch einer anderen Person zu verbinden. Somit erhielt der Angreifer Zugriff auf die gespeicherten Daten einer fremden Smart Watch, zum Beispiel auf die Telefonkontakte, den Live-Standort der Person u. ä. Dadurch wurde eine Übernahme und Steuerung beliebiger Benutzer-Accounts ermöglicht, ohne dass die eigentliche Inhaberin oder der Inhaber dies zwangsläufig bemerkt hätte. Die Geräte-IDs wurden fortlaufend vergeben, was eine Übernahme eines Benutzer-Accounts durch die fehlende Authentifizierung erleichterte. Um diese Schwachstellen auszunutzen zu können, bedurfte es keines tiefer gehenden technischen Wissens.

Nach Bekanntwerden der Schwachstellen beim Hersteller wurde das Produkt von diesem zunächst vom Markt genommen.

Der Hersteller überarbeitete die Smart Watch und berichtete dem BSI, dass die Schwachstellen nun geschlossen seien. Dies wurde durch eine erneute Überprüfung nachvollzogen. Hierbei war festzustellen, dass die bekannten Schwachstellen mit Hilfe eines Software-Updates der Smartphone-App und einer Schnittstelle am Server des Herstellers geschlossen wurden.

Ein solcher Fall ist keine Ausnahme und trat in der Vergangenheit bereits mehrfach in ähnlicher Form auf. Präventiv können bereits in der Konzeptions- und Entwicklungsphase von smarten Produkten Sicherheitsstandards wie zum Beispiel der europäische Standard ETSI EN 303 645 angewendet werden. Dieser fordert beispielsweise, dass die Kommunikation von sensiblen persönlichen Daten, insbesondere zu externen Services, nach dem Stand der Technik verschlüsselt sein muss. Außerdem adressiert der Standard eine Basisschutzanforderung für Consumer-IoT-Geräte, worunter auch die Smart Watches fallen. Das BSI beteiligt sich an der Entwicklung des Standards und den zugehörigen Prüfspezifikationen.

Generell lässt sich festhalten, dass Smart Watches und andere Geräte im Smart Home viele persönliche und sensible Daten generieren und speichern. Diese Daten sind ein wertvolles Ziel für Angreifer. Daher ist es wichtig und sinnvoll, diese Geräte entsprechend zu schützen.

Das BSI setzt sich dafür ein, ein angemessenes Schutzniveau im Bereich der IT-Sicherheit insbesondere bei smarten Verbraucherprodukten zu etablieren. Die Schaffung angemessener Sicherheitsstandards und deren flächendeckender Einsatz bei Herstellern und Entwicklern ist dabei ein vordringliches Ziel des BSI. Die Förderung von *Security by Design* und *Security by Default* von der Produktentwicklung über den kompletten Lebenszyklus hinweg kann dabei das Sicherheitsniveau signifikant anheben und die geschilderten Angriffsmöglichkeiten deutlich reduzieren. Hierzu befindet sich das BSI in einem stetigen Austausch mit wichtigen Stakeholdern und bietet darüber hinaus ein umfangreiches Online-Angebot, um einen selbstbestimmten und bewussten Umgang der Bürgerinnen und Bürger mit smarten Produkten und Services im *Internet of Things* und dem Smart Home zu fördern.

2.1.7 Sicherheit von Medizinprodukten

Die fortschreitende Digitalisierung im Gesundheitswesen hat nicht nur auf den Bereich der medizinischen Versorgung einen großen Einfluss, sondern auch auf die Medizintechnik und hier insbesondere auf die Vernetzung von Medizinprodukten. Schwachstellen in und an vernetzten

Medizinprodukten müssen als potenzielle Einfallstore für Kriminelle gesehen werden. Ihre Ausnutzung könnte die Vertraulichkeit, die Integrität und die Verfügbarkeit von Daten betreffen und möglicherweise zu gesundheitlichem Schaden oder im schlimmsten Fall sogar zum Tod von Patientinnen und Patienten führen. Daher ist die Diskussion zur Cyber-Sicherheit von Medizinprodukten ein Thema, das weltweit nicht nur Hersteller und Betreiber, sondern auch Patientinnen und Patienten bewegt.

Das BSI sieht sich in der Verantwortung, die Cyber-Sicherheit im Bereich der vernetzten Medizinprodukte, beispielsweise durch Projekt- oder Gremienarbeit und Publikationen, mitzugestalten und voranzutreiben. Das BSI-Projekt ManiMed – Manipulation von Medizinprodukten - soll im Folgenden näher beleuchtet werden, da eine solche Untersuchung bisher weder auf nationaler noch internationaler Ebene durchgeführt wurde und die Ergebnisse möglicherweise wegweisend für diesen Bereich des Gesundheitswesens sein können.

ManiMed – Manipulation von Medizinprodukten

Das Projekt ManiMed startete Anfang 2019 und hat den Anspruch bis zum Projektende (Q4/2020), die Cyber-Sicherheitslage von vernetzten Medizinprodukten möglichst realistisch abzubilden. Darüber hinaus soll es dazu beitragen, dass sowohl die Kooperation zwischen allen Beteiligten (Hersteller, Sicherheitsforscher und Behörden) als auch alle Prozesse, die zu einem Coordinated Vulnerability Disclosure (CVD, koordinierte Offenlegung von Schwachstellen in IT-Produkten) gehören, aktiv vorgelebt werden. Dadurch wird die Sensibilität für und die Handhabbarkeit von Schwachstellen gestärkt und so ein Beitrag dafür geleistet, die Cyber-Sicherheit im Bereich von vernetzten Medizinprodukten langfristig auf einem hohen Niveau zu halten.

Je zwei Produkte aus fünf unterschiedlichen Gerätegruppen wurden zur IT-sicherheitstechnischen Untersuchung ausgewählt. Diese sollten im Idealfall eine hohe Anzahl an Schnittstellen aufweisen (große Angriffsfläche) und erst innerhalb der letzten fünf Jahre in Deutschland in den Verkehr gebracht worden sein. Es wurden Produkte aus den folgenden Geräteklassen ausgewählt:

- Implantierbare Herzschrittmacher oder Defibrillatoren und deren Zubehör,
- Insulinpumpen,
- Beatmungsgeräte,
- Patientenmonitore,
- Infusionspumpen.

Die Produkte wurden tiefgehenden IT-sicherheitstechnischen Prüfungen durch die *ERNW Research GmbH* unter-

zogen und die gefundenen Schwachstellen in Form eines detaillierten Prüfberichts dem Hersteller übermittelt. Im Anschluss wurden diese in vertrauensvoller Zusammenarbeit mit dem Hersteller, den Sicherheitsforschern und dem BSI diskutiert.

Der Hersteller erarbeitet aus dem vorliegenden Prüfbericht eine Risikoeinschätzung und leitet ggf. weitere interne Prozesse ein. Das Vorgehen im Projekt orientiert sich an einem CVD, bei dem die gefundenen IT-Sicherheitslücken vorerst nicht veröffentlicht werden (mind. 90 Tage), damit der Hersteller Zeit hat, sie zu beheben und entsprechende Sicherheitsupdates zu entwickeln, zu überprüfen und auszurollen. Sollte der Hersteller anhand der gefundenen Schwachstellen jedoch ein Patientenrisiko im Zuge seiner Risikoeinschätzung erkennen können, so wird das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) als zuständige Aufsichtsbehörde für Medizinprodukte-Vigilanz hinzugezogen.

Die Kommunikation zwischen allen Beteiligten und das Sicherstellen von gegenseitigem Vertrauen während der Zusammenarbeit ist, neben der technischen Expertise, ein eminent wichtiger Aspekt in diesem Projekt. Der transparente und offene Umgang mit Schwachstellen und der entsprechende Kommunikationsaustausch in diesem Bereich sind notwendig, um dieses Vertrauen langfristig aufzubauen, zu halten und zu stärken. Erst wenn die Schwachstellen behoben sind, werden sie, in Absprache mit dem Hersteller, veröffentlicht und gegebenenfalls auf einschlägigen IT-Sicherheitskonferenzen vorgestellt. Von den insgesamt zehn Produkten, die im Rahmen des Projekts untersucht werden, konnten die meisten Produkte durch Teststellungsverträge mit den entsprechenden Herstellern zur Verfügung gestellt werden. Das BSI begrüßt die Bereitschaft der Hersteller, ihre Produkte auf Cyber-Sicherheitseigenschaften testen zu lassen und mit Sicherheitsforschern und dem BSI zusammenzuarbeiten.

Die aktuellen und teils kritischen Ergebnisse zeigen bereits, dass Schwachstellen bestehen, die durchaus häufiger auftreten, und dass bereits zum Projektende konkrete Aussagen zur Cyber-Sicherheitslage von Medizinprodukten getroffen werden können. In der abschließenden IT-Sicherheitsbetrachtung sollen die Ergebnisse des Projekts in verständlicher Form dargestellt werden. Das Projekt soll dazu beitragen, dass die Gefährdungslage bezüglich der Cyber-Sicherheitseigenschaften von vernetzten Medizinprodukten besser eingeschätzt werden kann. Idealerweise fließen die Ergebnisse, die sich aus den Tests ergeben, in die Standardisierung ein und helfen dem BSI bei der Erstellung Technischer Richtlinien und weiterer Publikationen.

2.1.8 Corona-Warn-App

Aufgrund der aktuellen Pandemielage durch die Verbreitung des Corona-Virus besteht nicht nur international, sondern auch in Deutschland großes Interesse an einer mobilen *Applikation*, die bei der Nachverfolgung und Unterbrechung von Infektionsketten unterstützen soll. Um eine möglichst große Akzeptanz in der Bevölkerung zu erreichen, muss eine solche *App* nicht nur ihren Zweck im Sinne der Pandemie-Eindämmung erfüllen, sondern auch möglichst hohen Anforderungen von Datenschutz und Datensicherheit gerecht werden. Die deutsche Lösung heißt *Corona-Warn-App* (CWA) und wurde im Auftrag der Bundesregierung von der Deutschen Telekom AG und SAP entwickelt. Das BSI hat die Entwicklung der *Corona-Warn-App* eng begleitet, etwa durch entwicklungsbegleitende Tests der *App* und der zugehörigen Backend-Infrastruktur sowie in beratender Funktion bei der Erarbeitung und Umsetzung des Sicherheitskonzepts. Die *Corona-Warn-App* ist seit 16. Juni 2020 in den *App*-Stores zum Download verfügbar.

Die Bundesregierung hat sich bei der Entwicklung der *App* für ein transparentes Vorgehen entschieden. Die *Corona-Warn-App* ist daher eine Open-Source-Entwicklung. Das bedeutet, dass der Code der *Applikationen* und des Hintergrundsystems in einem GitHub-Repository öffentlich zur Verfügung stehen. Bereits in der Entwicklungsphase wurden die *App* und das entsprechende Hintergrundsystem kontinuierlich durch das BSI begleitet und untersucht, etwa durch Penetrationstests von *Applikation* und Hintergrundsystem. Darüber hinaus war das BSI beratend hinsichtlich der Fachsicherheitskonzepte tätig. Alle vom BSI und seinen Dienstleistern gefundenen Schwachstellen, die die IT-Sicherheit betreffen, wurden vom BSI auf GitHub eingepflegt und von den Entwicklern behoben. Durch die vertrauensvolle und eng verzahnte Zusammenarbeit konnten die Entwickler das Gesamtsystem kontinuierlich IT-sicherheitstechnisch verbessern und eine Lösung zur Verfügung stellen, die ein Höchstmaß an Informationssicherheit bietet. Das BSI wird auch weiterhin die CWA IT-sicherheitstechnisch begleiten.

2.1.9 eHealth / elektronische Gesundheitskarte

Die elektronische Gesundheitskarte (eGK) in Verbindung mit dem Ausbau der Telematikinfrastruktur (TI) zur Vernetzung aller Beteiligten im Gesundheitswesen ist ein gutes Beispiel dafür, wie diese zunehmende Vernetzung in Verbindung mit einer voranschreitenden Digitalisierung zur Steigerung der Effizienz in der Versorgung und zur Erhöhung der Sicherheit von Patientinnen und Patienten beitragen kann. Die Entwicklung und der zukünftige Einsatz von neuen Anwendungen, zum Beispiel das

Notfalldatenmanagement (NFDM), der eMedikationsplan im Zusammenhang mit der Arzneimitteltherapiesicherheit (AMTS) und die elektronische Patientenakte (ePA), eröffnen den Nutzerinnen und Nutzern der TI neue Möglichkeiten.

Auf der Basis von Spezifikationen der Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH (gematik) hat das BSI entsprechende Technische Richtlinien verfasst⁷. Diese helfen, die mit den bisherigen Basisfunktionen ausgestatteten Konnektoren zur Anbindung an die TI, die vom BSI zertifiziert sind und sich u. a. in Arztpraxen und Krankenhäusern im Einsatz befinden, sicher um die neuen Funktionen zu erweitern. So können zukünftig auf Wunsch von Patientinnen und Patienten Daten für den medizinischen Notfall und eMedikationspläne in Verbindung mit der eGK sicher gespeichert und für einen Anwendungsfall bereitgestellt werden. Im Kontext des eMedikationsplans bedeutet dies, dass im Fall einer neuen Verschreibung von Medikamenten durch den behandelnden Arzt Wechselwirkungen mit bereits bestehenden Medikationen leichter als bisher abgeglichen und dadurch mögliche Risiken minimiert werden können.

Mit der eGK steht zukünftig den Mitgliedern einer gesetzlichen Krankenkasse zusätzlich zu den bisherigen Funktionen auch eine elektronische Patientenakte zur Verfügung. Nach dem Einverständnis und der Freigabe des Versicherten können behandelnde Ärzte oder Krankenhäuser dann auf die jeweilige Akte sicher zugreifen, um medizinische Daten von Patientinnen und Patienten einzusehen und zu ergänzen. Mit Hilfe eines vom BSI zertifizierten Konnektors können auch praxisübergreifende medizinische Behandlungen effizient aufeinander abgestimmt werden. Für Patientinnen und Patienten belastende Mehrfachuntersuchungen und damit verbundene Verzögerungen im Behandlungsablauf können so im Idealfall vermieden werden.

Unabhängig von einer Praxis oder von einem Krankenhaus ist dann auch für Patientinnen und Patienten selbst der individuelle Zugriff auf die eigene Akte möglich und kann mittels eigener Geräte (PC oder mobil mittels Smartphone oder Tablet) und einer von der gematik zugelassenen Software erfolgen.

2.1.10 Sicherheit von Bezahlvverfahren

Die seit dem 13. Januar 2018 gültige und in Deutschland durch das Zahlungsdiensteaufsichtsgesetz (ZAG) umgesetzte zweite Zahlungsdiensterichtlinie (Payment Service Directive 2, PSD2) zielt darauf ab, die Sicherheit im Zahlungsverkehr zu erhöhen, den Verbraucherschutz zu stärken, Innovationen zu fördern und den Wettbewerb auf dem Markt zu steigern.

Um die Anforderungen der PSD2 zu konkretisieren, wurden von der Europäischen Bankenaufsichtsbehörde (EBA) in Kooperation mit der Europäischen Zentralbank (EZB) Regulierungsstandards (Regulatory Technical Standards, RTS) unter anderem zur starken Kundenauthentifizierung formuliert, um die Sicherheit bei digitalen Finanzgeschäften zu erhöhen. Authentifizierungslösungen, die auf zwei unabhängigen Elementen der Kategorien Wissen, Besitz oder Inhärenz (Biometrie) beruhen, gelten als starke Kundenauthentifizierung (Strong Customer Authentication, SCA). Dazu gehören zum Beispiel die *Authentifizierung* mit physischer Karte in Form einer Chipkarte (Besitzfaktor) und PIN (Wissensfaktor). Auch chipTAN, SMS-TAN und pushTAN (jeweils Besitzfaktor) in Kombination mit einem wissensbasierten Authentifizierungsfaktor, also zum Beispiel der Online-Banking-PIN oder digitale Karten (Besitzfaktor) mit Fingerabdruck (biometrischer Faktor) erfüllen die Anforderungen.

Grundsätzlich beziehen sich die Anforderungen der PSD2 nur auf Authentifizierungslösungen für elektronische Zahlungen, die von Kundinnen und Kunden initiiert sind. Dazu zählen Transaktionen, die mit digitalen oder physischen Karten durchgeführt werden, also sowohl Transaktionen an einem Zahlungsterminal (Point of Sale, POS) und Geldautomatenverfügungen als auch Zahlungen im E-Commerce wie zum Beispiel Kreditkartenzahlungen, paypal etc. Lastschriften und Käufe auf Rechnungen fallen nicht unter diese Vorgaben.

Die zunehmende Digitalisierung auch im Finanzwesen führt zu einem grundlegenden Wandel der Bezahlverfahren. Dafür ist das Bezahlen mit mobilen Geräten ein gutes Beispiel: Aufgrund immer leistungstärkerer Smartphones mit immer größeren Displays und der Bereitstellung verschiedenster Funktionen zur Verbindung - Near Field Communication (NFC), Beacon und Bluetooth Low Energy (BLE), Barcode und Quick Response Code (QR-Code) - steigt die Benutzerfreundlichkeit, und auch die mobilen Bezahlösungen selbst werden funktioneller und einfacher in der Bedienung. Alternativ bieten Banken und Zahlungsdienstleister neben dem klassischen Online-Banking via Webportal vermehrt Banking-Apps an. Diese können teilweise für klassische Bankgeschäfte, wie Transaktionen oder Daueraufträge, genutzt werden, aber auch für Zahlungen am POS und im E-Commerce.

Besonders wichtig ist aber, sich nicht von Bequemlichkeit leiten zu lassen, sondern der Sicherheit den Vorzug zu geben. Ein Verzicht auf starke Kundenauthentifizierung zugunsten einer schnellen Abwicklung ohne Aufwand für Nutzerinnen und Nutzer ist der Sicherheit abträglich. Die Anwendung des Verfahrens für sichere Online-Kreditkartenzahlung 3D-Secure ist beispielsweise bei Online-Einkäufen noch nicht vollständig verpflichtend. Hier können

Nutzerinnen und Nutzer keinen Einfluss nehmen, da der Online-Händler bestimmt, wie er dieses Authentifizierungsverfahren implementiert. Nutzerinnen und Nutzer können aber zum Beispiel darauf achten, in Online-Shops einzukaufen, bei denen die Nutzung der Kreditkarte durch 3D-Secure abgesichert ist.

War bisher beim Online-Banking der Einsatz von Anmelde- und die Eingabe einer vier- bis sechs-stelligen PIN zur Anmeldung sowie einer TAN-Eingabe zur Freigabe der Transaktion als Quasi-Standard etabliert und erfolgte die Freigabe einer Zahlung am POS durch die PIN-Eingabe oder eine Unterschrift, so können Nutzerinnen und Nutzer heutzutage mit ihren mobilen Geräten Zahlungen autorisieren.

Nutzerinnen und Nutzer verwenden die Entsperrmechanismen – die Eingabe der Geräte-PIN, eines Passwortes oder die Nutzung biometrischer Verfahren – ihres mobilen Gerätes zur Autorisierung. Gerade die Verwendung von Biometrie kann jedoch eine trügerische Sicherheit beim Benutzer hervorrufen. Auch wenn biometrische Verfahren grundsätzlich zur Identifizierung und Autorisierung geeignet sind, spielt die Qualität der verbauten Komponenten wie Fingerabdrucksensor oder Kamera eine entscheidende Rolle. Um die Qualität der verwendeten Sensoren zu bewerten und so die Sicherheit bei Bezahlverfahren mit dem Mobilgerät zu verbessern, entwickelt das BSI Prüfkriterien für biometrische Authentifizierungsmechanismen. Da es sich bei Smartphones um Geräte handelt, die in keiner kontrollierbaren Umgebung eingesetzt werden, bestehen hier besondere Gefahren, denen mit diesen Prüfkriterien begegnet werden soll.

Insgesamt müssen die dadurch entstehenden Risiken durch Sicherheitsanalysen der Gesamtarchitektur und Sicherheitsgutachten auf ein akzeptables Maß reduziert werden und nicht sichere Verfahren durch geeignete Maßnahmen erkannt und gegebenenfalls auch deaktiviert werden.

Grundsätzlich ist wichtig, Nutzerinnen und Nutzern nicht zusätzliche Sicherungsmethoden aufzuzwingen, sondern benutzerfreundliche und sichere Verfahren zu forcieren. Hierzu wurden weiterführende Informationen, auch zur Sicherheit von Bezahlverfahren sowohl im eCommerce als auch am Point of Sales, in der Broschüre „Sicher zahlen im E-Commerce. Fragen und Antworten zu Online-Bezahlverfahren“ zusammengefasst. Die Wahl eines sicheren Online-Bezahlverfahrens ist jedoch nur eine von vielen Maßnahmen zur Verbesserung der persönlichen Cyber-Sicherheit.

2.1.11 Zwei-Faktor-Authentisierung

Der übliche Weg, sich bei einem Online-Dienst zu authentisieren, ist nach wie vor die Eingabe eines Passwortes.

Hier wird ein einzelner Faktor – das Wissen des Passworts – vom Dienst abgefragt, um den Nutzer zu authentifizieren. Passwörter als Authentisierungsmechanismus sind einfach umzusetzen, haben aber mehrere Nachteile: Zum einen reicht die Kenntnis dieses einen Faktors Wissen, um den Authentisierungsmechanismus zu brechen, und zum anderen ist es aufwändig, für jeden Dienst ein sicheres und individuelles Passwort zu wählen, dieses auswendig zu lernen oder in einem Passwortmanager zu verwalten.

Immer mehr Dienste fragen neben dem Passwort einen zweiten Faktor ab, um Nutzerinnen und Nutzer sicherer identifizieren zu können, zum Beispiel mit einer weiteren Abfrage von Wissen in Form eines Authentisierungs-codes, der auf das Smartphone gesendet wird. Eine höhere Sicherheit ist hier aber nur dann gegeben, wenn eine echte Trennung der Geräte stattfindet und sich die Faktoren nicht gleichermaßen angreifen lassen. Wenn, zum Beispiel für eine Smartphone-Anwendung, als erster Faktor ein Passwort und als zweiter Faktor ein an das Smartphone geschickter Code verwendet wird, kann beides durch Schadsoftware auf dem Smartphone ausgelesen werden und ist daher ungeeignet. Darüber hinaus ergeben sich oft weitere Usability-Probleme, zum Beispiel bei einem Wechsel des Smartphones oder der Mobilfunknummer.

Besser ist, wenn bei einer *Zwei-Faktor-Authentisierung* zwei Faktoren aus unterschiedlichen Kategorien (Besitz, Wissen, Biometrie) abgefragt werden. Durch die Kombination der Stärken der einzelnen Faktoren wird der Angriff um ein Vielfaches erschwert. Dabei sollten biometrische Merkmale nicht beim Online-Dienst gespeichert, sondern lokal zur Freischaltung zum Beispiel des Smartphones als Besitzfaktor verwendet werden, welches sich dann gegenüber dem Online-Dienst durch kryptografische Methoden authentisiert.

Die Fast-Identity-Online-Allianz (FIDO) wurde 2013 mit vielen verschiedenen Vertretern aus Staat und Industrie gegründet, um offene und lizenzfreie Industriestandards für die weltweite *Authentisierung* im Internet zu entwickeln. Nach FIDO sind bisher drei Standards entwickelt worden:

- Der Universal Second Factor (U2F) passt sich in Form eines Hardware-Tokens nahtlos in existierende Web-Infrastrukturen ein, da der Besitz des Authentifikators im zweiten Schritt nach einer erfolgreichen *Passwort-Authentisierung* nachgewiesen wird.
- Das Universal Authentication Framework (UAF) erlaubt die passwortlose *Authentisierung*, indem das Passwort durch biometrische Verfahren oder eine PIN in einer sicheren *Zwei-Faktor-Authentisierung* ersetzt wird.

- Die Fortentwicklung FIDO 2.0 besteht aus dem Web Authentication Standard (WebAuthn) des World Wide Web Consortiums (W3C) und verschiedenen Client-to-Authenticator-Protokollen (CTAP), über die der Webbrowser mit den FIDO-Token kommuniziert.

Ein Nachweis über die Sicherheit des verwendeten FIDO-Authentifikators 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 Authentifikatoren beteiligt.

Der Nachweis eines hohen Sicherheitsniveaus kann durch eine Zertifizierung nach Common Criteria erbracht werden. Das BSI hat hierzu ein Schutzprofil mit hoher Prüftiefe für sichere FIDO-U2F-Token veröffentlicht, nach dem ein durch das BSI entwickelter FIDO-U2F-Token erfolgreich zertifiziert worden ist. Ohne eine Prüfung mit entsprechender Sicherheitszertifizierung ist die Gefahr für Implementierungsfehler hoch (vgl. Kapitel *Schwachstellen in Hardware-Produkten*, Seite 26). Auch eine Zertifizierung nach den FIDO-Sicherheitsstandards steht kurz vor dem Abschluss.

Das BSI wird den Quelltext des sicherheitszertifizierten FIDO-Tokens in Kürze als Open Source veröffentlichen, um damit einen Beitrag zur Transparenz und Verbreitung einer sicheren U2F-Implementierung zu leisten. Diese Open Source-Implementierung kann von jedem interessierten Nutzer als Grundlage eigener U2F-Implementierung auf JavaCard-Smartkarten genutzt werden.

Haben zu Beginn der FIDO-Initiative viele Großkonzerne ihre Dienste um die Möglichkeit zur *Authentisierung* mit FIDO ergänzt, stagniert die Nutzung von FIDO-Token mittlerweile, und die Nutzung als Massenprodukt hat sich bislang noch nicht etablieren können.

2.1.12 Bewertung von elektronischen Identifizierungsverfahren

Schon seit vielen Jahren sind Online-Banking und -Shopping aus dem Alltag vieler Bürgerinnen und Bürger nicht mehr wegzudenken. Bis Ende 2022 sollen in Deutschland auch Verwaltungsdienstleistungen grundsätzlich online angeboten werden. Diese Anwendungen haben alle gemeinsam, dass sie auf einer vertrauenswürdigen, gegenseitigen Identifizierung aufbauen. Denn sofern es Angreifern gelingt, entweder die Identität des Senders oder des Empfängers vorzutauschen, können teilweise beträchtliche Schäden entstehen. Durch einen solchen Identitätsbetrug werden einerseits häufig Bürgerinnen und Bürger geschädigt, andererseits aber auch die öffentliche Hand und Unternehmen, wie etwa in Fällen von nachgeahmten Webseiten zur Beantragung von COVID-19-Soforthilfen.

Das BSI arbeitet an verschiedenen Stellen präventiv, um für Staat, Wirtschaft und Gesellschaft eine Risikominimierung von Identitätsbetrug zu ermöglichen. Neben der aktiven Gestaltung hochsicherer Identifizierungslösungen, wie der Online-Ausweiskfunktion, hat das BSI zwei Technische Richtlinien erarbeitet, die es erlauben, verschiedenste Verfahren zu elektronischen Identitäten und Vertrauensdiensten für Online-Prozesse systematisch zu bewerten und Vertrauensniveaus zuzuordnen. Die BSI TR-03107-1 behandelt Vertrauensniveaus sowie Mechanismen für Elektronische Identitäten und Vertrauensdienste im E-Government. Komplementär dazu bietet die BSI TR-03147 eine Möglichkeit zur Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen.

Das BSI hat nun ein Vorhaben gestartet, um anhand dieser Technischen Richtlinien die Sicherheit verschiedener privatwirtschaftlicher elektronischer Identifizierungsverfahren mit Blick auch auf eine Nutzung im E-Government zu bewerten. Die Bewertung erfolgt hierbei differenziert mit Bezug auf die Vertrauensniveaus normal, substantiell und hoch, die in BSI TR-03107-1 näher definiert sind. Im Berichtszeitraum erfolgte die Bewertung von zwei elektronischen Identifizierungsverfahren. Die Ergebnisse der Bewertungen berichtet das BSI an das BMI, das als die für das E-Government zuständige Stelle über die Zustimmung zur Nutzung entscheidet.

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

2.1.13 Sichere elektronische Identitäten auf dem Smartphone

Ein Großteil des heutigen Lebens findet digital statt. Viele Dienstleistungen werden problemlos mit Hilfe des Smartphones bezogen. Um eine Vielzahl von Online-Ser-

vices, wie Banking, Einkaufen oder Social Media nutzen zu können, ist eine elektronische Identität (eID) notwendig. Um diese sicher auf dem Smartphone abzuspeichern und auch datensensible Dienste dort nutzbar zu machen, arbeitet das BSI im Rahmen des Förderprojekts OPTIMOS 2.0 an Lösungen, wie dies nutzerfreundlich umgesetzt werden kann.

Der Begriff eID ist dabei sehr generisch und kann für ganz verschiedene Online-Zugänge stehen wie zum Beispiel das Pseudonym, mit dem man in einem Online-Forum aktiv ist, einen Account in einem Sozialen Netzwerk, als Käufer in einem Online-Shop aufzutreten oder Bankkunde beim Online-Banking zu sein.

Jede dieser eIDs muss gegen Missbrauch geschützt werden. Der Schutz muss je nach Art der elektronischen Identität unterschiedlich stark sein. Manchmal genügt schon die Eingabe einfacher Zugangsdaten (z. B. Nutzernamen und Passwort), jedoch ist diese Art von Schutz bei sensiblen Daten nicht ausreichend. Sollen beispielsweise mit dem Smartphone Bankgeschäfte erledigt oder gar der Zutritt auf das Firmengelände gesteuert werden, sollte eine entsprechende eID stärker geschützt sein. Natürlich ist es nicht notwendig, dass für alle Anwendungsfälle höchste Sicherheitsanforderungen eingehalten werden. Nutzerinnen und Nutzer erwarten dennoch zu Recht, dass ihre Identität nicht einfach gestohlen oder manipuliert werden kann.

Schutz der eIDs

Smartphones sind, wie jedes vernetzte Gerät, ständig der Gefahr eines Cyber-Angriffs ausgesetzt. Darum müssen besondere Voraussetzungen erfüllt sein, um davon ausgehen zu können, dass eIDs auf dem Smartphone sicher gespeichert sind. Die „Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG“, kurz eIDAS-Verordnung, und ihre definierten Vertrauensniveaus bilden hierfür den rechtlichen Rahmen.

Die eIDAS-Verordnung unterscheidet drei Vertrauensniveaus: gering, substantiell und hoch. An jedes dieser Vertrauensniveaus ist eine Widerstandsfähigkeit gegen ein definiertes Angriffspotenzial geknüpft. Das BSI stellt Herstellern mit seinen Technischen Richtlinien Hilfsmittel zur Verfügung, um Anforderungen an die Sicherheit gemäß dem Stand der Technik zu erfüllen. So ist die Technische Richtlinie TR-03107 die nationale Ausprägung der eIDAS-Regulierung. Sie bietet viele Hinweise, welche Voraussetzungen einzuhalten sind, um die genannten Vertrauensniveaus und damit eine bestimmte Widerstandsfähigkeit gegen Cyber-Angriffe zu erreichen.

In den letzten Jahren hat das BSI viele Gespräche mit Herstellern von mobilen Endgeräten geführt und seine Expertise in verschiedenen Standardisierungsgremien eingebracht. Diese Tätigkeiten wurden mit dem Ziel durchgeführt, Hersteller für die Anforderungen an Sicherheit in Smartphones, Tablets und Wearables zu sensibilisieren und die Ansprüche des BSI in internationalen Standards zu verankern. Nur Standards ermöglichen, dass jede Nutzerin und jeder Nutzer von mobilen Geräten notwendige Sicherheitsfunktionen erhält, um die eigene eID zu schützen.

OPTIMOS 2.0

In dem vom Bundesministerium für Wirtschaft und Energie (BMWi) geförderten Forschungsprojekt OPTIMOS 2.0 entwickelt ein Konsortium aus Universitäten, Behörden und Unternehmen Lösungen, wie eIDs sicher und praktikabel auf Smartphones gelangen können. Mit OPTIMOS 2.0 soll eine Infrastruktur geschaffen werden, die für alle Service-Anbieter diskriminierungsfrei zugänglich ist und höchste Sicherheits- und Datenschutzstandards erfüllt. Das zentrale Element ist der *Trusted Service Provider*, der als Schnittstelle zwischen Diensteanbietern und Endkunden die Aufgabe übernimmt, die eIDs sicher auf dem mobilen Endgerät aufzubringen. Um dies zu ermöglichen, engagiert sich das BSI in der Standardisierung der notwendigen Komponenten, Interfaces und Abläufe, damit die entwickelte Technologie für möglichst viele Endnutzerinnen und Endnutzer zur Verfügung steht. Auf dem Digitalgipfel 2019 konnten bereits erfolgreich Prototypen gezeigt werden, in denen unterschiedliche Partner aus der Wirtschaft eingebunden waren.

2.1.14 Biometrie im Zeitalter der Künstlichen Intelligenz

Biometrische Sicherheitstechnologien gewinnen in verschiedensten staatlichen und kommerziellen Anwendungsbereichen stetig an Bedeutung. Ihr Erfolg basiert zu einem großen Teil auf dem Einsatz von tiefen neuronalen Netzen (DNNs), einer Komponente von künstlich intelligenten (KI) Systemen. Diese ermöglichen eine zuvor unbekannte Genauigkeit, Robustheit und Geschwindigkeit bei 1:1-, 1:N- und N:N-Abgleichen von biometrischen Merkmalen. Zuvor undenkbar, können mittlerweile z. B. Frontal- und Profilaufnahmen von Gesichtern mit hoher Genauigkeit abgeglichen werden. Aktuelle hoheitliche und kommerzielle biometrische Systeme werden regelmäßig im BSI im Hinblick auf ihre IT-Sicherheit überprüft und Technische Richtlinien für deren Auswahl und Einsatz entwickelt. Um hierbei den Besonderheiten von KI-Systemen Rechnung zu tragen, werden diese im BSI detailliert untersucht. Die wesentlichen Aspekte und Erkenntnisse dieser Untersuchungen werden im Folgenden anhand von Abbildung 6 erläutert:

Das BSI ist laut BSI-Gesetz (§ 3 Abs.1 S.2 Nr.7) befugt, im KI-Biometrie-Systeme treffen anhand von Sensordaten Entscheidungen über die Identität von Personen (Abb. 6 mitte: in blau ist der korrekte Regelbetrieb dargestellt, in rot ist links der Fall eines *adversarialen Angriffs* und rechts der Fall eines *Morphing-Angriffs* dargestellt). Diese Systeme können aufgrund ihrer Komplexität nicht direkt von den Entwicklern konstruiert werden, sondern werden (Abb. 6 von links nach rechts) mithilfe von KI-Modellen, maschinellen Lernverfahren und Daten

KI-Biometrie: Betrieb, Training & Angriff

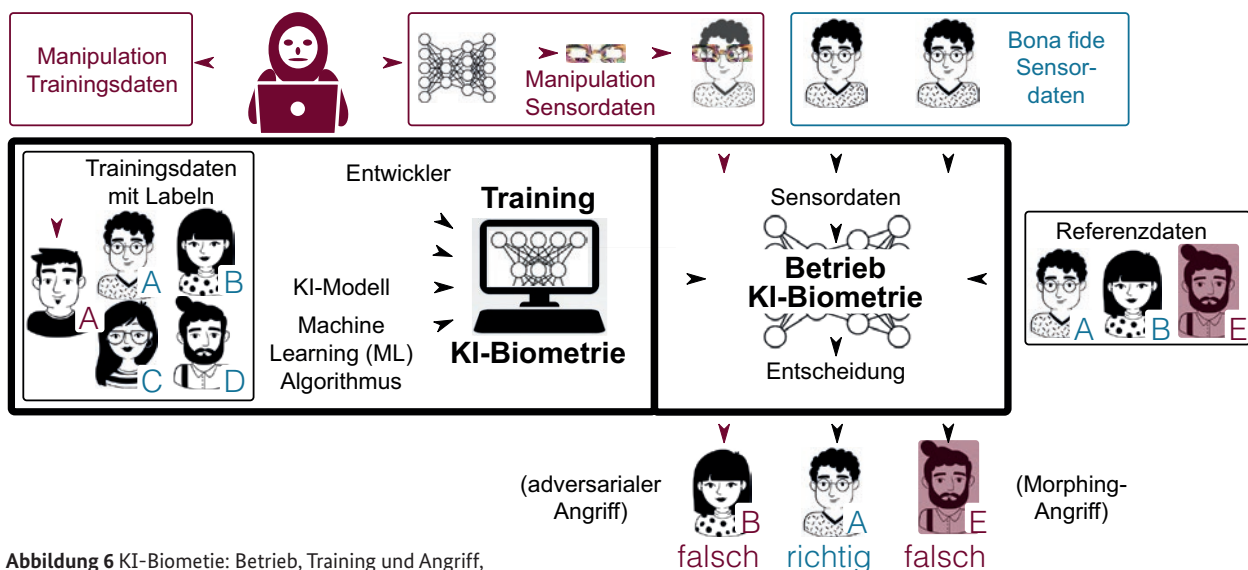


Abbildung 6 KI-Biometrie: Betrieb, Training und Angriff, Quelle: <https://de.freepik.com>, BSI

in einer z. T. komplexen Prozesskette trainiert, getestet und in den Betrieb überführt. Hohe Genauigkeit und Robustheit von KI-Systemen erfordern vor dem Betrieb Trainings und Tests mit einer großen Menge an geeigneten Trainings- und Testdaten, eine hohe Rechenleistung und eine hinreichende Erfahrung der Entwickler. Eine entsprechende Untersuchungsplattform für die Schwachstellenanalyse biometrischer KI-Systeme wurde im letzten Berichtszeitraum im BSI etabliert.

Neben einer hohen Performanz und Robustheit besitzen KI-Systeme im Vergleich zu klassischen IT-Systemen qualitativ neue Verwundbarkeiten mit potenziell ernststen Implikationen für die IT-Sicherheit. Einerseits können Angreifer Trainingsdaten manipulieren (Abb. 6 links oben), was z. B. zum Eintrainieren von schwer detektierbaren Hintertüren in das KI-System führen kann. Andererseits können Angreifer Referenzdaten manipulieren, z. B. durch das Verschmelzen mehrerer Gesichter zu einem Ausweisfoto (Gesichts-Morphing, vgl. rotes Gesichtsbild im Kasten Referenzdaten in Abb. 6). Außerdem können Angreifer die aktuellen Sensordaten während des Betriebs durch die Präsentation von Artefakten, z. B. im Rahmen von adversarialen Angriffen (Abb. 6 mitte oben) oder sogenannten Deep Fakes, manipulieren. Bei adversarialen Angriffen werden Sensordaten vom Angreifer so modifiziert, dass dies einerseits Menschen i. d. R. nicht als Angriff auffällt (bei Bildern z. B. ein leichtes Rauschmuster oder ein Aufkleber mit einem bunten Muster im Bild), andererseits aber das KI-System eine andere Entscheidung trifft, als ursprünglich vom Entwickler beabsichtigt. Hierbei werden KI-spezifische Verwundbarkeiten ausgenutzt. Bei Deep Fakes werden Sensordaten so manipuliert, dass in erster Linie Menschen und optional auch KI-Systeme. Zur Generierung dieser Artefakte werden oftmals wiederum KI-Systeme eingesetzt.

Für Angriffe auf die Gesichtsbio-metrie können u. a. Mützenaufnäher oder Brillengestelle mit speziellen Mustern präpariert werden, um zu einer gezielten Falschklassifikation der Person zu führen (in Abb. 6 wird Person A mit manipulierter Brille als Person B erkannt; in den realen Daten der Abb. 7 wird Person 3 mittels Brillenangriff zu fast 80 % als Person 1 und nur zu <5 % als Person 3 erkannt). Die zurzeit dominant eingesetzten DNNs lassen sich aufgrund inhärenter Eigenschaften sehr schwer interpretieren, d. h. ihre Entscheidungen lassen sich in der Regel nicht nachvollziehen. Hieraus folgt, dass die oben genannten Angriffe nur sehr schwer erkannt werden können und es neuer Ansätze zur verbesserten Interpretierbarkeit von KI-Systemen bedarf. Die verschiedenen Aspekte von Angriffen und Verteidigungsmaßnahmen werden momentan im Rahmen von wissenschaftlichen Arbeiten in Kooperationen mit führenden nationalen

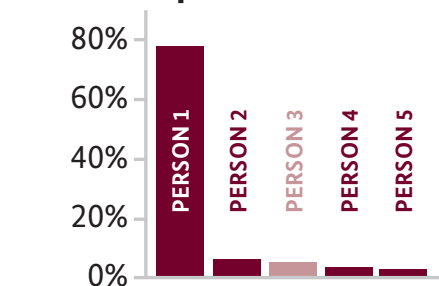


Abbildung 7 Wahrscheinlichkeit Top 5 Konfidenz, Quelle: GettyImages ©Morsa Images, BSI

Forschungseinrichtungen im BSI untersucht. Die neuen Verwundbarkeiten von KI-Systemen und die Möglichkeiten zu deren Evaluation wurden systematisch in einem wissenschaftlichen Überblicksartikel des BSI aufgearbeitet (vgl. Kapitel *Künstliche Intelligenz*, Seite 74).

2.2 Wirtschaft / Kritische Infrastrukturen

Die deutsche Wirtschaft hängt in hohem Maße von einer funktionierenden IT ab. In besonderer Weise gilt dies für Betreiber Kritischer Infrastrukturen (KRITIS). Daher prüft das BSI fortwährend, ob und inwieweit ein ausreichender Schutz gewährleistet ist, und schafft zugleich die Voraussetzungen für eine Weiterentwicklung der entsprechenden Infrastrukturen. Mit der Freigabe für den Rollout intelligenter Messsysteme wurde so beispielsweise ein wichtiger Schritt für die Digitalisierung der Energiewende unternommen und gleichzeitig ein Beitrag geleistet, die Netze besser vor Cyber-Angriffen zu schützen. Auch beim Ausbau der 5G-Netze oder der Verbreitung intelligenter Fahrsysteme wirkt das BSI im Zusammenspiel mit den jeweiligen Herstellern und Betreibern auf ein angemessenes Sicherheitsniveau hin. Über die Allianz für Cyber-Sicherheit treibt das BSI gemeinsam mit Partnern zusätzlich auch den Austausch mit der Wirtschaft zu und den Aufbau von IT-Sicherheits-Know-how voran.

2.2.1 Gefährdungslage Wirtschaft mit besonderer Betrachtung Kritischer Infrastrukturen

Kritische Infrastrukturen (KRITIS) sind Organisationen mit wichtiger Bedeutung für das Gemeinwesen. Sie erbringen kritische Dienstleistungen, wie beispielsweise Lebensmittel-, Wasser- oder Stromversorgung, aber auch die medizinische Versorgung, die Verarbeitung und Speicherung von Daten in Rechenzentren oder die Bargeldversorgung. Alle diese Dienstleistungen werden inzwischen mit einem massiven Einsatz von Informationstechnik erbracht. Sie sind daher ganz besonders von einer störungsfrei arbeitenden IT abhängig. Eine Störung, Beeinträchtigung oder auch ein Ausfall dieser Dienstleistungen durch einen IT-Sicherheitsvorfall kann zu nachhaltig wirkenden Versorgungsengpässen, erheblichen Störungen der öffentlichen Sicherheit oder anderen dramatischen Folgen führen.

Diese Abhängigkeit von IT betrifft natürlich nicht nur Kritische Infrastrukturen, sondern fast ausnahmslos die gesamte Wirtschaft. Informationstechnologie ist allgegenwärtig – in der Bürowelt, aber auch in der industriellen Produktion. Bei Cyber-Angriffen, technischem Versagen oder anderen Vorfällen können IT-Systeme nicht nur ausfallen oder zerstört werden, es bestehen auch weitere Gefahren, zum Beispiel, dass Daten in die falschen Hände geraten oder manipuliert werden.

Definition Kritischer Infrastrukturen

Die Nationale KRITIS-Strategie aus dem Jahr 2009 definiert neun Sektoren der Kritischen Infrastrukturen: Energie, Informationstechnik und Telekommunikation, Gesundheit, Transport und Verkehr, Medien und Kultur, Wasser, Finanz- und Versicherungswesen, Ernährung

sowie Staat und Verwaltung. Alle Organisationen aus diesen Sektoren zählen unabhängig von ihrer Größe zu den Kritischen Infrastrukturen (KRITIS).

Im BSI-Gesetz (BSIG) wurde aufbauend auf dieser Definition und in Verbindung mit der BSI-Kritisverordnung (BSI-KritisV) eine Konkretisierung in Hinblick auf die zu schützenden IT-Systeme in diesen Sektoren vorgenommen. Die BSI-KritisV legt anhand messbarer und nachvollziehbarer Kriterien fest, welche Organisationen unter den Regelungsbereich des BSIG fallen. Organisationen sind demnach Betreiber Kritischer Infrastrukturen gemäß § 10 Abs. 1 BSIG i. V. m. BSI-KritisV, wenn sie einem der sieben Sektoren aus den §§ 2 bis 8 der BSI-KritisV angehören (alle obigen außer Medien und Kultur sowie Staat und Verwaltung), kritische Dienstleistungen gem. § 1 Abs. 3 BSI-KritisV erbringen und dabei die dort definierten Schwellenwerte überschreiten.

Welche Unternehmen aus Ländersicht als Betreiber Kritischer Infrastrukturen gelten, richtet sich ausschließlich nach den entsprechenden Landesgesetzen und den von den zuständigen Behörden der Bundesländer bekannt gegebenen Kriterien, die sich z. T. auch an der BSI-Kritisverordnung orientieren.

Mit dem IT-Sicherheitsgesetz (IT-SiG) hat die Bundesregierung im Jahr 2015 im BSI-Gesetz und in weiteren Gesetzen neue Pflichten für KRITIS-Betreiber verankert. So sieht das BSI-Gesetz für KRITIS-Betreiber Maßnahmen zur Prävention (§ 8a) und zur Bewältigung (§ 8b) von IT-Sicherheitsvorfällen oder IT-Störungen vor.

2.2.1.1 Präventive Maßnahmen nach § 8a BSI-Gesetz für Betreiber Kritischer Infrastrukturen




<p>Sicherheits- & Risikokultur</p>	<ul style="list-style-type: none"> ■ Betreiber muss angemessene Maßnahmen nach Stand der Technik treffen ■ Branchenspezifische Sicherheitsstandards 	 <p>§ 8a (1) § 8a (2)</p>	<p>Branchenspezifische Sicherheitsstandards</p>
<p>Wirksamkeit der Maßnahmen</p>	<ul style="list-style-type: none"> ■ Auditierungspflicht (alle 2 Jahre) ■ Nachweis gegenüber BSI ■ Überprüfung der Einhaltung vor Ort 	 <p>§ 8a (3) § 8a (4)</p>	<p>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</p>
<p>Warnungen & Lagebilder</p>	<ul style="list-style-type: none"> ■ BSI: Erstellung/Verteilung von Warnungen & Lagebildern ■ KRITIS-Betreiber: Meldepflicht von (erheblichen) Vorfällen ■ KRITIS-Betreiber: hat Informationsrecht 	 <p>§ 8b (1) § 8b (2) § 8b (3)</p>	

Abbildung 8 Übersicht der wesentlichen Regelungen im BSI-Gesetz für Kritische Infrastrukturen, Quelle: BSI

nen die Branchen branchenspezifische Sicherheitsstandards (B3S) erarbeiten, für die das BSI auf Antrag feststellt, ob sie geeignet sind, die Anforderungen nach § 8a Abs. 1 BSIG zu gewährleisten. Über zwanzig KRITIS-Branchen haben bereits B3S erstellt oder erarbeiten solche. Zwölf davon wurden bereits vom BSI mit positivem Ergebnis auf Eignung geprüft. Die aktuelle Liste der B3S steht auf der BSI-Webseite (vgl. *Quellenverzeichnis*²⁵: www.bsi.bund.de) zur Verfügung.

Aufgrund der dynamischen technischen Entwicklung muss die Eignung eines B3S nach zwei Jahren erneut vom BSI festgestellt werden. Da die Erstellung der ersten B3S bereits über zwei Jahre zurückliegt, wurden oder werden diese überarbeitet und erneut zur Eignungsprüfung vorgelegt. Im Berichtszeitraum hat das BSI für die B3S aus den folgenden Branchen die Eignung festgestellt:

- Wasser/Abwasser (Wiederholungsprüfung)
- Lebensmittelhandel (Wiederholungsprüfung)

Erkenntnisse aus den Nachweisen von KRITIS-Betreibern

Die Betreiber Kritischer Infrastrukturen müssen angemessene Sicherheitsmaßnahmen zum Schutz ihrer IT-Systeme, Komponenten und Prozesse umsetzen, wobei der Stand der Technik eingehalten werden soll. Dies müssen sie nach § 8a Abs. 3 BSIG alle zwei Jahre gegenüber dem BSI nachweisen, sofern sie nicht einer Nachweispflicht einer anderen Behörde gegenüber unterliegen wie zum Beispiel Betreiber von Energieversorgungs- oder Telekommunikationsnetzen (§ 8a Abs. 3 und § 8d Abs. 2 BSIG). Ein Nachweis nach § 8a Abs. 3 BSIG ist die Dokumentation einer durchgeführten Prüfung einer KRITIS-Anlage durch eine vom KRITIS-Betreiber beauftragte prüfende Stelle. Um den Betreibern die Erstellung ihrer Nachweise zu erleichtern, hat das BSI im Mai 2019 die Version 1.0 der Orientierungshilfe zu Nachweisen gemäß § 8a Abs. 3 BSIG veröffentlicht (vgl. *Quellenverzeichnis*²⁶: www.bsi.bund.de).

Im Jahr 2019 waren 358 Betreiber nachweispflichtig. Im Berichtszeitraum erhielt das BSI 350 Nachweise. Alle Nachweise werden einer Vollständigkeitsprüfung und einer Plausibilitätsprüfung unterzogen sowie in ihrer Gesamtheit ausgewertet, um Schwerpunktthemen, Herausforderungen und Trends aufzudecken. Eine Auswertung der aufgedeckten Sicherheitsmängel der einzelnen Sektoren zeigt unterschiedliche Schwerpunkte.

Aufgrund der zentralen Bedeutung der Branche Informationstechnik für andere kritische Dienstleistungen existiert dort ein tief verankertes Verständnis über den Stellenwert der Informationssicherheit. Viele Betreiber dieser Branche verfügen bereits über ein langjährig etabliertes Managementsystem für Informationssicherheit

(Information Security Management System, ISMS) und Business Continuity Management System (BCMS). Zudem werden viele Betreiber aus der Branche im Rahmen von Kundenaudits mit überprüft. Dadurch werden bestehende IT-Sicherheitsmängel bereits früher aufgedeckt und abgestellt. In der Branche Informationstechnik wurden daher von den Prüfern nur wenige Mängel aufgedeckt.

Im Sektor Gesundheit im Bereich der medizinischen Versorgung legen viele Betreiber den Fokus derzeit vor allem auf die Umsetzung von technischen IT-Sicherheitsmaßnahmen. Bei der Umsetzung von organisatorischen IT-Sicherheitsmaßnahmen ist dagegen noch Verbesserungspotenzial erkennbar. Aufgrund oftmals fehlender Sensibilisierung der Managementebene in Bezug auf die IT-Sicherheit wurden bei einer Vielzahl von Betreibern notwendige Richtlinien für das ISMS noch nicht vollständig erstellt oder noch nicht final durch die Geschäftsführung oder den Vorstand verabschiedet. Bei einigen Betreibern wurde zudem das IT-Risikomanagement, das Risikomanagement der Medizintechnik oder das IT-Notfallmanagement noch nicht in das klinikweite Risikomanagement oder Business Continuity Management überführt. In Pharmaunternehmen ist festzustellen, dass vor allem die zentrale Absicherung von mehreren Standorten und die Absicherung der bei der Arzneimittelherstellung eingesetzten industriellen Steuerungssysteme besondere Herausforderungen darstellen.

Für die Branchen Lebensmittelhandel und -produktion im Sektor Ernährung zeigt sich ein vergleichbares Bild. Auch hier sind die Betreiber technisch gut aufgestellt. Die erkennbaren organisatorischen Mängel wie Schwächen in Prozessen, Richtlinien oder Zuständigkeiten sind in neu eingeführten Managementsystemen begründet. Eine besondere Herausforderung ist die Absicherung industrieller IT-Komponenten. Die Branche benötigt zudem Konzepte, um Notfallpläne auch im 24/7-Schichtbetrieb ohne größere Schwierigkeiten umsetzen zu können.

Der Sektor Transport und Verkehr ist mit seinen Branchen Luftfahrt, See- & Binnenschifffahrt, Schienenverkehr, Straßenverkehr, ÖPNV und Logistik sehr divers aufgestellt. Branchenübergreifend ist zu erkennen, dass bei vielen Betreibern die getroffenen technischen und organisatorischen Maßnahmen noch nicht vollständig über einen ganzheitlichen Managementprozess, wie etwa ein ISMS, abgebildet werden. Schwächen sind zum Beispiel im Brandschutz und bei der Zugriffs- und Zutrittskontrolle zu erkennen. Oft fehlt es noch an einer ausreichenden Sensibilisierung und Schulung der Beschäftigten.

In den Sektoren Energie und Wasser ist erkennbar, dass ein Großteil der festgestellten Mängel in den Mängelkategorien Netztrennung, Notfallmanagement und physischer

Sicherheit liegt. Eine funktionierende Netztrennung ist zur effektiven Abwehr von Angriffen wichtig. Sie unterbindet den unbefugten Zugang aus dem Internet oder aus Büro- netzen in Produktionsnetze (wo beispielsweise Maschinen gesteuert werden) und damit zur kritischen Dienstlei- tung und detektiert unbefugte Aktivitäten an eventuell vorhandenen Netzübergängen. Das Notfallmanagement lebt durch funktionierende Regelungen und Prozesse. Seine große Bedeutung wird gerade durch die eingetrete- ne COVID-19-Pandemie deutlich. Sie wirkt sich teilweise unmittelbar auf die IT-Sicherheit aus, insbesondere wenn aus Gründen der Notfallbewältigung geltende Sicher- heitsregeln geändert oder sogar gelockert werden müssen, während zeitgleich weniger IT-Fachleute in den Organisa- tionen verfügbar sind. Mängel bei der physischen Sicher- heit sind nicht weniger wichtig, erfordern aber einerseits typischerweise eine längere Planung der umzusetzenden Maßnahmen und können andererseits in der Übergangs- zeit oft durch organisatorische Maßnahmen kompensiert werden. Von Freigaben in den Unternehmen bis hin zu Baugenehmigungen und deren Umsetzung liegen teilweise lange Zeiträume bis zur endgültigen Behebung der Mängel. Für den Zeitraum bis zum Abschluss der Maßnahmen müssen Betreiber geeignete andere Schutzmaßnahmen treffen, um dem bestehenden Risiko zu begegnen.

Für alle Mängelkategorien ist das BSI in Zusammenarbeit mit den Betreibern bestrebt, eine kurzfristige Mängelbe- hebung voranzubringen. Letztlich ist die Erhöhung des IT-Sicherheitsniveaus beim Betrieb Kritischer Infrastruk- turen erklärtes gemeinsames Ziel von Betreibern und dem BSI. Aus diesem Grund steht das BSI in kontinuierlichem Austausch mit den Betreibern und begleitet und fördert die Abstellung der Mängel.

2.2.1.2 Reaktive Maßnahmen nach § 8b BSI-Gesetz: Erkenntnisse aus Meldungen von KRITIS-Betreibern

Mit dem IT-Sicherheitsgesetz wurde im Jahr 2015 in § 8b Abs. 4 BSI-Gesetz eine Meldepflicht für Betreiber Kritischer Infrastrukturen eingeführt. Im Berichtszeitraum gingen beim BSI 419 entsprechende Meldungen ein, die Verteilung auf die KRITIS-Sektoren zeigt Tabelle 1.

Energie	Ernährung	Finanzen u. Versicherungen	Gesundheit	IT+TK ⁸	Kerntechn. Anlagen	Transport & Verkehr	Wasser	Summe
73	9	65	134	75	0	56	7	419

Tabelle 1 Meldungszahlen nach KRITIS-Sektoren im Berichtszeitraum

Die Gefährdungslage im Bereich Kritische Infrastrukturen liegt weiterhin auf hohem Niveau. Im Berichtszeitraum gab es jedoch keine Bedrohungen, die sich ausschließlich gegen Kritische Infrastrukturen gerichtet haben.

Die im Berichtszeitraum eingegangenen Meldungen und deren Art zeigen gerade für die Branche Elektrizität deutlich, wie sehr sie im Fokus von Angreifern steht und wie diese ver- suchen, in interne IT-Systeme einzudringen. Als Methoden dafür beobachteten die Betreiber verstärkt aktives Scanning, um vorhandene Schwachstellen in den direkt mit dem In- ternet verbundenen Systemen zu finden und diese gegebe- nenfalls auszunutzen. Auch das Abgreifen von Zugangs- und Kontaktdaten über das Ausspähen von mit der Elektrizitäts- branche verbundenen Dritten wurde beobachtet.

Im Berichtszeitraum gab es in den Sektoren Energie und Wasser mehrere Vorfälle, die auf Störungen in für den Betrieb der Kritischen Infrastrukturen notwendigen Steue- rungskomponenten zurückzuführen waren. Die Störungen mussten mit teilweise erheblichem Aufwand, mitunter über einen Monat hinweg, behoben werden. Aufgrund der Umsicht und den vorhandenen Redundanzen bei den Betreibern kam es in keinem der Vorfälle zu einer Ver- sorgungsunterbrechung. Da Funktionsstörungen in den Komponenten nur in Kooperation mit den Herstellern und Dienstleistern behoben werden können, zeigen diese Vorfälle jedoch deutlich, wie wichtig es ist, dass hier alle Beteiligten am gleichen Strang ziehen, um einen größtmög- lichen Schutz zu realisieren.

Im Sektor Gesundheit entfielen die meisten Meldungen auf ein technisches Versagen, gefolgt von Cyber-Angriffen, Ausfall externer Dienste und Anwendungs- bzw. Konfigu- rationsfehler. Im Sektor Transport und Verkehr handelte es sich bei den eingegangenen Meldungen nicht um IT-Sicherheitsvorfälle, sondern um die Anzeige von tech- nischen IT-Störungen. Auch im Sektor Ernährung lassen sich die meisten gemeldeten IT-Störungen Kritischer Infrastrukturen auf ein technisches Versagen insbesonde- re der Stromversorgung zurückführen.

Im Sektor Finanzen und Versicherungen führten DDoS- Angriffe auf IT-Infrastrukturen und Online-Dienste von Banken im ersten Quartal 2020 zu Störungen im Zah- lungsverkehr. Es kam an mehreren Tagen zu gezielten An- griffen, in deren Verlauf wechselnde bzw. weiterentwickel- te Angriffsmuster zu verzeichnen waren. Maßnahmen zur DDoS-Mitigation zeigten anfangs nur eine eingeschränkte

Wirkung. Durch Hinzunahme weiterer Maßnahmen, u. a. gegen Angriffe auf der Netzwerk- und der Anwendungse- bene, war eine erfolgreiche Abwehr möglich und weitere Angriffe blieben aus.

Generell zeigt sich das Bild, dass die meisten gemeldeten Vorfälle durch den Ausfall von IT-Infrastruktur hervorgerufen wurden. So entfallen beispielsweise 2019 im Sektor Finanzen und Versicherungen nahezu drei von vier Meldungen auf technisches Versagen, etwas mehr als ein Zehntel der Meldungen auf organisatorische Ursachen und etwas weniger als ein Zehntel auf das Versagen genutzter Infrastruktur. Lediglich ein Zwanzigstel der Meldungen erfolgten auf Grund eines technischen Angriffes. Bei den Angriffen stehen sektorübergreifend DDoS-Angriffe und Ransomware-Vorfälle im Vordergrund.

Unterstützung der KRITIS-Betreiber bei der Krisenbewältigung

Die COVID-19-Pandemie stellt für KRITIS-Betreiber eine besondere Herausforderung dar, da sie auch in Krisenzeiten die Versorgung der Bevölkerung mit den kritischen Dienstleistungen aufrechterhalten müssen. Viele Betreiber baten daher BSI um Bescheinigungen, um nachweisen zu können, dass sie Kritische Infrastrukturen betreiben. Das BSI hat allen registrierten Betreibern entsprechende Bescheinigungen ausgestellt.

Das Pandemiegeschehen führt zu neuen Situationen, die auch für den Bereich Cyber-Sicherheit eine Herausforderung darstellen. So verlegen viele Menschen ihren Arbeitsplatz in die eigene Wohnung, und der Staat hat für viele Berufsgruppen Soforthilfen angeboten, die über das Internet beantragt werden müssen. Das BSI hat verschiedene Warnmeldungen, Hintergrundinformationen und Management-Informationen zur Lage verschickt, u. a. zu strategischen Auswirkungen der COVID-19-Pandemie auf die IT-Sicherheitslage in Deutschland, Hinweise zum sicheren mobilen Arbeiten oder zu möglichen Gefährdungen bei der Nutzung von COVID-19-Soforthilfe-Antragsseiten.

Die Krisensituation beeinträchtigt auch die Umsetzung des BSI-Gesetzes durch die KRITIS-Betreiber. So sind beispielsweise aufgrund von Reise- und Kontaktbeschränkungen Vor-Ort-Prüfungen bei Betreibern nicht durchführbar. Das BSI hat daher das Mahnwesen für die Betreiber ausgesetzt, deren Nachweistermine in den Monaten März bis Juli 2020 liegen, und nimmt dieses erst fünf Monate später wieder auf. Hierdurch können die Betreiber ihre Ressourcen auf die Bewältigung der Krise und die Bereitstellung der kritischen Dienstleistungen konzentrieren.

2.2.2 UP KRITIS

Die Initiative zur Zusammenarbeit von Wirtschaft und Staat zum Schutz Kritischer Infrastrukturen in Deutsch-

land *UP KRITIS* (vgl. *Quellenverzeichnis*²⁷: www.upkritis.de) ist eine öffentlich-private Kooperation zwischen den Betreibern Kritischer Infrastrukturen (KRITIS), deren Verbänden und den zuständigen staatlichen Stellen. Im Mai 2020 nahmen 700 Organisationen am *UP KRITIS* teil.

Der *UP KRITIS* hat das Ziel, die Versorgung mit Dienstleistungen Kritischer Infrastrukturen in Deutschland aufrecht zu erhalten. Da Kritische Infrastrukturen immer mehr auf Informations- und Kommunikationstechnik (IT&TK) angewiesen sind, ist dieser Bereich ein zentraler Aufgabenschwerpunkt. Der *UP KRITIS* behandelt aber auch Themen, die über den Fokus auf IT&TK hinausgehen. Für einen umfassenden Schutz der Kritischen Infrastrukturen müssen physischer Schutz und IT-Sicherheit gemeinsam bedacht werden, was auch die COVID-19-Pandemie gezeigt hat.

Inhaltlich wird im *UP KRITIS* unter anderem an Themen zum Risikomanagement und Krisenmanagement gearbeitet. Diese Arbeiten finden insbesondere in den Themen- und Branchenarbeitskreisen des *UP KRITIS* statt. Dort entstehen beispielsweise Positionspapiere oder branchenspezifische Sicherheitsstandards. So veröffentlichte der Themenarbeitskreis Anforderungen an Lieferanten und Hersteller eine aktualisierte Version seines Papiers „Best-Practice-Empfehlungen für Anforderungen an Lieferanten zur Gewährleistung der Informationssicherheit in Kritischen Infrastrukturen“ und ein Security Level Agreement, das aus Arbeiten im Branchenarbeitskreis Medien hervorging und KRITIS-Betreibern eine Vorlage zur Vereinbarung der erforderlichen Qualität und IT-Sicherheit von Arbeitsprozessen zwischen Lieferanten und Betreibern anbietet.

Am *UP KRITIS* teilnehmende Organisationen haben sich darauf verständigt, sich untereinander zur aktuellen Bedrohungslage auszutauschen. Hierzu werden die Branchenarbeitskreise im *UP KRITIS* genutzt. Damit die Ergebnisse dieses Prozesses sektorübergreifend vergleichbar sind und kontinuierlich erfasst werden können, haben Teilnehmer des Themenarbeitskreises Operativer Informationsaustausch eine Risikomatrix entwickelt. Diese unterstützt die strukturierte Erfassung von Risiken, deren Darstellung und Bewertung sowie die Dokumentation des zeitlichen Verlaufs (vgl. Tabelle 2, Seite 56).

Die ersten Rückmeldungen aus neun Branchen zu den identifizierten Risiken wurden bereits ausgewertet, wobei sich zwei Themenschwerpunkte herauskristallisiert haben:

1. Schwachstellen / fehlende Sicherheits-Patches
2. *Advanced Persistent Threats* (APT)

Risikomatrix BAK Beispiel, Stand 02.04.2020	Brutto-Betrachtungen (ohne Maßnahmen)					Netto	
Bedrohung	Risiko Vormonat	Risiko-Trend	Eintrittswahrscheinlichkeit	Schadenspotenzial	Risiko	Einschätzung Verwundbarkeit	Bemerkung
	(ohne Maßnahmen)	(ohne Maßnahmen)	(gering / mittel / hoch / sehr hoch)	(gering / mittel / hoch / sehr hoch)	(ohne Maßnahmen)	(Verwundbarkeit nach Maßnahmen)	
Sektorübergreifende Bedrohungen (gemäß B3S-Orientierungshilfe A1)	aus Vormonat kopieren		ausfüllen	ausfüllen		ausfüllen	
Kategorie „Cyber-Angriffe“							
Hacking und Manipulation	kritisch		unwahrscheinlich	kritisch	mittel	unwahrscheinlich	Fokus: externe Angreifer
Schadprogramme	existenzbedrohend		sehr wahrscheinlich	existenzbedrohend	existenzbedrohend	sehr wahrscheinlich	Fokus: erfolgreiches Einnistern von Malware (beliebige Quelle)
Advanced Persistent Threat (APT)	existenzbedrohend		wahrscheinlich	existenzbedrohend	existenzbedrohend	wahrscheinlich	Fokus: gezielte, zeitl. ausgedehnte Angriffe gegen dedizierte Unternehmen (meist Wirtschaftsspionage, Wettbewerber)
Kategorie „Phishing“							
Identitätsmissbrauch (Phishing, Skimming, Zertifikatsfälschung)	kritisch		wahrscheinlich	mittel	mittel	unwahrscheinlich	Fokus: technische Angriffe mit dem Ziel Identitäten Dritter anzunehmen
Missbrauch (Innentäter)	kritisch		unwahrscheinlich	existenzbedrohend	kritisch	wahrscheinlich	Fokus: bewusste Handlungen von (unzufriedenen) Mitarbeitern
Social Engineering (Phishing, Vishing (Voice-Phishing))	mittel		unwahrscheinlich	mittel	mittel	unwahrscheinlich	Fokus: Angriffe gegen Personen, um Informationen über Dritte und Org.-Einheiten zu erhalten
Kategorie „Prozess-Schwächen“							
Abhängigkeiten von Dienstleistern und Herstellern (Ausfall externer Dienstleister)	mittel		wahrscheinlich	mittel	mittel	unwahrscheinlich	Fokus: dedizierte Lieferanten (z. B. im Umfeld Production-IT, NLT) sowie Partner, Cloud-Dienstleister usw.
Unbefugter Zugriff	existenzbedrohend		wahrscheinlich	existenzbedrohend	existenzbedrohend	wahrscheinlich	Fokus: Schwachstellen in Berechtigungs- und Zugriffs-Management (inkl. organisat. Prozesse)
Schwachstellen / fehlende Sicherheits-Patches	kritisch		sehr wahrscheinlich	mittel	kritisch	wahrscheinlich	Fokus: System- und Anwendungssicherheit inkl. Patch-Management-Prozess
Kategorie „Angriffe gegen Verfügbarkeit“							
Manipulation, Diebstahl, Verlust, Zerstörung von IT oder IT-relevanten Anlagen und Anlagenteilen	kritisch		unwahrscheinlich	kritisch	mittel	unwahrscheinlich	Fokus: NLT, PLT, Fernwirktechnik, Router, Modems auf Anlagen sowie IT im RZ und Endgeräte
Gezielte Störung / Verhinderung von Diensten (DDoS, gezielte Systemabstürze, ...)	mittel		unwahrscheinlich	mittel	mittel	sehr unwahrscheinlich	Fokus: externe (Überlast-)Angriffe gegen IT-Systeme / Applikationen
Beschädigung oder Zerstörung verfahrenstechnischer Komponenten, Ausrüstungen und Systemen	gering		wahrscheinlich	gering	gering	unwahrscheinlich	Fokus: Sabotage (physisch) von Anlagen „im Feld“ (Schaltanlagen, Trafostationen, Pumpen etc.)
Kategorie „Höhere Gewalt“							
Naturgefahren	gering		unwahrscheinlich	mittel	mittel	unwahrscheinlich	Fokus: Gefahren speziell für Systeme, Anlagen, Standorte, die zur Erbringung des Geschäfts notwendig sind (z. B. RZ-Standorte, Stromtrassen, Kläranlagen usw.)
Weitere übergreifende Bedrohungen (z. B. aus aktuellen Anlässen, sofern diese oben nicht zugeordnet werden können)							
Fehlendes Personal (z. B. Krankheit, Fluktuation, Umstrukturierung, Bereitstellung Ressourcen)	kritisch		wahrscheinlich	kritisch	kritisch	wahrscheinlich	Fokus: Betriebs- und Sicherheitsprozesse können nicht aufrecht erhalten werden, auf Ereignisse / Vorfälle kann nicht angemessen reagiert werden
Branchenspezifische Bedrohungen (Strom, Wasser, Gas, TK usw.)							
Firmware-Angriffe auf Spezialsysteme	gering		unwahrscheinlich	kritisch	mittel	unwahrscheinlich	
Manipulation von produzierten Systemen	kritisch		wahrscheinlich	kritisch	kritisch	unwahrscheinlich	
Manipulation eingehender Datenströme	mittel		sehr unwahrscheinlich	existenzbedrohend	mittel	wahrscheinlich	

Tabelle 2 Risikomatrix (mit beispielhaften Werten), Quelle: UP KRITIS

Aus diesen Ergebnissen wird beispielsweise geschlossen, dass sich der UP KRITIS noch intensiver mit dem Thema Anforderungen an Lieferanten und Hersteller beschäftigen muss. Ein Arbeitskreis zu diesem Thema besteht im UP KRITIS bereits. Auch das Thema APT wird bereits im UP KRITIS diskutiert. Hier wird die Gründung eines Themenarbeitskreises Detektion angestrebt, um die frühzeitige Erkennung von APT-Angriffen zu fördern.

2.2.3 Zertifizierung intelligenter Messsysteme im Energiebereich

Das BSI hat die technische Möglichkeit zum Einbau intelligenter Messsysteme festgestellt und damit die Freigabe für den Rollout von intelligenten Messsystemen mit Bekanntgabe zum 24. Februar 2020 erteilt. Damit wird ein wichtiger Meilenstein für die Digitalisierung der Energiewende erreicht.

Nach der Veröffentlichung der zweiten Marktanalyse des BSI am 31. Januar 2020 sind nun die Voraussetzungen zum Einbau von intelligenten Messsystemen erfüllt, da drei Smart-Meter-Gateway-Hersteller das Produkt-Zertifizierungsverfahren des BSI erfolgreich abgeschlossen haben.

Zunächst müssen Messstellenbetreiber die etwa vier Millionen Stromkunden mit einem intelligenten Messsystem ausstatten, die einen Jahresstromverbrauch zwischen 6.000 kWh und 100.000 kWh haben. Dafür haben die Messstellenbetreiber nach Feststellung der technischen Möglichkeit insgesamt acht Jahre Zeit, also bis 2028. Mindestens zehn Prozent dieser Pflichteinbautfälle müssen jedoch innerhalb der ersten drei Jahre mit einem intelligenten Messsystem ausgestattet werden. Bei einem Jahresstromverbrauch von weniger als 6.000 kWh ist der Einbau optional, wobei die Entscheidung über einen Einbau beim sogenannten grundzuständigen Messstellenbetreiber liegt (standardmäßig der Stromnetzbetreiber). Dezentrale Erzeugungsanlagen (sogenannte EEG- und KWKG-Anlagen) und flexible Verbraucher (sogenannte steuerbare Verbrauchseinrichtungen nach § 14a Energiewirtschaftsgesetz) müssen zunächst nicht ausgestattet werden, da das Bundeswirtschaftsministerium hierzu Anpassungen des Rechtsrahmens für 2020 angekündigt hat.

Durch die Verwendung von intelligenten Messsystemen – und der damit einhergehenden Nutzung von zertifizierten Smart-Meter-Gateways – werden zukünftig wichtige Systeme des Energienetzes über eine sichere Kommunikationsinfrastruktur vernetzt. Zugleich wird Cyber-Angriffen auf solche Systeme wirksam begegnet. Durch den Einsatz von Smart-Meter-Gateways können Netzzustandsdaten erhoben werden, sodass Transparenz über die Leistungsflüsse im Verteilnetz entsteht. Zudem können flexible Verbrauchseinrichtungen (Wärmepumpen, Elektromobile usw.) und dezentrale Erzeugungsanlagen zukünftig über das Smart-Meter-Gateway gesteuert und somit netz- und marktdienlich eingesetzt werden. Nur wenn dezentrale Erzeugungs- und Verbrauchsanlagen über das Smart-Meter-Gateway gesteuert werden, kann der Anteil erneuerbarer Energien in den Netzen weiter erhöht und beispielsweise die für die Elektromobilität notwendige Ladeinfrastruktur ohne einen umfangreichen und kostenintensiven Netzausbau integriert werden.

Mit dem Einbau von intelligenten Messsystemen wird daher ein wesentlicher Beitrag geleistet, um die Klima- und Energiewendeziele zu erreichen. Gemeinsam mit dem Bundeswirtschaftsministerium hat das BSI bereits 2019 eine Standardisierungsstrategie zur sektorübergreifenden Digitalisierung der Energiewende erarbeitet

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

2.2.4 Moderne Telekommunikationsinfrastrukturen (5G)

Die Digitalisierung ermöglicht höhere Geschwindigkeit, Effizienz und Effektivität in wirtschaftlichen und behördlichen Abläufen sowie mehr Komfort und Bequemlichkeit im privaten Bereich. Eine technologische Basis dieser Entwicklungen ist der Mobilfunkstandard 5G, der schnellere Verbindungen, weniger Latenzzeit und höhere Datenraten ermöglichen soll. Die neue 5G-Technologie wird gemeinhin als entscheidender Faktor für die positive Entwicklung des Standorts Deutschland in den kommenden Jahren angesehen. Aufgabe des BSI ist es, die Voraussetzungen dafür zu schaffen, dass die 5G-Netze das höchstmögliche Niveau an Vertraulichkeit, Integrität und Authentizität erreichen. Basis für den Aufbau sicherer 5G-Netze ist aktuell der Katalog von Sicherheitsanforderungen, den die Bundesnetzagentur gemeinsam mit dem BSI und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) auf Grundlage der Bestimmungen von § 109 TKG aktualisiert hat und der für die neu aufzubauenden 5G-Netze zur Anwendung kommen wird. Neben der Überarbeitung des Sicherheitskatalogs für Netzbetreiber und Diensteanbieter wurden auch erste Vorgaben zur Zertifizierung von Netzkomponenten erarbeitet und auf europäischer und internationaler Ebene diskutiert.

Sicherheitskatalog

Das Telekommunikationsgesetz (TKG) definiert die gesetzlichen Rahmenbedingungen für Betreiber von Telekommunikationsnetzen. Für die IT-Sicherheit ist dabei vor allem § 109 Abs. 6 des TKG relevant, der die nationalen Sicherheitsanforderungen an die Telekommunikationsinfrastrukturen in Form des sogenannten Sicherheitskatalogs regelt. Der Katalog wurde im Einvernehmen mit dem BSI und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit durch die Bundesnetzagentur erstellt und laufend an die technischen und regulatorischen Rahmenbedingungen angepasst. Im Rahmen dieser regelmäßigen Überarbeitung und Aktualisierung des Sicherheitskatalogs wurde vor allem dem neuen Mobilfunkstandard 5G Rechnung getragen und der Katalog um eine zweite Anlage mit

zusätzlichen Sicherheitsanforderungen für öffentliche Telekommunikationsnetze und -dienste mit erhöhtem Gefährdungspotenzial ergänzt.

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

Zertifizierungsstrategie

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

Ausgangspunkt für die Produktzertifizierung ist das von der Global System for Mobile Communications Association (GSMA) entwickelte Prüf- und Auditierungsschema Network Equipment Security Assurance Scheme (NESAS). Zusammen mit der GSMA entwickelt das BSI derzeit das NESAS-Schema mit dem Ziel weiter, dieses als europäisches Zertifizierungsschema im Gesetzespaket zur Cyber-Sicherheit Cybersecurity Act zu verankern und weitere Prüfanforderungen wie etwa einen sicheren Produktlebenszyklus inkl. Supply-Chain-Betrachtung in den Standard zu integrieren. Entsprechend der Technologie- und Marktentwicklung soll zu einem späteren Zeitpunkt die Produktzertifizierung um die Schemata Beschleunigte Sicherheitszertifizierung (BSZ) und Common Criteria⁹ (CC) ergänzt werden. Ziel ist, dass für ausgewählte, kritische Netzfunktionen Schutzprofile nach CC erarbeitet und europäisch harmonisiert bzw. standardisiert werden.

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

Die im Rahmen der 5G-Zertifizierungsstrategie ausgewählten Schemata zur Produkt- und Systemzertifizierung sollen in einer Technischen Richtlinie des BSI zusammengefasst werden, auf die im Sicherheitskatalog verpflichtend verwiesen wird. Die Technische Richtlinie wird bis Ende 2020 durch das BSI veröffentlicht und fortlaufend gepflegt.

Europäische Harmonisierung

Auf europäischer Ebene wird die Einführung von Netztechnik der 5. Generation als wichtige Voraussetzung für künftige digitale Dienste in einem digitalen Binnenmarkt gesehen. Dabei empfiehlt die Kommission ein abgestimmtes Vorgehen bei der Sicherheit von 5G-Netzen und veröffentlicht in ihrer Empfehlung Cyber-Sicherheit der 5G-Netze ((EU) 2019/534 vom 26. März 2019) einen Fahrplan zur Erarbeitung einer europaweiten Toolbox von Maßnahmen zur Erhöhung der Sicherheit in 5G-Telekommunikationsnetzen. Zu diesen Maßnahmen gehören insbesondere die Einrichtung einer Kooperationsgruppe, die Erstellung einer koordinierten europäischen Risikobewertung sowie die Entwicklung eines harmonisierten Maßnahmenkatalogs zur Bewältigung der identifizierten Risiken.

Die Kooperationsgruppe wurde bereits im April 2019 als Arbeitsgruppe zu 5G (auch NIS 5G Workstream genannt) unter dem Dach der NIS Cooperation Group eingerichtet. Das BSI beteiligt sich von Anfang an an dieser Arbeitsgruppe. Insbesondere setzt sich das BSI dafür ein, geeignete Zertifizierungsschemata (z. B. das oben genannte NESAS-Schema) als europäische Zertifizierungsschemata einzuführen. Bisher verfügbare Ergebnisse der Arbeitsgruppe sind die beiden Publikationen CG Publication 02/2019 - Risk assessment of 5G networks vom 9. Oktober 2019 und CG Publication 01/2020 - Cybersecurity of 5G networks: EU toolbox of risk mitigating measures vom 29. Januar 2020.

2.2.5 IT-Sicherheit in intelligenten Verkehrssystemen (C-ITS)

Fahrerassistenzsysteme

Fahrerassistenzsysteme befinden sich in nahezu allen im Straßenverkehr teilnehmenden PKWs. Angefangen vom ABS bis hin zum automatischen Notbremsassistenten werden in modernen Autos immer mehr Aufgaben von der Fahrerin oder dem Fahrer an das Fahrzeug abgegeben, sodass das Fahrzeug selbstständig Fahrbefehle ausführen kann. Fahrerassistenzsysteme sind ein Zwischenschritt auf dem Weg zum automatisierten Fahren. Das BSI führt sog. Spoofing-Angriffe, das heißt Täuschungsmanöver auf optische Fahrerassistenzsysteme durch, um die Robustheit aktueller Systeme gegenüber praktischen Angriffen zu untersuchen und Hinweise auf Verbesserungspotenziale aufzuzeigen.

Damit ein Fahrerassistenzsystem auf Basis einer Vielzahl von internen und externen Sensorinformationen relevante Informationen über den Zustand des Fahrzeugs und der Umwelt extrahieren kann, um hieraus Entscheidungen

abzuleiten, werden häufig Verfahren aus dem Gebiet der Künstlichen Intelligenz (KI) verwendet. Ein Beispiel hierfür ist die Detektion von Verkehrsschildern, bei welcher mit Hilfe eines tiefen neuronalen Netzes die Positionen und Arten der sich im Bild befindlichen Verkehrsschilder erkannt werden. Diese oft höchst komplexen Systeme gehen jedoch i. d. R. damit einher, dass sie äußerst schwer zu interpretieren und qualitativ neuen Angriffen ausgesetzt sind. So ist es beispielsweise möglich, mit einem speziellen, unscheinbaren Sticker, der auf ein Verkehrsschild geklebt wird, die Entscheidung des KI-Systems komplett zu verändern. Das BSI betreut mehrere Abschlussarbeiten im Kontext dieser Problematiken und engagiert sich bei der Erstellung von möglichen Kriterien und Methoden zur Überprüfung dieser Systeme in der Arbeitsgruppe KI, zwischen dem BSI und dem Verband der TÜV.

Fahrzeug-zu-X-Kommunikation

Die Fahrzeug-zu-Fahrzeug- bzw. Fahrzeug-zu-Infrastruktur-Kommunikation für kooperative intelligente Transportsysteme wird ab 2020 in den Markt eingeführt. Um eine europaweit interoperable sichere Kommunikation zu ermöglichen, baut die EU-Kommission derzeit die zentralen Instanzen der hierfür vorgesehenen *Public-Key*-Infrastruktur auf. In einer vom Trust List Manager der EU-Kommission bereitgestellten European Certificate Trust List werden die vertrauenswürdigen Wurzelzertifizierungsstellen (Root Certification Authorities) der Verkehrsinfrastrukturbetreiber in den einzelnen Mitgliedsländern und der Automobilhersteller verzeichnet. Das BSI hat an der Spezifikation der Prozesse und Protokolle der zentralen Stellen im Rahmen einer Arbeitsgruppe bei der EU-Kommission mitgewirkt.

Auch auf nationaler Ebene sollen die vorgesehenen *Public-Key*-Infrastruktur-Instanzen (PKI-Instanzen) für Verkehrsinfrastrukturkomponenten (Road Side Units) ab 2020 für einen ersten Produktivbetrieb bereitgestellt werden. Das BSI unterstützt das Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) und die Verkehrsinfrastrukturbetreiber bei der Festlegung der organisatorischen und technischen Vorgaben für diese Systeme.

Im vergangenen Jahr wurde ein erstes Schutzprofil aus dem Kontext kooperativer intelligenter Verkehrssysteme auf Grundlage der Common Criteria beim BSI zertifiziert. Das „Protection Profile for a Road Works Warning Gateway“ legt IT-Sicherheitsanforderungen an eine elektronische Komponente für fahrbare Absperrtafeln an Autobahnen fest, die im Rahmen der Fahrzeug-zu-Infrastruktur-Kommunikation Warnnachrichten an herannahende Fahrzeuge verschicken und umgekehrt auch Statusinformationen der einzelnen Fahrzeuge empfangen können. Die Informationen sollen zur Erstellung von lokalen Verkehrslagebildern verwendet werden.

2.2.6 Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme

Im Zuge der Digitalisierung werden Geschäftsvorfälle heutzutage immer häufiger elektronisch erfasst. Die Nutzung unterschiedlichster Arten von Registrierkassen prägt den Kassenmarkt für den Einzelhandel deutlich. Von der klassischen Kasse über Tablets und Smartphones hin zu Kassen in Serverfarmen sind alle erdenklichen Typen vertreten. Hierdurch haben sich die technischen Herausforderungen für die Steuerprüfung stark verändert, insbesondere 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. Dafür enthält die technische Sicherheitseinrichtung ein Sicherheitsmodul, das gewährleistet, dass Aufzeichnungen nicht nachträglich unerkannt geändert, gelöscht oder erzeugt werden können.

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

Die technischen Anforderungen und Prüfvorschriften an die Komponenten der technischen Sicherheitseinrichtung ergeben sich aus der Abgabenordnung und werden vom BSI im Auftrag des Bundesministeriums der Finanzen (BMF) in Technischen Richtlinien und Schutzprofilen festgelegt. Dies ist in der Abgabenordnung (dem elementaren Gesetz des deutschen Steuerrechts) festgelegt und die Erstellung der Vorgaben geschieht daraus folgend im Auftrag des BMF.

Die Technischen Richtlinien und Schutzprofile wurden in Abstimmung mit einschlägigen Fachverbänden und Herstellern zeitgerecht 2018 fertiggestellt und veröffentlicht.

Weiterhin hat das BSI im Rahmen einer Übergangsregelung für das Jahr 2019 den Herstellern ermöglicht, einen Teil der zeitaufwändigen Sicherheitszertifizierung durch ein positives Gutachten des BSI zu ersetzen, um auf diese Weise möglichst frühzeitig technische Sicherheitseinrichtungen auf dem Markt verfügbar zu machen. Technische Sicherheitseinrichtungen dürfen unter dieser Übergangsregelung für ein Jahr ab Ausstellung des Gutachtens ins Feld gebracht werden.

Vier technische Sicherheitseinrichtungen haben die Zertifizierung unter Nutzung der Übergangsregelung bereits erfolgreich bestanden und sind auf dem Markt verfügbar.

2.2.7 Zertifizierung

Das BSI bietet im Rahmen seiner Dienstleistungen unterschiedliche Zertifizierungsverfahren an. Zu den etablierten Verfahren im Bereich der Produktzertifizierung zählt die Zertifizierung nach Common Criteria (ISO/IEC 15408). Ferner können Produkte auch nach den Technischen Richtlinien des BSI zertifiziert werden. Im Bereich der Managementsysteme erlaubt der ebenfalls seit Jahren praktizierte Grundschutz-Standard die Zertifizierung eines Information Security Management System (ISMS).

Zertifizierung nach Common Criteria (ISO/IEC 15408)

Die Zertifizierung der IT-Sicherheit eines Produktes durch das BSI bedeutet: Es wurde auf Basis öffentlicher Prüfkriterien und in einem transparenten Prozess von einer unabhängigen Partei geprüft (vgl. *Quellenverzeichnis*²⁸: www.bsi.bund.de).

Beschafferinnen und Beschaffer entnehmen einem Zertifikat des BSI:

- Transparenz über die Wirksamkeit der Sicherheitsleistung
- Entscheidungshilfe für die Nutzbarkeit des Produktes
- Vergleichbarkeit der Sicherheitsleistung
- Konformität mit internationalen oder nationalen Standards.

Die Prüfkriterien Common Criteria, die seinerzeit von den am internationalen Abkommen Common Criteria Recognition Agreement (CCRA, vgl. *Quellenverzeichnis*²⁹: www.commoncriteriaportal.org) beteiligten Nationen erstellt und gepflegt wurden, wurden von der Internationalen Standardisierungsorganisation ISO übernommen. Derzeit wird der Standard aktualisiert und erwei-

tert. Das BSI arbeitet mit Expertinnen und Experten aus Prüfstellen und der Industrie über das Deutsche Institut für Normung (DIN) an diesem Programm mit. Ziel ist, sowohl die Konzepte zur Spezifikation der Sicherheitsanforderungen als auch die Evaluierungsmethodik zu erweitern, um die Anwendbarkeit des Standards für neue Technologien zu verbessern.

Die EU-Kommission hat sich im Rahmen der Förderung von Cyber-Sicherheit in Europa des Themas Zertifizierung angenommen. Das Gesetzespaket zur Cyber-Sicherheit (Cybersecurity Act), in dem auch ein EU-weites IT-Sicherheitszertifizierungsmodell verankert ist, trat am 27. Juni 2019 in Kraft. Die EU-Mitgliedstaaten haben mit SOGIS-MRA bereits ein starkes, eingespieltes Zertifizierungskonzept in Verwendung, das aktuell unter dem neuen EU-Dach verankert wird.

Die Forderung nach zertifizierten Produkten wurde in den letzten Jahren auch in zahlreichen Gesetzen und Verordnungen verankert. Vielfach betrifft dies die Digitalisierungsprojekte der Bundesregierung zum Beispiel in den Bereichen des Einsatzes digitaler Technologien im Gesundheitswesen (eHealth), Hoheitliche Dokumente, Intelligente Messsysteme (Smart Metering), Digitale Signaturen und seit neuestem auch im Bereich der Registrierkassen, um den Schutz vor Manipulation an digitalen Grundaufzeichnungen sicherzustellen.

Die Durchführung der Produktzertifizierung wird durch Schutzprofile (Protection Profiles, PP) unterstützt. Sie beschreiben einen Standard an Sicherheitsanforderungen für einen bestimmten Produkttyp. Beispiele für neue Schutzprofile sind:

- PP Cryptographic Service Provider Light (CSPL), eingesetzt z. B. in elektronischen Kassensystemen
- PP Roadworks Warning Unit, eingesetzt um vor herannahendem Verkehr vor einer Straßenbaustelle zu warnen

Zertifizierung nach Technischen Richtlinien

Funktionalität und Interoperabilität als Produkteigenschaft werden im Rahmen der Technischen Richtlinien des BSI durch funktionale Anforderungen als Standard beschrieben und können danach implementiert werden. Die Konformität eines IT-Produkts oder -Systems mit einer TR kann dann durch das BSI mit einem Zertifikat bestätigt werden.

Im Zuge dieses Verfahrens wird von einer neutralen Prüfstelle eine Konformitätsprüfung auf Grundlage der in der TR definierten Prüfspezifikationen durchgeführt. Die Prüfung wird von der zuständigen Zertifizierungsstelle

im BSI überwacht und nach erfolgreichem Abschluss mit einem Konformitätsbescheid und einem Zertifikat bestätigt. Die Zertifizierungsstelle ist für einige TRs durch die Deutsche Akkreditierungsstelle (DAkkS) akkreditiert.

Zertifizierung eines ISMS nach BSI-Grundschutz

Neben der Produktzertifizierung wird auch eine Zertifizierung von Managementsystemen angeboten, die an die weit verbreitete Zertifizierung nach ISO/IEC 27001 angelehnt ist und auf Basis des im BSI entwickelten IT-Grundschutzes durchgeführt wird. Die Vorgehensweise nach IT-Grundschutz und die im IT-Grundschutz enthaltenen Empfehlungen von Standard-Sicherheitsmaßnahmen stellen inzwischen einen De-Facto-Standard für IT-Sicherheit dar.

Zertifizierung in Zahlen

Im Rahmen der Common Criteria-Zertifizierung beim BSI wurden im Berichtszeitraum insgesamt 63 Produkt-, 25 Standort- und 9 Schutzprofilzertifikate ausgestellt.

Außerdem wurden 77 Verfahren nach Technischen Richtlinien in 12 Prüfbereichen abgeschlossen, wobei 47 Erst- und Rezertifizierungen, 23 Maintenance-Verfahren sowie 7 Überwachungsaudits durchgeführt wurden.

Im Bereich des IT-Grundschutzes wurden im Berichtszeitraum insgesamt 112 Verfahren erfolgreich abgeschlossen, davon waren 43 ISO 27001 Zertifikate auf Basis von IT-Grundschutz, zusätzlich wurden 69 Überwachungsaudits durchgeführt.

Im internationalen Vergleich liegt das BSI seit Jahren immer unter den Top 5 der CCRA-Zertifizierungsnationen mit den meist ausgestellten Zertifikaten.

2.2.8 IT-Grundschutzprofile und Testate

Der IT-Grundschutz ist seit über 25 Jahren ein bewährtes Angebot des BSI, das Unternehmen und Behörden nutzen können, um die Informationssicherheit in ihrer Institution zu erhöhen. Das umfangreiche Portfolio enthält Empfehlungen und Anforderungen zu allen Fragen der Informationssicherheit. Das Angebot richtet sich sowohl an Anwenderinnen und Anwender, die sich erstmalig mit IT-Grundschutz beschäftigen, als auch an fortgeschrittene Anwenderinnen und Anwender in Unternehmen und Behörden. Grundlegende Kenntnisse über Methoden und Vorgehensweisen vermitteln die BSI-Standards; mit den IT-Grundschutz-Bausteinen aus dem IT-Grundschutz-Kompendium kann gezielt daran gearbeitet werden, den Status der Informationssicherheit einer Institution zu verbessern.

IT-Grundschutz-Profile – Schablonen für Informationssicherheit

Seit 2018 bieten IT-Grundschutz-Profile als Muster für Sicherheitskonzepte einen erleichterten Einstieg in den IT-Grundschutz. Sie ermöglichen erste Schritte für den Aufbau eines ISMS sowie eines Sicherheitskonzepts. Ein IT-Grundschutz-Profil bildet als Schablone eine Referenzarchitektur eines bestimmten Anwendungsfalls ab.

Auf der BSI-Webseite sind zu den unterschiedlichsten Anwendungsgebieten und Branchen IT-Grundschutz-Profile veröffentlicht und können für eigene Sicherheitsbetrachtungen genutzt werden, zum Beispiel Handwerksbetriebe, Handwerkskammern, Hochschulen, Kommunalverwaltungen, Oberste Landesbehörden, Papierfabriken, Reedereien (Land- und Schiffsbetriebe).

IT-Grundschutz-Profile haben einen Revisionszyklus und werden regelmäßig, zum Beispiel aufgrund neuer Erkenntnisse oder auf Basis der jährlich aktualisierten Edition des IT-Grundschutz-Kompendiums, angepasst und überarbeitet

Zurzeit werden IT-Grundschutz-Profile für weitere Branchen erstellt. Das IT-Grundschutz-Referat des BSI veranstaltet gemeinsam mit der Allianz für Cyber-Sicherheit Workshops, um interessierte Anwenderinnen und Anwender bei der Erstellung eines neuen IT-Grundschutz-Profils zu unterstützen. Perspektivisches Ziel ist es, zu möglichst vielen Themen und für unterschiedliche Branchen IT-Grundschutz-Profile zu veröffentlichen, damit sich Anwenderinnen und Anwender dieser erprobten und praktikablen Arbeitshilfe bedienen können.

IT-Grundschutz-Testat nach der Basis-Absicherung

Die Vorgehensweise Basis-Absicherung nach IT-Grundschutz kann als schlanker Einstieg in den Aufbau eines ISMS in einer Institution dienen. Im Fokus der Sicherheitsbetrachtungen stehen die Basis-Anforderungen aus dem IT-Grundschutz-Kompendium, die eine grundlegende Erst-Absicherung über alle Geschäftsprozesse bzw. Fachaufgaben hinweg bieten. Die Umsetzung lässt sich mit einem vergleichsweise geringen finanziellen, personellen und zeitlichen Aufwand realisieren. Daher eignet sich die Basis-Absicherung besonders für kleine und mittlere Unternehmen (KMU) oder kleinere Kommunen, die einen ganzheitlichen Ansatz zum Aufbau eines ISMS verfolgen wollen.

Unternehmen und Behörden können mit einem Testat nach abgeschlossener Basis-Absicherung nachweisen, dass sie den IT-Grundschutz gemäß der gleichnamigen Absicherung umgesetzt haben. Mit diesem Testat kann eine Institution belegen, dass sie alle Geschäftsprozesse

bzw. Fachaufgaben, Daten und Komponenten des betrachteten Informationsverbundes unter technischen, infrastrukturellen, organisatorischen und personellen Aspekten mit einem Mindestmaß an Informationssicherheit abgesichert hat.

Die Standard- bzw. Kern-Absicherung aus dem IT-Grundschutz beinhaltet die Vorgehensweisen, die angestrebt werden sollten, um eine Institution angemessen und umfassend nach dem Stand der Technik zu schützen. Um dieses empfohlene Sicherheitsniveau gegenüber Dritten nachweisen zu können, kann ein ISO 27001-Zertifikat auf der Basis des IT-Grundschutzes erworben werden.

2.2.9 Unterstützung beim sicheren Umstieg ins Home-Office

Spätestens im März 2020 wurden die Auswirkungen der COVID-19-Pandemie auch in Deutschland für alle Teile der Gesellschaft spürbar. Um ihren Betrieb zumindest eingeschränkt aufrechterhalten zu können, verlegten viele Organisationen Arbeitsplätze kurzerhand ins Home-Office. Diese tiefgreifende Veränderung brachte zahlreiche Herausforderungen mit sich, da IT-Infrastrukturen signifikant angepasst werden mussten – einige Institutionen richteten Heimarbeitsplätze erstmalig ein.

Das BSI reagierte zeitnah auf diesen Bedarf und veröffentlichte am 18. März 2020 mit einer Pressemeldung erste Empfehlungen zum sicheren mobilen Arbeiten und weiteren Ausbau bereits vorhandener Home-Office-Infrastrukturen anhand der Top 5 Sicherheitsmaßnahmen (vgl. *Quellenverzeichnis*³⁰: www.bsi.bund.de). Den unterschiedlichen Zielgruppen aus der Verwaltung wurden zusätzlich durch die Sicherheitsberatung des BSI weitere Angebote zum sicheren mobilen Arbeiten im Home-Office zur Verfügung gestellt. Diese orientierten sich insbesondere an den unterschiedlichen Erfahrungs- und Umsetzungsgraden der Organisationen. So wurden Behörden mit verschiedenen Informationen gezielt bei der Absicherung bestehender und der Einrichtung neuer Home-Office-Arbeitsplätze beraten. Die besonderen Anforderungen hinsichtlich des erhöhten Schutzbedarfs der verarbeiteten Daten in dieser Zielgruppe fanden dabei stets Berücksichtigung.

Im Rahmen der Allianz für Cyber-Sicherheit wurde eine Online-Checkliste realisiert, die sich vor allem an die Unternehmen richtet, die bislang noch nicht mit dem Thema Home-Office in Berührung gekommen sind. „Home-Office? – Aber sicher!“ beinhaltet eine Liste mit kurzfristig realisierbaren, pragmatischen Lösungen, die einerseits die Arbeitsfähigkeit von Organisationen erhalten, gleichzeitig jedoch Vertraulichkeit, Verfügbarkeit und Integrität gewährleisten (vgl. *Quellenverzeichnis*³¹: www.bsi.bund.de). Gleichzeitig können Unternehmen mit Erfahrung im

Home-Office die Ausführungen nutzen, um bereits getroffene Maßnahmen zu überprüfen.

Alle Institutionen einte der verstärkte Bedarf an Videokonferenz-Lösungen. Um hier kurzfristig fundierte Empfehlungen geben zu können, wurde eine Task Force zu dem Thema gegründet. Zudem veröffentlichte das BSI am 14. April 2020 das „Kompendium Videokonferenzsysteme“. Hier finden Planer, Beschaffer, Betreiber, Administratoren, Revisoren und Nutzer Informationen, um den gesamten Lebenszyklus organisationsinterner Videokonferenzsysteme sicher zu gestalten (vgl. *Quellenverzeichnis*³²: www.bsi.bund.de).

Begleitet wurden die verschiedenen Empfehlungen zum sicheren mobilen Arbeiten im Home-Office durch anlassbezogene und zielgruppenspezifische Warnmeldungen zu den Gefährdungen, die im Rahmen der COVID-19-Pandemie auftraten (vgl. Kapitel *Gefährdungen der Cyber-Sicherheit durch die COVID-19-Pandemie*, Seite 33).

Es ist davon auszugehen, dass die Pandemie die Art, wie Institutionen arbeiten, nachhaltig verändern wird. Die COVID-19-Pandemie ist also auch eine Chance für die Digitalisierung der Arbeitswelt. Durch die zahlreichen Angebote des BSI konnten bereits jetzt verschiedene Zielgruppen mit operativen und strategischen Informationen versorgt, das Bewusstsein für Informationssicherheit im Home-Office geschaffen und auch die Zielgruppen des BSI durch individuelle Hilfestellungen unterstützt werden.

2.2.10 Allianz für Cyber-Sicherheit

Vor dem Hintergrund der ständig wachsenden Herausforderungen durch die zunehmende Digitalisierung schließen sich immer mehr Organisationen der Allianz für Cyber-Sicherheit an. In Kooperation mit mehr als 130 Partnern aus der Wirtschaft stellt das BSI auf dieser Plattform seit 2012 verschiedene Formate zum Austausch und Aufbau von IT-Sicherheits-Know-how zur Verfügung. Zu den kostenlosen Angeboten zählen u. a. Cyber-Sicherheits-Tage, Seminare und Empfehlungen.

In den vergangenen 12 Monaten registrierten sich über 900 weitere Organisationen bei der Initiative, um Zugriff auf die zahlreichen Angebote zu erhalten und in den Verteiler für Warnmeldungen des BSI aufgenommen zu werden. Mit mehr als 4.400 Mitgliedern ist die Allianz für Cyber-Sicherheit damit eine der größten Unternehmensgemeinschaften Deutschlands zum Thema Cyber-Sicherheit.

Um den registrierten Organisationen zielführende Handreichungen zu liefern, realisiert die Allianz für Cyber-Sicherheit regelmäßig neue Formate – insbesondere in Kooperation mit den Spitzenverbänden, die im Beirat der

Initiative vertreten sind. Hierzu zählte u. a. der mit Unterstützung der Deutschen Industrie- und Handelskammer am 26. September 2019 in Berlin ausgerichtete Cyber-Sicherheits-Tag, an dem mehr als 300 Mitglieder teilnahmen. Parallel wurde die Veranstaltung medial begleitet. Ein Video steht auf der Webseite Allianz für Cyber-Sicherheit (vgl. *Quellenverzeichnis*³³: www.allianz-fuer-cybersicherheit.de) zur Verfügung.

2.2.11 Dialog verschiedener Cyber-Sicherheitsinitiativen in Deutschland

Seit dem Jahr 2017 lädt das BSI deutsche Cyber-Sicherheitsinitiativen unter dem Dach der Allianz für Cyber-Sicherheit zum Dialog ein. Ziel ist es insbesondere, in gemeinsamen Projekten neue Angebote zur Förderung von Cyber-Sicherheit zu schaffen und diese durch abgestimmte Kommunikationsmaßnahmen möglichst vielen Interessenten zur Verfügung zu stellen.

Auch im aktuellen Berichtszeitraum blicken die Teilnehmer auf zahlreiche Kampagnen zurück. Der Schwerpunkt lag einerseits auf der Sensibilisierung von Mitarbeiterinnen und Mitarbeitern für den sicheren Umgang mit Informationstechnik (IT Security Awareness) und andererseits auf der Erhöhung der Cyber-Resilienz in Unternehmen. Eines der Ergebnisse dieser Arbeitsgruppen ist das Service-Paket: Einstieg ins IT-Notfallmanagement, das wesentliche Schritte zum eigenen Betriebskontinuitätsmanagement skizziert. Auf besonders großes Interesse innerhalb dieser Veröffentlichung stieß dabei die IT-Notfallkarte, die analog zum Schild „Verhalten im Brandfall“ am Arbeitsplatz eingesetzt werden kann und Handlungsanweisungen bei IT-Sicherheitsvorfällen aufzeigt. Weitere Informationen finden Sie auf der Webseite der Allianz für Cyber-Sicherheit (vgl. *Quellenverzeichnis*³³: www.allianz-fuer-cybersicherheit.de).

Charakteristisch für die Zusammenarbeit war einmal mehr die interdisziplinäre Zusammensetzung der Arbeitsgruppen: Hier kamen unterschiedliche Fähigkeiten und Hintergründe zusammen, sodass mit unterschiedlichen Blickwinkeln und Erfahrungen Projekte entwickelt und vorangetrieben werden konnten. Mit den vielfältigen Kompetenzen im Rücken war es unter anderem möglich, die ursprünglich nur für deutsche KMU konzipierte IT-Notfallkarte zu einer universell einsetzbaren Maßnahme weiterzuentwickeln. Durch das Engagement der Mitwirkenden ist nun ein Instrument entstanden, das sowohl in KMU als auch in Großkonzernen Anwendung findet. Durch die Übersetzung in zahlreiche Sprachen kann die IT-Notfallkarte auch im internationalen Kontext angewendet werden.

2.2.12 Sonstige Lösungen / Angebote für die Wirtschaft

Kriterienkatalog für die Sicherheit von Cloud-Diensten

Der Cloud Computing Compliance Criteria Catalogue (C5) ist ein Kriterienkatalog für die Sicherheit von *Cloud*-Diensten. Er dient sowohl Anbietern zum Beleg der Sicherheit ihrer *Cloud*-Dienste als auch Kunden, die auf der Grundlage des Prüfberichts ihr Risiko der *Cloud*-Nutzung steuern können.

Der C5 wurde 2016 vom BSI veröffentlicht und hat sich weltweit verbreitet. 2019 wurde er überarbeitet. Neben der BSI-internen Expertise haben dabei Anbieter, Anwender, Verbände und Prüfer in Feedbackworkshops ihre Erfahrungen und Anliegen beige-steuert. Leitendes Credo war, das gute Sicherheitsniveau zu erhalten oder zu erhöhen, aber dass diese Sicherheit auch umsetzbar bleiben und in ihrer Wirkung noch mehr bei den Kunden ankommen muss. Daneben waren neue Regelungen wie der EU Cybersecurity Act (EUCSA) zu berücksichtigen. Auf der Messe für IT-Sicherheit it-sa 2019 wurde schließlich der Entwurf des neuen C5:2020 zur Kommentierung veröffentlicht. Nach Berücksichtigung aller Kommentare wurde der neue C5:2020 am 21. Januar 2020 in Frankfurt am Main vor 90 Fachexpertinnen und -experten der Öffentlichkeit vorgestellt.

Der C5:2020 enthält unter anderem

- Den neuen Regelungsbereich Produktsicherheit; Ausgehend von Artikel 51 des EUCSA werden die Sicherheitsziele für *Cloud*-Services ausgestaltet.
- Den neuen Regelungsbereich zum Umgang mit staatlichen Ermittlungsanfragen; Der *Cloud*-Anbieter muss den Kunden nachweisen, dass Ermittlungsanfragen nach einem geregelten Prozess mit juristischer Prüfung erfolgen und nur solche Daten herausgegeben werden, bei denen die juristische Prüfung die Rechtmäßigkeit der Anfrage ergeben hat.
- Kriterien für korrespondierende Nutzerkontrollen; Alle C5-Berichte enthalten Angaben dazu, was der Kunde für die Sicherheit des *Cloud*-Dienstes beitragen muss – dies ist Ausdruck des Prinzips der geteilten Verantwortung. Im C5:2020 wird dieser Aspekt durch korrespondierende Kriterien adressiert. Diese geben zu jedem Kriterium für den *Cloud*-Anbieter an, ob der Kunde etwas dazu beitragen kann und worin dieser Beitrag – allgemein betrachtet – besteht. Dies muss aber in jedem Einzelfall durch anwendungsfall-spezifische Maßnahmen konkretisiert werden.

Ein C5-Bericht bietet jeder Kundin und jedem Kunden eine aussagekräftige Grundlage für das eigene Risikomanagement, die jede Vertragsverhandlung zwischen Anbieter und Kunde bei Sicherheitsfragen katalysiert. Mit den Verbesserungen im neuen C5:2020 wird die Sicherheit im *Cloud Computing*, die ein wesentlicher Teil der Informationssicherheit einer modernen Digitalisierung ist, für Staat, Wirtschaft und Gesellschaft weiter ausgestaltet und damit voran getrieben.

Investitionsprüfung

Das BSI wird vom BMI bei Verfahren zur Prüfung von Investitionen durch ausländische Investoren in inländische Unternehmen und Produktionsstätten nach §§ 4ff. des Außenwirtschaftsgesetzes (AWG) bzw. §§ 55ff. und §§ 60ff. der Außenwirtschaftsverordnung (AWV) im Rahmen seiner Zuständigkeit beteiligt.

Prüfungsmaßstab ist hierbei, ob wesentliche Sicherheitsinteressen, die öffentliche Ordnung oder die Sicherheit der Bundesrepublik Deutschland durch den beabsichtigten Erwerb gefährdet sind. Dies gilt beispielsweise in Fällen, in denen die Zielgesellschaft Produkte oder wesentliche Komponenten in für Verschlusssachen (VS) zugelassenen Systeme herstellt oder hergestellt hat, ein Betreiber Kritischer Infrastrukturen ist oder branchenspezifische Software zum Betrieb Kritischer Infrastrukturen herstellt.

Unter Berücksichtigung der jeweiligen wirtschaftlichen, rechtlichen und technologischen Situation des Erwerbers und der Zielgesellschaft analysiert und bewertet das

BSI mögliche Gefährdungssituationen hinsichtlich der IT-Sicherheit. Die Gefährdungsbewertung fließt in das sicherheitspolitische Votum des BMI ein.

Auf EU-Ebene hat die sogenannte EU-Screening-Verordnung 2019/452 zum Ziel, Direktinvestitionen durch Unionsfremde effektiver überprüfen zu können. Auch Deutschland hat damit begonnen, Außenwirtschaftsgesetz (AWG) und Außenwirtschaftsverordnung (AWV) der EU-Verordnung anzupassen.

Die Anzahl der durch das BSI begleiteten Einzelprüfungen im Zusammenhang mit Investitionskontrollverfahren hat sich fast jedes Jahr verdoppelt. Sie stieg von vier Verfahren 2015 auf 71 Verfahren 2019. Die seit Januar 2020 eingegangenen Verfahren haben den Trend zur jährlichen Verdopplung bestätigt, so dass das BSI 2020 voraussichtlich an mehr als 100 Prüfverfahren mitwirken wird.

2.3 Staat und Verwaltung

Die Regierungsnetze vor Attacken zu schützen, gehört zu zentralen Aufgaben und den besonderen Herausforderungen des BSI. Als Teil des Nationalen Cyber-Abwehrzentrums und Betreiber des Bundes Security Operations Centers (BSOC) sowie des *CERT Bund* nimmt es hier eine zentrale Rolle ein. Das BSI analysiert Cyber-Attacken und Schadsoftware und entwickelt Maßnahmen zum Schließen entdeckter Sicherheitslücken. Daneben spielt das Thema Vorsorge eine große Rolle, indem Länder und

AWG Verfahren und Nachgänge

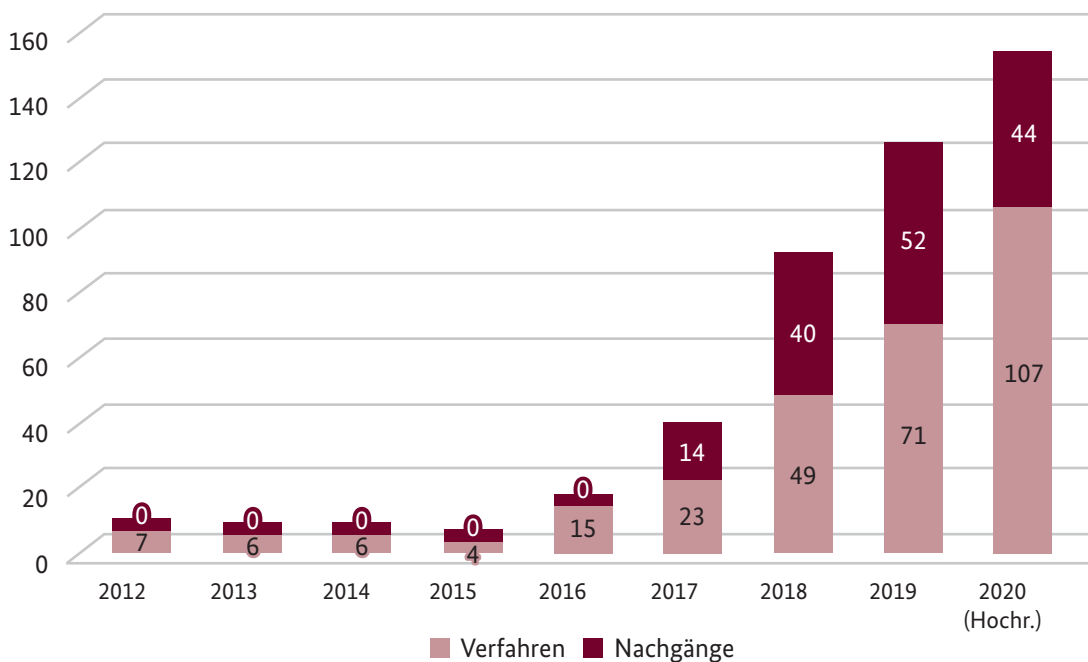


Abbildung 9 Entwicklung der Einzelprüfungen im Zusammenhang mit Einzelprüfungsverfahren, Quelle: BSI

Kommunen mit der Informationssicherheitsberatung beim Aufbau und Betrieb von Informationstechnik unterstützt werden. Mit seiner Expertise berät das BSI zudem in zahlreichen Projekten rund um die Implementierung und Weiterentwicklung der IT-Infrastruktur und den Einsatz neuer Sicherheitstechnologien.

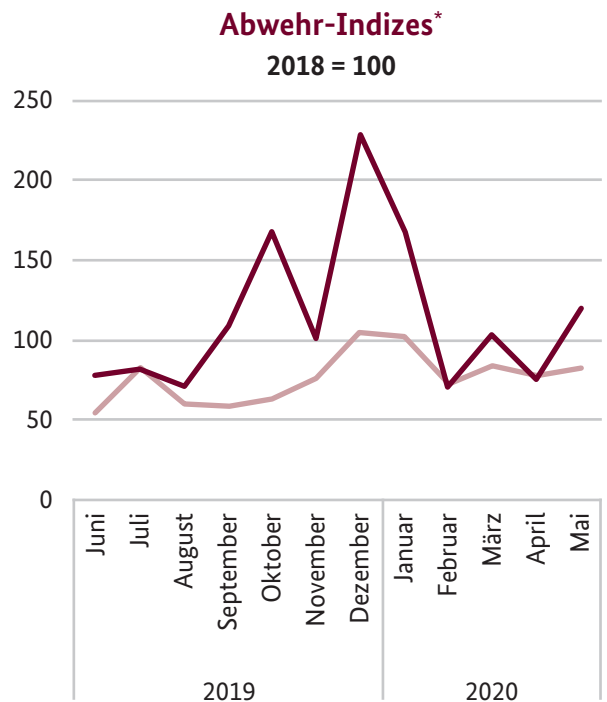
2.3.1 Die Gefährdungslage in der Bundesverwaltung

Tag für Tag sind die Regierungsnetze Cyber-Bedrohungen aus dem Internet ausgesetzt. Das sind nicht nur die ungezielten Massenangriffe, denen alle Internet-Nutzerinnen und -Nutzer ausgesetzt sind, sondern auch ganz gezielte Angriffskampagnen gegen die Regierungsnetze.

Für die Abwehr von Massenangriffen werden Spam-Filter, Webfilter und Virens Scanner eingesetzt. Die wesentlichen *Angriffsvektoren* für Massenangriffe sind auch in der Bundesverwaltung schädliche E-Mail-Anhänge einerseits und Links in E-Mails, Social-Media-Accounts oder auf Webseiten andererseits. In beiden Fällen werden Nutzerinnen und Nutzer mit *Social-Engineering*-Methoden zum Klicken verleitet und installieren dadurch ein Schadprogramm auf ihrem System.

Im Berichtszeitraum wurde die Bundesverwaltung verstärkt mit Links in E-Mails, Social-Media-Accounts und auf Webseiten angegriffen. Solche Links führen Nutzerinnen und Nutzer auf Internetserver, auf denen die Angreifer Schadcode zum Download bereithalten. Mit Hilfe von Webfiltern schützt das BSI die Netze des Bundes vor Angriffen. Webseiten, die Schadprogramme enthalten, werden in den Webfiltern zentral gesperrt, sodass aus der Bundesverwaltung nicht darauf zugegriffen werden kann. Im aktuellen Berichtszeitraum mussten rund 52.000 zusätzliche Webseiten gesperrt werden. Gegenüber dem vergangenen Berichtszeitraum ist das ein Anstieg von rund 46 Prozent. Dabei wurden zu Beginn des vierten Quartals 2019 und insbesondere zum Jahresende 2019 auffällig viele neue Sperrungen nötig. Im Dezember 2019 erreichte der Index der Webseiten-Sperrungen einen Spitzenwert von 230 Punkten und lag damit mehr als doppelt so hoch wie noch im Jahresdurchschnitt 2018.

Auch bei Angriffen mit Schadprogrammen via E-Mail war um den Jahreswechsel eine Angriffswelle zu beobachten. Im Vergleich zu früheren Wellen um den Jahreswechsel fiel diese jedoch spürbar geringer aus und endete bereits Anfang Februar. Mittels automatisierter Antivirus-Schutzmaßnahmen wurden daher pro Monat durchschnittlich rund 35.000 solcher schädlicher E-Mails in Echtzeit abgefangen, bevor sie die Postfächer der Empfänger erreichten. Davon wurden pro Monat durchschnittlich rund 9.200 schädliche E-Mails nur



- Abgewehrte Schadprogramm-Angriffe auf die Bundesverwaltung
- Neue Webseiten-Sperrungen

Abbildung 10 Abwehr-Indizes, Quelle: BSI-Auswertung eigener Quellen

*Ohne Angriffe auf Behörden, die nicht an den zentralen Schutzmaßnahmen des BSI teilnehmen.

aufgrund eigens erstellter Antivirus-Signaturen erfasst. Die Entwicklung dieser Indikatoren im Vergleich zum Vorjahresbericht ist einerseits auf die Veränderung der Taktik bei Schadsoftware-Angriffen zurückzuführen. Hier hat sich der Trend verstärkt fortgesetzt, dass Schadprogramme häufig nicht als Dateianhang in E-Mails versendet, sondern über Links in E-Mails verteilt werden.

Den automatisierten Antivirus-Schutzmaßnahmen nachgelagert betreibt das BSI ein weiteres System zur Detektion von Schadprogrammen im Datenverkehr der Regierungsnetze. Mit einer Kombination aus automatisierten Testverfahren und manueller Analyse eignet sich dieses System insbesondere zur Detektion von gezielten Angriffen und neuartigen Schadprogramm-Varianten. Die Analysten des BSI konnten auf diese Weise durchschnittlich weitere 4.900 Angriffe pro Monat detektieren, die von den eingesetzten kommerziellen Schutzprodukten nicht erkannt oder blockiert worden waren.

Neben den genannten Virens Scannern und Webfiltern werden die Netze des Bundes auch zentral vor unerwünschten Spam-E-Mails geschützt. Das betrifft nicht nur unerwünschte Werbe-E-Mails, sondern auch Cyber-Angriffe, wie *Phishing*-E-Mails, *Malware-Spam* oder Mas-senviren. Der Anteil unerwünschter Spam-Mails an allen

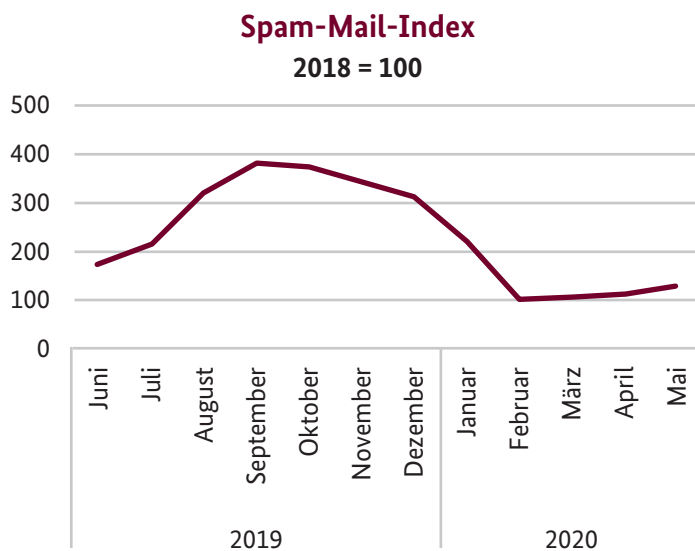


Abbildung 11 Spam-Mail-Index, Quelle: BSI-Auswertung eigener Quellen

in den Netzen des Bundes eingegangenen E-Mails lag im Berichtszeitraum bei durchschnittlich 76 Prozent. Das sind sieben Prozentpunkte mehr, als im vergangenen Berichtszeitraum mit 69 Prozent.

Aufkommen und Entwicklung der *Spam*-E-Mails in den Netzen des Bundes werden durch den Spam-Mail-Index gemessen. Der Anstieg des Indikators ist hauptsächlich auf die ausgeprägten *Spam*-Wellen im dritten Quartal 2019 zurückzuführen. Er lag im September 2019 bei 382 Punkten und damit fast viermal so hoch wie im Jahresdurchschnitt 2018. Die *Spam*-Welle endete Anfang Februar abrupt und hat sich seitdem auf niedrigerem Niveau stabilisiert.

2.3.2 Nationales Cyber-Abwehrzentrum

Das Nationale Cyber-Abwehrzentrum (Cyber-AZ) ist die Informations- und Kooperationsplattform auf Bundesebene zum operativen Austausch zwischen Behörden mit unterschiedlichen Zuständigkeiten im Bereich Cyber-Sicherheit. Als Kernbehörden arbeiten darin das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), das Bundesamt für den Militärischen Abschirmdienst (BAMAD), das BSI, das Bundesamt für Verfassungsschutz (BfV), das Bundeskriminalamt (BKA), der Bundesnachrichtendienst (BND), das Bundespolizeipräsidium (BPOLP) sowie das Kommando Cyber- und Informationsraum (KdoCIR) der Bundeswehr zusammen. Weitere staatliche Einrichtungen sind als assoziierte Stellen beteiligt. Darüber hinaus werden zusätzliche Partner aus verschiedenen Bereichen jeweils anlassbezogen eingebunden; auf Ebene der Bundesländer beispielsweise auch CERTs, Landeskriminalämter und Landesämter für Verfassungsschutz. Im Zuge der Weiterentwicklung des Cyber-AZ wurde im vergangenen Jahr vereinbart, dass sich die Kernbehörden künftig bei der Koordination des Cyber-AZ abwechseln.

Ende 2019 hat das BKA diese Aufgabe übernommen. Das BSI stellt als gastgebende Behörde weiterhin das Kernpersonal der Geschäftsstelle des Cyber-AZ, die Räumlichkeiten sowie die gemeinsame IT-Infrastruktur.

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

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

Durch die verstärkte Verlagerung vieler Aktivitäten ins Netz während der COVID-19-Pandemie lag im Berichtszeitraum ein besonderer Schwerpunkt auf der gemeinsamen Beurteilung der Entwicklung der Cyber-Sicherheitslage und der Koordination von Maßnahmen zum Schutz gefährdeter Einrichtungen.

2.3.3 Bundes Security Operations Center

Zum Schutz der Regierungsnetze und IT-Systeme des Bundes vor Cyber-Angriffen betreibt das BSI das Bundes Security Operations Center (BSOC). Ziel ist es, durch eine größtmögliche Automatisierung unter Nutzung aktueller Standardprodukte, Eigenentwicklungen und Künstlicher Intelligenz (KI)-unterstützter Verfahren ausreichend Freiräume für die unverzichtbaren manuellen Analysen von Angriffen und Schadsoftware durch Expertinnen und Experten des BSI zu schaffen. Diese sind auch bislang schon Voraussetzung für die sehr erfolgreiche Erkennung von Angriffen gegen die Bundesverwaltung.

Die Aufgaben des BSOC umfassen unter anderem Dienstleistungen zur Erfassung und Auswertung von Protokollierungs- und Sensordaten sowie zur Erkennung und Abwehr von Schadsoftware in E-Mails und im Webverkehr. Hierfür hat das BSI verschiedene Systeme entwickelt, die unter anderem durch eigene Antivirus-Signaturen, Detektoren und technische Plattformen kontinuierlich an die Bedrohungslage angepasst werden.

Hierbei erfolgt die Detektion nicht nur an den Netzgrenzen, sondern es werden auch Endsysteme in den geschützten Einrichtungen berücksichtigt.

Um die Analyse- und Reaktionsfähigkeit des Bundes gegen Cyber-Angriffe insgesamt noch weiter zu verbessern und die in der Bundesverwaltung verfügbaren Ressourcen zielgerichteter einzusetzen, arbeitet das BSI bei der Erkennung und Abwehr von Cyber-Angriffen eng mit anderen Bundesbehörden zusammen. Speziell wurde zusammen mit den IT-Dienstleistern des Bundes der BSOC-Verbund ins Leben gerufen. Dieser vernetzt die zentralen Dienstleistungen des BSI mit den lokalen Sicherheitsmaßnahmen der beteiligten Bundesbehörden, insbesondere im Bereich der operativen Informationssicherheit.

2.3.4 Computer Emergency Response Team für Bundesbehörden

Für präventive und aktive Maßnahmen bei Sicherheitslücken und IT-Sicherheitsvorfällen betreibt das BSI das *Computer Emergency Response Team* für Bundesbehörden (*CERT-Bund*). Das *CERT-Bund* erarbeitet und veröffentlicht präventive Handlungsempfehlungen zur Schadensvermeidung, Hinweise auf Schwachstellen in Hardware- und Software-Produkten und reaktive Maßnahmen zur Schadensbegrenzung oder -beseitigung. Darüber hinaus unterstützt *CERT-Bund* anlassbezogen die Reaktion auf IT-Sicherheitsvorfälle und benachrichtigt beispielsweise deutsche Netzbetreiber täglich über unterschiedliche, offen im Internet erreichbare oder verwundbare Server und Zugänge. Die *Provider* werden gebeten, ihre betroffenen Kundinnen und Kunden entsprechend zu informieren.

Die Dienstleistungen des *CERT-Bund* stehen in erster Linie den Bundesbehörden zur Verfügung. Dabei stellt das *CERT-Bund* zusammen mit dem Nationalen IT-Lagezentrum des BSI eine 24-Stunden-Rufbereitschaft sicher, analysiert eingehende Vorfallmeldungen, betreibt einen Warn- und Informationsdienst und bietet aktive Unterstützung in Form von Koordination und Analysen bei IT-Sicherheitsvorfällen an. Zur Reaktion auf Schwachstellen setzt *CERT-Bund* auf CVD. Dieser Prozess für die Veröffentlichung von Schwachstellen regelt und optimiert den notwendigen Austausch zwischen Findern, Herstellern und ggf. weiteren Betroffenen wie zum Beispiel Zulieferern. Oberstes Ziel ist, das nutzerseitig durch Schwachstellen entstehende Risiko so gering wie möglich zu halten. Hierfür müssen sich Schwachstellenentdecker sowie Nutzerinnen und Nutzer darauf verlassen können, dass der Hersteller seiner Verantwortung nachkommt und die gemeldeten Fehler im Sinne der *Security-by-Design*-Philosophie gemäß den

Regeln des CVD-Prozesses und der beispielsweise darin zugesicherten Frist korrigiert.

Für eine vertrauensvolle Zusammenarbeit im Rahmen eines externen Meldeprozesses sind eine verbindliche Kommunikation und verlässliche Reaktionsprozesse elementar. Um Hersteller und Finder bei der Koordination zu unterstützen, kann mitunter auch das BSI hinzugezogen werden. Die Betreuung von Schwachstellenmeldungen, ggf. benötigte vermittelnde Tätigkeiten sowie das Informieren von potenziell Betroffenen leistet *CERT-Bund*.

Im Berichtszeitraum wurden mehr als 20 CVD-Fälle unterstützt und darüber hinaus im Rahmen von Sicherheitsstudien des BSI detektierte Schwachstellen an Hersteller gemeldet. Dazu gehörten unter anderem Schwachstellen in Energiemess- sowie industriellen Steuerungssystemen, in Anwendungen und *Apps* des Gesundheits- und Finanzwesens, in Mikrocontrollern und Hardware-Token, in *Blockchain*-Anwendungen sowie Software-Produkten.

Darüber hinaus wurden *CERT-Bund* im Berichtszeitraum sechs Datenfunde vorgelegt. Datenfunde sind Sammlungen aus frei im Internet verfügbaren Identitätsdaten, die zum Beispiel von IT-Sicherheitsforscherinnen und -forschern oder anderen Spezialistinnen und Spezialisten im Rahmen von Recherchen gefunden wurden. *CERT-Bund* analysierte die Datenfunde in enger Abstimmung mit den Findern und auf der Grundlage eines eigens hierfür entwickelten Fragebogens. Die Analyse ergab, dass es sich bei den sechs Datenfunden um veraltete Daten wie zum Beispiel mittlerweile geänderte Passwörter handelte, über die zwar kein unmittelbarer Zugriff auf die betroffenen Accounts mehr möglich war, die aber gleichwohl auch künftig noch für die Erzeugung echt wirkender *Phishing*-E-Mails verwendet werden könnten.

Zur steten Weiterentwicklung der Analyse- und Reaktionsfähigkeiten kooperiert *CERT-Bund* national und international mit vielen *CERTs* anderer Organisationen, Länder und Unternehmen. Diese Vernetzung ermöglicht unter anderem, kurzfristig auf sich verändernde Lagen über Zuständigkeitsgrenzen hinweg zu reagieren und die von der Veränderung Betroffenen zu erreichen. Das *CERT-Bund* ist außerdem die zentrale Ansprechstelle für IT-sicherheitsrelevante Vorfälle in Deutschland.

Zusammen mit den anderen durch das BSI wahrgenommenen Aufgaben als BSOC und zentrales Lagezentrum des Bundes für Cyber-Sicherheitsvorfälle wird gewährleistet, dass Angriffe erkannt und dass schnell, im Bedarfsfall auch vor Ort (MIRT), darauf reagiert werden kann.

2.3.5 Nationales Verbindungswesen

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

Nach der erfolgreichen Pilotierung des Nationalen Verbindungswesens im Rhein-Main-Gebiet 2017 wurden 2018 und 2019 weitere Verbindungsstellen eröffnet. Das Nationale Verbindungswesen zählt nunmehr sechs Verbindungsstellen – Berlin, Bonn, Dresden, Hamburg, Stuttgart, Wiesbaden – und hat somit erstmals Anlaufstellen mit direkten Ansprechpartnerinnen und Ansprechpartnern für alle 16 Bundesländer geschaffen. Über diese Verbindungsstellen werden die Produkte und Dienstleistungen des BSI für die Zielgruppen Staat, Wirtschaft und Gesellschaft und somit das Thema Informationssicherheit für das ganze Land zur Verfügung gestellt.

Die Kooperationen zwischen dem BSI und den Bundesländern werden aktuell weiter ausgebaut. Hierfür wurden seitens des BSI spezielle Kooperationsfelder im Bereich der Cyber-Sicherheit entwickelt. Aus diesen Feldern können die Länder – ganz nach dem jeweiligen Bedarf – Kooperationen auswählen und so ihre Informationssicherheit gemeinsam mit dem BSI vorantreiben. Das BSI als die Cyber-Sicherheitsbehörde des Bundes begreift Cyber-Sicherheit als gesamtstaatliche Aufgabe und wird diesen kooperativen Ansatz weiter fortentwickeln.

2.3.6 Realisierung des Umsetzungsplans Bund (UP Bund)

Übergeordnetes Ziel des UP Bund ist die kontinuierliche Verbesserung der Informationssicherheit in der Bundesverwaltung durch ein Monitoring und eine gezielte, ressortübergreifende Steuerung. Die Realisierung des Umsetzungsplans Bund (UP Bund) wird daher jährlich evaluiert. Nach Inkrafttreten des neuen UP Bund 2017 wurde die Erhebung auf Basis eines prozessorientierten Ansatzes neu konzipiert und konnte im vergangenen Berichtszeitraum erstmalig in der Neukonzeption durchgeführt werden.

Mit Hilfe der gewählten Reifegradmethodik wurden erstmals konkrete Maßnahmen identifiziert und priorisiert dargestellt, um die Informationssicherheit in Einrichtungen und Ressorts effektiv und effizient zu erhöhen. Die Aufteilung in zwei Bereiche – Reifegradmethodik und flexible Erhebung einzelner, z. B. quantitativer Daten außerhalb des Reifegradmodells – hat

sich bewährt und wird auch in der Erhebung im Jahr 2020 weiterverfolgt. Durch die Wiederverwendung der Reifegradfragen werden Kosten- und Zeitaufwände eingespart und die Vergleichbarkeit zwischen den Berichtsperioden wird gewährleistet. Im flexiblen Modell wurden die Fragen an neuartige Entwicklungen und Themen der Informationssicherheit angepasst (z. B. Emotet) und sprachlich optimiert, wie es bereits bei der Neukonzeption vorgesehen war. Insgesamt sinkt mit der neuen Durchführungsmethodik der Zeitaufwand für die Informationssicherheitsbeauftragten während der Erhebung. Unterstützt wird dies durch eine engmaschige Nutzerbetreuung bei qualitativer Steigerung der Erhebung.

Mit der zweiten Sachstandserhebung UP Bund werden die Vorteile der Neukonzeption vollständig realisiert. Für die aktuelle Berichtsperiode kann gezielt dokumentiert werden, welche der empfohlenen Maßnahmen aus der letztjährigen Erhebung (2019) durchgeführt wurden. Zudem können erstmals unterschiedliche Prüfungsperioden anhand definierter quantitativer Kennzahlen (Reife- und Fähigkeitsgrade) miteinander verglichen werden, um Erfolge und ungenutztes Potenzial bei der Umsetzung transparent zu machen. Die jährliche Durchführung der Sachstandserhebung legt somit einrichtungsübergreifende, ressortweite Trends in der Informationssicherheit offen, welche die effektive und effiziente Priorisierung, Planung und Implementierung von Maßnahmen fördert und die Ziele des UP Bund nachhaltig unterstützt.

2.3.7 Informationssicherheitsberatung

Die unbefugte Veröffentlichung von persönlichen Daten im Internet, die Anfang 2019 publik wurde, war auch in der zweiten Jahreshälfte 2019 ein Schwerpunkt in der Beratung von Betroffenen. Die kurzfristig entwickelten Handreichungen und Konzepte wurden und werden stetig ergänzt, angepasst und aktualisiert, um eine breite Verwendung der Dokumente zu ermöglichen. Ein zweiter Schwerpunkt zeigte sich in der Beratung der Verwaltung im Kontext der neuen Gefährdung durch Emotet.

Die Sicherheitsberatung unterstützte weiterhin bei großen Digitalisierungsvorhaben der Verwaltung, beispielsweise im Rahmen der Umsetzung des Onlinezugangsgesetzes (OZG) oder bei der Absicherung des elektronischen Rechtsverkehrs. Im Zuge der Landtagswahlen wurden die Verantwortlichen der Bundesländer unterstützt. Die Beratung von Behörden und Ressorts der Bundesverwaltung bei Aufbau, Erhalt und Verbesserung des ISMS ist weiterhin von großer Bedeutung. Hier ist unter anderem die Unterstützung bei größeren Projekten in der Bundesverwaltung und bei der Erstellung von Sicherheitskonzeptionen zu nennen. Ebenso zählt

hierzu die Unterstützung bei allen aktuellen Problemstellungen, zum Beispiel der verstärkten Nutzung von Home-Office während der COVID-19-Pandemie.

Die Zusammenarbeit mit der Bundesakademie für öffentliche Verwaltung (BAköV) wurde nochmals intensiviert. So konnte unter anderem das Handbuch für die Fortbildung von IT-Sicherheitsbeauftragten in der öffentlichen Verwaltung maßgeblich überarbeitet und seit Anfang 2020 in einer aktuellen und modernen Fassung in der Fortbildung eingesetzt werden.

Informationssicherheitsberatung für Länder und Kommunen

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

Auf Basis der mit den Bundesländern abgeschlossenen Absichtserklärungen konnten erste konkrete Unterstützungprojekte mit verschiedenen Landesverwaltungen erfolgreich durchgeführt und abgeschlossen werden. Durch Mitarbeit in Gremien, wie der Arbeitsgruppe Informationssicherheit (AG InfoSic) des IT-Planungsrates sowie der Kommission IuK-Sicherheit im Rahmen der Innenministerkonferenz, wird ein kontinuierlicher Einblick in die Lage der Informationssicherheit vor Ort ermöglicht.

Auch die Zusammenarbeit mit Kommunen konnte durch Kooperation mit den kommunalen Spitzenverbänden vertieft und u. a. durch die Mitwirkung bei der Weiterentwicklung von gemeinsamen Lösungsansätzen bei Ebenen übergreifenden Verfahren ausgebaut werden.

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 im Schengen-Raum. Hierzu werden das Europäische Ein-/Ausreiseregister (Entry-Exit-System, EES) und das Europäische Reiseinformations- und -authorisierungssystem (European Travel Information and Authorisation System, ETIAS) mit dem polizeilichen Schengener 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 Digitalisierung im Grenzkontrollprozess durch die Einführung des Ein-/Ausreiseregisters und der Vorabüberprüfung durch den ETIAS-Antrag, den jede und jeder visumsbefreite Reisende stellen muss, wird es möglich sein, über Gesichtsbild und Fingerabdrücke von Reisenden aus Drittstaaten zukünftig Doppel- und Tarnidentitäten sicher zu erkennen. Durch die Möglichkeit des Abgleichs mit allen relevanten EU-Informationssystemen werden somit die letzten Schlupflöcher für Identitätsmissbrauch technisch geschlossen. Dies ist die Grundlage für die Erkennung irregulärer Migration und terroristischer Aktivitäten.

Das BSI ist dabei Teil der nationalen behördenübergreifenden Projektgruppe Smart Borders unter Federführung des BMI und unterstützt das Vorhaben mit technischen Spezifikationen und Vorgaben zur Umsetzung eines sicheren Identitätsmanagement-Prozesses auf allen Ebenen. Adressaten sind neben den operativen polizeilichen Behörden auf Bundesebene zukünftig auch die Asyl- und Migrationsbehörden der einzelnen Bundesländer.

Neben den Technischen Richtlinien (TR) für die hoheitliche Prüfung von elektronischen Reisedokumenten hat das BSI auch für die biometrischen Verfahren der Grenzkontrolle im Jahr 2019 die erste Version der TR BSI TR-03156 „Hoheitliches Identitätsmanagement in Verbindung mit EU-Informationssystemen“ vorgelegt, welche die Identitätsmanagementprozesse des Smart-Borders-Vorhabens im Bereich der neu zu schaffenden Grenzkontrollsysteme regelt. Damit liegt erstmals eine Beschreibung für sichere Kontrollverfahren unter Nutzung der neuen technischen Möglichkeiten auf europäischer Ebene vor.

Darüber hinaus lag 2019 ein Schwerpunkt der Arbeiten in der Ausgestaltung der technischen Vorgaben der neuen EU-Verordnungen zur Interoperabilität und der aktuell laufenden Novellierung des Visa-Informationssystems.

2.3.9 Technologieverifikation in sogenannten Security Labs

Die Quellcodeanalyse dient der Untersuchung sicherheitskritischer Technologien, welche beim Bund oder in sensitiven Infrastrukturen in Deutschland eingesetzt werden. Ziel ist es, gewonnene, zielgruppenspezifische Erkenntnisse über konkrete Technologien als Handlungsempfehlungen im Sinne einer Lösung für den cyber-

sicheren Betrieb (bspw. in Kritischen Infrastrukturen) zur Verfügung zu stellen, und somit zur Sicherheit aller beizutragen. Das BSI steht dazu im Kontakt mit zahlreichen Herstellern von Informations- und Kommunikationstechnik und intensiviert den technischen Dialog über sogenannte Security Labs. Diese Labs dienen zum einen als Austauschplattform, um Meetings und mit den Entwicklungsabteilungen rund um den Globus durchzuführen, zum anderen können dort tiefere technische Diskussionen und Einblicke bis hin zur Einsichtnahme auf Quellcodeebene realisiert werden. Dabei werden die BSI-Mitarbeiterinnen und -Mitarbeiter unter anderem von auf Codeaudits spezialisierten Expertinnen und Experten akkreditierter Prüflabore unterstützt. Durch diesen engen Austausch mit den Entwicklungsabteilungen des Herstellers lassen sich frühzeitig Trends und Risiken erkennen.

Grundlagen für die Quellcodeanalyse

Bei der Quellcodeanalyse werden für die Sicherheit relevante Codeabschnitte und -module genauer analysiert. Eine wichtige Grundvoraussetzung jeder Analyse ist sicherzustellen, dass der analysierte Code tatsächlich in einem Produkt zum Einsatz kommt. Eine sehr zuverlässige Methode ist, den Code selber zu kompilieren. Umgangssprachlich wird dieser Vorgang auch als Bauen der Software bezeichnet. Gewissermaßen kann versucht werden, eine Analogie zum Hausbau zu nehmen: Hier entspricht der Quellcode den Bauplänen des Hauses und der fertige Bau dem sogenannten Kompilat. Der Architekt kann gewisse Aussagen über ein Gebäude anhand der Pläne tätigen, jedoch ist viel tiefgründigeres Wissen vorhanden, wenn der Bau persönlich begleitet oder durchgeführt wurde. Beim Hausbau zu berücksichtigen sind auch äußere Einflüsse wie zum Beispiel das verwendete Werkzeug oder die Umgebungstemperatur, die einen Einfluss auf das Endresultat haben. Bei Quellcodeanalysen gilt das Gleiche: Das fertige Kompilat ist extrem abhängig von Umgebungsfaktoren wie zum Beispiel der Uhrzeit oder der zum Kompilieren verwendeten Software-Umgebung. Um dennoch eine eindeutige Zuordnung zu ermöglichen, setzt das BSI auf die Normalisierung dieser Faktoren. In der Fachsprache wird von sogenannten Reproducible Builds gesprochen. Bei Quellcodeanalysen kann durch diese Methode ein eindeutiger Zusammenhang zwischen dem untersuchten Quelltext und der auf dem Produkt laufenden Version hergestellt werden. Dies wird durch sogenannte Prüfsummen sichergestellt, die nach einem erfolgreichen Kompilierungsprozess aufgezeichnet werden. Dieses geschieht in der Regel ausschließlich durch BSI-Mitarbeiterinnen und -Mitarbeiter, die den Bauprozess beim Hersteller vor Ort persönlich durchführen. Werden diese Prüfsummen in einer Datenbank abgelegt, so kann im späteren Verlauf der Betreiber (z. B.

Mobilfunkbetreiber) automatisiert testen, ob diese geprüfte Software auch tatsächlich auf seinen Geräten installiert worden ist. Das hierfür verwendete Verfahren wird als Remote Attestation bezeichnet.

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 T-Systems zur Verfügung gestellt wird, bietet eine wesentliche Entscheidungsgrundlage für die jeweils Verantwortlichen, ob und unter welchen Bedingungen eine *App* eingesetzt werden kann. Damit wird eine größtmögliche Flexibilität beim Einsatz zusätzlicher populärer oder individuell benötigter *Apps* erreicht. Bei den *App-Prüfungen* werden sowohl sicherheitstechnische als auch datenschutzrelevante Aspekte berücksichtigt. Die Prüfberichte enthalten zudem ggf. 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 Ergebnisse geprüfter *Apps* zurückgreifen als auch bei Bedarf neue Prüfungen anstoßen. Dabei ist es auch möglich, *Apps* fortlaufend prüfen zu lassen, damit Ergebnisse von bereits freigegebenen *Apps* immer auf dem aktuellen Stand sind.

Derzeit (Stand: Mai 2020) wird der *App-Testing-Dienst* von registrierten Nutzerinnen und Nutzern aus mehr als 50 Behörden und Organisationen verwendet, für über 300 bereits geprüfte *Apps* stehen die Prüfergebnisse zum Abruf bereit.

2.3.11 Abstrahlsicherheit

Geht es um den Schutz von Staatsgeheimnissen, so sind zusätzlich zu den in der breiten Öffentlichkeit viel diskutierten Gefährdungen und Angriffen auf die

Vertraulichkeit kritischer Informationen auch die nicht unerheblichen Kapazitäten fremder Nachrichtendienste zu berücksichtigen. Bei der elektronischen Verarbeitung von Verschlusssachen prüft das BSI die IT-Hardware, mit der eine Verschlusssachen-Verarbeitung vorgenommen wird, auf kompromittierende Abstrahlung. Unter diesem Begriff werden alle elektromagnetischen Effekte zusammengefasst, die beim Betrieb eines IT-Gerätes als Begleiterscheinung auftreten und aus denen sich mit geeigneten Mitteln und Methoden die verarbeiteten Informationen rekonstruieren lassen. Da keine aktiven Abwehrhandlungen gegen diese Art der verdeckten, unbefugten Informationsbeschaffung existieren, sind konsequente Präventionsmaßnahmen geboten.

Zur Absicherung der IT-Hardware der Bundesverwaltung und weiterer bundesunmittelbarer Stellen hat das BSI eine Reihe von Unternehmen mit speziellen Fachkenntnissen anerkannt, die gegen kompromittierende Abstrahlung gesicherte IT-Hardware herstellen. Das BSI prüft die Wirksamkeit dieser Schutzmaßnahmen und unterstützt darüber hinaus Bedarfsträger mit Beratungsleistungen und Vor-Ort-Prüfungen an besonders sicherheitskritischen Systemen.

2.3.12 Lauschabwehr

Zu den Aufgaben der BSI-Lauschabwehr, abhörgefährdete Bereiche von Behörden des Bundes und der Länder sowie bei der geheimschutzbetreuten Wirtschaft zu überprüfen, gehörte im Jahr 2019 auch die technische Betreuung der Versteigerung von 5G-Frequenzbereichen bei der Bundesnetzagentur in Mainz. Dabei galt es sicherzustellen, dass die Gebotsabgaben der Netzbetreiber vertraulich blieben. Diese groß angelegte Aktion konnte ohne außergewöhnliche Vorkommnisse erfolgreich durchgeführt werden.

Zudem fanden Konferenzen statt, bei denen VS-eingestufte Inhalte erörtert wurden. Diese wurden wie in den vergangenen Jahren mit Beratungs- und Prüfmaßnahmen begleitet.

2.3.13 VS-Zulassung und Herstellerqualifizierung

Das BSI stellt auf der Grundlage der §§ 51 und 52 der Allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung, VSA) Zulassungsnachweise für IT-Sicherheitsprodukte aus. Mit der Zulassung wird diesen Produkten bescheinigt, dass sie im Rahmen des Geheimschutzes zum Schutz von VS IT in angemessen sicherer Weise verwendet werden können.

Im aktuellen Berichtszeitraum hat das BSI 66 Zulassungen erteilt bzw. verlängert. Die Anzahl der zugelassenen IT-Sicherheitsprodukte bzw. Produktversionen konnte damit auf insgesamt 216 weiter erhöht werden. Allgemein zugelassene Produkte können der tagesaktuell gepflegten BSI-Schrift 7164 entnommen werden.

Neben der Bearbeitung von Zulassungsverfahren fanden im Berichtszeitraum auch zahlreiche von der BSI-Zulassungsstelle durchgeführte Seminare und Informationsveranstaltungen statt, um die Inhalte der VSA-Novelle, die im August 2018 veröffentlicht wurde zu vermitteln.

Weiterführende Hinweise zur Zulassung sowie auch die BSI-Schrift 7164 finden Sie unter www.bsi.bund.de (vgl. *Quellenverzeichnis*³⁴: www.bsi.bund.de).

Herstellerqualifizierung

Eine erfolgreich absolvierte Herstellerqualifizierung stellt für einen Hersteller die Voraussetzung dafür dar, dass seine IT-Sicherheitsprodukte das qualifizierte Zulassungsverfahren VS-NUR FÜR DEN DIENSTGEBRAUCH durchlaufen können. In dieser wird einem Hersteller nach erfolgreicher Bewertung der Entwicklungsprozesse durch das BSI das Vertrauen ausgesprochen, Produkte sicher im Sinne der VS-Zulassung entwickeln zu können. Damit kann ein qualifizierter Hersteller eine Produktzulassung schneller durchlaufen, als dies bei einem herkömmlichen Zulassungsverfahren der Fall wäre. Die Effizienz des Verfahrens konnte bereits in einer Vielzahl von erfolgreich durchlaufenen Zulassungsverfahren bestätigt werden, in denen eine Produktzulassung innerhalb von 4 bis 8 Wochen erlangt wurde.

Derzeit haben drei Hersteller eine Herstellerqualifizierung erfolgreich absolviert, vier weitere durchlaufen aktuell das Qualifizierungsverfahren.

VS-Anforderungsprofile

VS-Anforderungsprofile (VS-AP) beschreiben IT-Sicherheitsanforderungen an zuzulassende IT-Sicherheitsprodukte. Sie werden in einem kooperativen Vorgehen gemeinsam von Bedarfsträgern, Betreibern und dem BSI erstellt. Auf diese Weise wird sichergestellt, dass Sicherheitsanforderungen in harmonisierter, bedarfsgerechter und effizienter Weise festgeschrieben werden. Inzwischen wurden 13 abgeschlossene VS-Anforderungsprofile zu verschiedenen Produkttypen und die dazugehörige Reihe von IT-Sicherheitsprodukten, die konform zu diesen BSI-Anforderungen sind, veröffentlicht. Eine detaillierte Beschreibung und Auflistung vorhandener und in Arbeit befindlicher VS-APs finden Sie unter www.bsi.bund.de (vgl. *Quellenverzeichnis*³⁵: www.bsi.bund.de).

Integrationsverfahren von Common Criteria-Zertifizierungen in das Zulassungsschema des BSI

Die Versorgung von Nutzerinnen und Nutzern mit zugelassenen IT-Sicherheitsprodukten steht aufgrund sich ständig verändernder Bedrohungslagen und stetig kürzer werdender Produktentwicklungszyklen vor einer großen Herausforderung. Um diesen Gegebenheiten begegnen zu können, ist es erforderlich, das bestehende Zulassungsschema kontinuierlich zu verbessern und um innovative Methoden und Instrumente zu erweitern.

Neben dem bereits sehr erfolgreich in das Schema integrierte qualifizierte Zulassungsverfahren VS-NUR FÜR DEN DIENSTGEBRAUCH (vgl. *Quellenverzeichnis*³⁶: www.bsi.bund.de) arbeitet das BSI derzeit an der effizienten Integration von Common Criteria -Zertifizierungsergebnissen in das Zulassungsschema des BSI.

Hierbei handelt es sich um ein derzeit in der Erprobung befindliches Verfahren, mit dem zuvor vom BSI nach Common Criteria zertifizierte Produkte unter Nutzung von Synergieeffekten einer VS-Zulassung zugeführt werden können. Dabei werden die im Rahmen einer erfolgreich absolvierten Zertifizierung gewonnenen Prüfergebnisse soweit möglich bei der Zulassung wiederverwendet. Möglich ist dies, da das Evaluierungsvorgehen in beiden Bereichen (Common-Criteria-Zertifizierung und VS-Zulassung) auf sehr ähnlichen Philosophien beruht. Dadurch sind nur noch die über eine Common Criteria (CC)-Zertifizierung hinausgehenden Aspekte einer Untersuchung zu unterziehen. Verglichen mit dem Durchlaufen eines vollständigen Zulassungsverfahrens bedeutet die Gewährleistung des für die Zulassung erforderlichen Vertrauenswürdigkeitsniveaus für alle Parteien einen enormen Ressourcengewinn.

Erste Erprobungen des Verfahrens sind vielversprechend verlaufen, sodass mit einer Aufnahme des Verfahrens in das Zulassungsschema im Laufe des Jahres gerechnet wird.

Ziel: VS-Strategie

Das Ziel einer zukünftigen erfolgreichen Innovationsstrategie für den VS-Markt muss sein, mehr zugelassene VS-Lösungen schneller und bedarfsgerechter bereitzustellen. Dazu werden auf Basis definierter Handlungsfelder Entscheidungen über die Priorisierung von VS-Anforderungen und entsprechender Produktentwicklungen getroffen sowie Synergien durch organisationsübergreifende Bündelung von Ressourcen freigesetzt.

Ein effektiver und effizienter Weg, dies zu erreichen, besteht in regelmäßigen bi- und multilateralen Abstimmungen zwischen den im Zulassungsschema wirken-

den Stakeholdern. Hier sind insbesondere die Betreiber und Bedarfsträger, die Hersteller und Integratoren von VS-Produkten, die Prüflabore sowie das BMI und das BSI zu nennen. Ihnen muss es gelingen, ihre Ressourcen gemeinsam so einzusetzen, dass man den Schwerpunkt ihres Handelns von einer zumindest in Teilen reaktiven Position zu einer weitgehend proaktiven Gestaltung des VS-Marktes verlagert.

Der bi- und multilaterale Austausch zwischen den Stakeholdern wird auf unterschiedlichen Plattformen, den sogenannten Innovationsforen, praktiziert. Dem jährlich in Berlin stattfindenden Kongress Omniseure kommt dabei im Rahmen der zukünftigen VS-Strategie eine zentrale Rolle zu. Das BSI etabliert seit 2018 zunehmend den Themenkomplex VS als einen wesentlichen Schwerpunkt dieses Kongresses, der sich dadurch erfolgreich als „die“ Anlauf- und Referenzstelle zum Thema VS und Zulassung entwickelt.

Dabei soll interessierten Teilnehmerinnen und Teilnehmern die Gelegenheit gegeben werden, sich über den aktuellen Sachstand, Aktionen und geplante Vorhaben rund um den Themenkomplex VS und Zulassung zu informieren. Ferner bietet das BSI an, sich an der zukünftigen Ausrichtung der VS-Strategie aktiv zu beteiligen, zum Beispiel durch themenspezifische Workshops, Präsentationen mit und für die Stakeholder, multilaterale Diskussions- und Informationsrunden sowie bilaterale Gespräche.

Neben dem großen Interesse an den VS-Foren lässt sich der Erfolg der eingeschlagenen VS-Strategie und des verwendeten Formats auch an der stetig wachsenden Teilnehmerzahl der Stakeholder des Zulassungsschemas ablesen. Dies gilt sowohl für die kontinuierlich steigende Anzahl VS-bezogener Präsentationen als auch für die zunehmenden VS-spezifischen Aussteller.

2.3.14 Umsetzung des Onlinezugangsgesetzes: Komponenten für die sichere Digitalisierung von Verwaltungsprozessen

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

Vorgaben an die sichere Anbindung von Identifizierungs- und Authentisierungsverfahren an die Nutzerkonten werden in der Technischen Richtlinie TR-03160 Servicekonten des BSI gemacht. Damit wird den an die Nutzerkonten angebotenen Fachverfahren die Identität von Nutzerinnen und Nutzern auf dem jeweiligen Vertrauensniveau garantiert, ohne dass sie Details der Identifizierung und *Authentifizierung* kennen müssen. Zudem definiert die TR-03160 Vorgaben zur Interoperabilität der Lösungen von Bund und Ländern, um zu gewährleisten, dass Nutzerinnen und Nutzer sich nur bei einem Bundesland identifizieren müssen und anschließend auch Leistungen eines anderen Bundeslandes oder des Bundes in Anspruch nehmen können.

Für die elektronische Zustellung der in den Fachverfahren erstellten Bescheide stellen die Servicekonten Postfächer zur Verfügung. Auch die hierfür zu entwickelnden Vorgaben sollen in die TR-03160 einfließen und die Interoperabilität der unterschiedlichen Postfachlösungen gewährleisten.

Um Bescheide auch dann noch auf ihre Integrität prüfen zu können, wenn sie ausgedruckt vorliegen oder auf mobilen Geräten vorgezeigt werden, können sie mit kryptografisch gesicherten Barcodes versehen werden. Solche digitalen Siegel gemäß BSI TR-03137 werden bereits auf hoheitlichen Dokumenten wie zum Beispiel Ankunftsnachweisen verwendet, um die Echtheit der aufgedruckten Daten zweifelsfrei verifizieren zu können. Eine bereits vorbereitete Ergänzung der TR-03137 ermöglicht dann auch die Absicherung von Urkunden, Bescheiden und anderen Verwaltungsdokumenten.

2.4 Internationales

Das Thema IT-Sicherheit macht vor Grenzen nicht halt, genauso wenig wie die aktuellen Bedrohungen im Cyber-Raum. Um dem effektiv zu begegnen ist es notwendig, die Kräfte auf internationaler Ebene zu bündeln. Aus diesem Grund arbeitet das BSI mit seinen Partnern zusammen, bilateral oder in Gremien. In Europa und darüber hinaus sind die Expertinnen und Experten des BSI als Gesprächspartner gefragt. Ein Grund dafür ist die Überzeugung des BSI, dass die Cyber-Sicherheit in Deutschland nicht zuletzt durch internationale Zusammenarbeit und weltweiten Austausch gestärkt wird.

2.4.1 Internationales Engagement des BSI

Die internationale Zusammenarbeit ist für das BSI seit seiner Gründung vor fast 30 Jahren ein essenzieller Faktor zur Verbesserung der Cyber-Sicherheit. Ziel des BSI ist, neben seiner nationalen Rolle als Cyber-Sicherheitsbe-

hörde des Bundes, 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 mit Behörden, Organisationen, Unternehmen und Akteuren der Wissenschaft und Zivilgesellschaft weltweit. Die Arbeit an diversen Fachgremien zu Informations- und Cyber-Sicherheit im EU-, NATO- und internationalen Kontext ist dabei wesentlicher Bestandteil des internationalen Engagements des BSI.

Ein wichtiger Meilenstein der europäischen Zusammenarbeit war das auf Initiative und Einladung des BSI ausgerichtete Cyber Security Directors' Meeting, bei dem sich zu Beginn des Jahres erstmalig die Leiterinnen und Leiter der Cyber-Sicherheitsbehörden Europas zu einem exklusiven Austausch im Vorfeld der Münchner Sicherheitskonferenz trafen.

Darüber hinaus engagiert sich das BSI besonders bei der Vertiefung und dem Ausbau von bi- und multilateralen Partnerschaften mit Behörden der Cyber-Sicherheit, wobei hier momentan ein thematischer Schwerpunkt auf der Sicherheit von 5G-Mobilfunknetzen liegt. Auch in und gegenüber der NATO erfüllt das BSI als Cyber-Sicherheitsbehörde des Bundes eine wichtige Rolle. Seinem Anspruch folgend, zu einem weltweit hohen IT-Sicherheitsniveau beizutragen, unterstützt das BSI ein EU-Projekt zum Aufbau von Cyber-Sicherheitskapazitäten in den Staaten der östlichen EU-Partnerschaft.

2.4.2 eID: Europaweite Anerkennung der Online-Ausweisfunktion

Im Rahmen des Ausbaus der Digitalisierung gewinnen elektronische Identitäten und die damit verbundene elektronische Identifizierung von Personen und Dingen stark an Bedeutung. Nur mit sicheren elektronischen Identitäten kann ein Identitätsdiebstahl nachhaltig vermieden werden. Um die Reichweite der sicheren nationalen elektronischen Identitäten zu erweitern, wurden bereits 2014 in Hinblick auf die Digitalisierung des europäischen Binnenmarkts auf EU-Ebene im Rahmen der eIDAS-Verordnung einheitliche, europaweit geltende Rahmenbedingungen für die gegenseitige Anerkennung von elektronischen Identifizierungsmitteln und Vertrauensdiensten festgelegt.

Unter Mitarbeit des BSI hat Deutschland mit der Online-Ausweisfunktion des Personalausweises und des elektronischen Aufenthaltstitels das einer solchen Anerkennung vorgelagerte Notifizierungsverfahren bereits 2017 als erstes Land erfolgreich abgeschlossen. Die Notifizierung der Online-Ausweisfunktion auf dem höchsten

Vertrauensniveau gemäß der eIDAS-Verordnung wurde anschließend im September 2017 im Amtsblatt der EU veröffentlicht. Basierend darauf gilt seit September 2018 die gegenseitige Anerkennungspflicht. Alle EU/EWR-Mitgliedstaaten, die über entsprechende Online-Dienste verfügen, sind verpflichtet, die Online-Ausweisfunktion für Anwendungen des öffentlichen Sektors, d. h. insbesondere im E-Government, anzuerkennen und anzubinden.

Infolgedessen haben bis April 2020 mit technischer Unterstützung durch das BSI bereits 18 Staaten (Belgien, Dänemark, Estland, Finnland, Griechenland, Großbritannien, Italien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Österreich, Schweden, Slowakei, Slowenien, Spanien, Tschechische Republik) und die Europäische Kommission die Online-Ausweisfunktion erfolgreich in ihr eID-Schema eingebunden. Damit ist es bereits jetzt möglich, die Online-Ausweisfunktion in gewohnter Weise für Online-Dienste in mehr als der Hälfte der EWR-Staaten zu verwenden. Obwohl nicht alle verbleibenden Staaten über entsprechende Online-Dienste verfügen und somit von der Anerkennungsverpflichtung befreit sind, befinden sich acht Staaten (Stand: Mai 2020) im Testbetrieb oder in Vorbereitung dazu, sodass ein weiteres Wachstum der Abdeckung weiterhin zu erwarten ist.

Aber auch andere Länder zeigen Bestrebungen, ihre eID-Schemata zu notifizieren. So haben bis Ende April 2020 bereits 13 andere Staaten eID-Schemata notifiziert (Belgien, Dänemark, Estland, Großbritannien, Italien, Kroatien, Lettland, Luxemburg, Niederlande, Portugal, Slowakei, Spanien, Tschechische Republik). Weitere Verfahren laufen derzeit oder sind fast abgeschlossen. Das BSI wirkt auch an diesen Notifizierungsverfahren mit seiner Fachkenntnis mit.

Die eID-Schemata der verschiedenen Länder unterscheiden sich teilweise sehr stark. Viele der begutachteten eID-Systeme nutzen tatsächlich die nationalen, auf Chipkarten basierenden Ausweisdokumente. Andere basieren auf der Verwendung von zertifizierten SIM-Karten oder anderen hard- bzw. softwarebasierten Sicherheitseigenschaften von Endgeräten. Manche dieser Lösungen stützen sich auch auf die Nutzung von sogenannten Identitäts Providern, die teilweise privatwirtschaftlich agieren und gleichzeitig mehrere Identifizierungsmittel (Mobile-App basierte Verfahren, SMS-TAN etc.) anbieten können.

Diese verschiedenen Ansätze führen natürlich auch zu unterschiedlichen Bewertungen im Rahmen der zum Notifizierungsverfahren gehörenden Begutachtungen. Während beispielsweise die Chipkarten-basierten eID-Schemata allgemein dem höchsten Vertrauensniveau zugeordnet werden, werden Systeme, die auf der Nut-

zung von Video-Ident oder SMS-TAN zurückgreifen, nur einem mittleren Vertrauensniveau zugeordnet. Eine Sonderstellung nehmen App-basierte Verfahren ein, deren Bewertung stark von den eingesetzten Sicherheitsfunktionalitäten des Mobilgerätes abhängt.

Die anderen notifizierten elektronischen Identitäten werden im deutschen E-Government mit Hilfe der Nutzerkonten oder Bürgerportale im Rahmen der Umsetzung des Online-Zugangsgesetzes angebunden und so anerkannt. So ist beispielsweise geplant, das Bundesbürgerportal Mitte 2020 entsprechend freizuschalten.

2.5 Sonstige Entwicklungen in der IT-Sicherheit

Mit der technologischen Entwicklung stellen sich immer wieder neue Fragen zur Sicherheit, für die es gilt, Antworten zu finden. Deshalb arbeitet das BSI in verschiedenster Weise mit Universitäten, Fachhochschulen und anderen Forschungseinrichtungen zusammen. Künstliche Intelligenz ist dabei ein wichtiges Thema, zumal sie gleich in mehrfacher Hinsicht sicherheitsrelevante Fragen aufwirft. Ein weiteres wichtiges Thema: Kryptografie. Mit der Entwicklung von Quantencomputern wird auch die Sicherheit unserer digitalen Infrastruktur infrage gestellt, die derzeit vor allem auf dem Einsatz kryptografischer Verfahren beruht. Doch welche Möglichkeiten bietet Quantenkryptografie und wie ist der aktuelle Entwicklungsstand der Quantencomputer? Diesen Fragen geht das BSI gemeinsam mit seinen nach.

2.5.1 Künstliche Intelligenz

Methoden der Künstlichen Intelligenz (KI) zeigen in vielen Anwendungsbereichen, wie zum Beispiel der Objekterkennung auf Bildern, erstaunliche Leistungen und werden zunehmend in Bereichen eingesetzt, die unser tägliches Leben beeinflussen. Die Bedeutung des Themas für unsere Gesellschaft, die Wirtschaft und den Staat nimmt stetig zu. Dementsprechend hat das Thema KI auch für das BSI eine besondere Bedeutung.

Sicherheit von KI-Systemen

Trotz nennenswertem Fortschritt in der Forschung sind wichtige Aspekte von KI-basierten Systemen, zum Beispiel Robustheit und Verlässlichkeit von KI-Systemen, Transparenz, Erklärbarkeit von Entscheidungen und Nicht-Diskriminierung, derzeit noch nicht hinreichend verstanden. Handlungsbedarf sieht das BSI insbesondere bezüglich der Etablierung von verlässlichen Sicherheitseigenschaften, die auch in der KI-Strategie der Bundesregierung als wesentlich für die Akzeptanz in Wirtschaft

und Gesellschaft bewertet werden. Im Vergleich zu klassischen IT-Systemen existieren bei KI-Systemen neuartige *Angriffsvektoren*: Durch eine Manipulation von Trainings- oder Eingabedaten können die Systeme oft gezielt zu falschen Entscheidungen verleitet werden. Bereits geringfügige Änderungen, die schwierig zu detektieren und für Menschen möglicherweise nicht unmittelbar erkennbar sind, können gravierende Auswirkungen haben. Ein weiteres Beispiel ist, dass die Ausgaben von KI-Systemen unter bestimmten Umständen Rückschlüsse auf möglicherweise vertrauliche Trainingsdaten zulassen.

Im Berichtszeitraum betreute das BSI mehrere Abschlussarbeiten und Praktika, die sich mit Angriffen auf KI-Systeme und möglichen Verteidigungsstrategien auseinandersetzen, und veröffentlichte einen wissenschaftlichen Übersichtsartikel (vgl. *Quellenverzeichnis*³⁷: <http://arxiv.org>) über die Angreifbarkeit und Absicherung von ausgewählten KI-Modellen.

Neben der Analyse von Sicherheitseigenschaften ist deren Nachweisbarkeit im Rahmen von Prüfverfahren entscheidend. Das BSI arbeitete im Berichtszeitraum mit verschiedenen Partnern an der Entwicklung von Prüfkriterien und Prüfmethode für KI-Anwendungen in unterschiedlichen Domänen, insbesondere im Bereich Automotive und *Cloud-Services*.

Diese Aktivitäten werden zukünftig erweitert und in einem größeren Rahmen zusammengeführt: Das Deutsche Institut für Normung (DIN) erarbeitet, im Auftrag mehrerer Bundesministerien, eine Roadmap für Normen und Standards im Bereich der KI, die in den sicherheitstechnischen Aspekten wesentlich durch das BSI mitgestaltet wird. Insbesondere arbeitet das BSI federführend an einem Konzept zur Umsetzung dieser Roadmap mit. Das Konzept sieht vor, in einem breit angelegten nationalen Programm und unter Einbeziehung von relevanten Stakeholdern in den nächsten Jahren Prüfstandards für eine Vielzahl von KI-Anwendungsdomänen zu entwickeln, zu erproben und einzuführen.

Begleitend dazu war das BSI im Berichtszeitraum in weiteren relevanten Arbeitsgruppen vertreten, u. a. bei der Plattform Lernende Systeme (vgl. *Quellenverzeichnis*³⁸: www.plattform-lernende-systeme.de) und der ETSI Industry Specification Group Securing Artificial Intelligence (vgl. *Quellenverzeichnis*³⁹: www.etsi.org) und beteiligte sich an der Erstellung von Publikationen (vgl. *Quellenverzeichnis*⁴⁰: www.plattform-lernende-systeme.de) im Rahmen dieser Arbeitsgruppen.

Medienmanipulation mittels KI

KI-gestützte Methoden werden zunehmend zur Medienmanipulation eingesetzt: Während Fälschungen von Medien ohne den Einsatz von KI i. d. R. auf statische Inhalte (Bilder und Texte) beschränkt sind und einen hohen finanziellen und zeitlichen Aufwand erfordern, ermöglicht der Einsatz von KI als Angriffswerkzeug unter bestimmten Voraussetzungen die täuschend echte Manipulation von dynamischen Medieninhalten, u. a. von Gesichtern und Stimmen in Video- und Audiostreams. Die verschiedenen Verfahren werden dabei landläufig als Deep Fakes bezeichnet. Angreifer können diese Verfahren nutzen, um z. B. bei biometrischen Authentifizierungsverfahren in Videokonferenzen oder in über Soziale Medien geteilten Mediendateien, falsche Identitäten vorzutauschen. Das BSI betreute im Berichtszeitraum in diesem Themenfeld Masterarbeiten, die sich u. a. mit der Detektion von solchen Manipulationen beschäftigten.

Einsatz von KI in der Kryptografie

Im Berichtszeitraum befasste sich das BSI weiterhin mit dem Einsatz von KI-Methoden in der Kryptografie: Im Fokus der Untersuchungen standen die mathematische Kryptoanalyse (vgl. *Quellenverzeichnis*⁴¹: www.link.springer.com) und die *Seitenkanalangriffe* (vgl. *Quellenverzeichnis*⁴²: <https://eprint.iacr.org>). Ein wichtiger Aspekt der Untersuchungen war der Vergleich von KI-basierten mit konventionellen Angriffen, der in den betrachteten Szenarien eine leichte Überlegenheit von KI-basierten Ansätzen zeigte. Die erzielten Ergebnisse werden in Evaluierungsverfahren bei der Zertifizierung und Zulassung von Produkten verwendet, um kryptografische Algorithmen und deren Implementierungen zu beurteilen.

2.5.2 Kryptografie

Die Sicherheit unserer digitalen Infrastruktur beruht wesentlich auf kryptografischen Verfahren. Konkret verschlüsselt man in der digitalen Kommunikation Nachrichten mit einem kryptografischen Schlüssel, der vorher üblicherweise mit einem *Public-Key*-Verfahren vereinbart wurde. Dabei stützt sich die Sicherheit der Schlüsselvereinbarung auf die angenommene Schwierigkeit bestimmter mathematischer Probleme. Beispielsweise basiert die Sicherheit des gängigen RSA-Verfahrens, das zum Verschlüsseln aber auch zum Signieren verwendet wird, auf der Tatsache, dass es im Allgemeinen schwierig ist, große Zahlen in ihre Primfaktoren zu zerlegen.

Mit heutigen Mitteln sind die gängigen *Public-Key*-Verfahren nicht zu brechen. Dies gilt jedoch nicht mehr, wenn Quantencomputer mit ausreichender Leistungsfähigkeit verfügbar sind. In den letzten Jahren ist die Entwicklung von Quantentechnologien rasant vorangeschritten (vgl. *Entwicklungsstand Quantencomputer*, Seite 76), sodass dieser Zeitpunkt in greifbare Nähe rückt.

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

Erste quantencomputerresistente Verfahren zum Schlüsseltransport werden bereits in der Technischen Richtlinie TR-02102 empfohlen. Dabei ist zu beachten, dass diese Verfahren sich noch in der Standardisierung befinden und vor allem als erste Empfehlungen für den Schutz von Daten mit langfristigem Schutzbedarf gedacht sind. Das BSI hat zudem erste Handlungsempfehlungen zur Migration zu Post-Quanten-Kryptografie veröffentlicht, die schon heute umgesetzt werden können, um der Bedrohung durch Quantencomputer zu begegnen.

Ein alternativer Ansatz zur Post-Quanten-Kryptografie ist die Quantenkryptografie, insbesondere die Quantum Key Distribution (QKD). Die Quantenkryptografie verspricht, Sicherheit auf Basis von Naturgesetzen zu garantieren. Das BSI wird ein Schutzprofil zur Evaluierung von QKD-Produkten nach Common Criteria erstellen lassen sowie die theoretische und praktische Sicherheit von QKD weiter untersuchen.

Im Rahmen des Projekts QuNET des Bundesministeriums für Bildung und Forschung (BMBF) wird die Entwicklung von Quantenkryptografie gefördert. Eine erste Demonstrationsstrecke für einen quantencomputerresistenten Schlüsselaustausch zwischen BMBF und BSI wird voraussichtlich im Herbst 2020 der Öffentlichkeit präsentiert. Das QuNET-Konsortium, BMBF und BSI sind intensiv mit den Vorbereitungen beschäftigt. Das BSI ist ebenfalls in das Projekt Q.Link.X eingebunden. Q.Link.X ist ein Verbundprojekt von Forschungseinrichtungen und Firmen in Deutschland, das die Grundlagen für Quantenrepeater und damit Quantennetze schaffen soll.

Forschung und Industrie arbeiten ebenfalls an Quantenzufallsgeneratoren. Hierbei schafft das BSI in Kooperation mit dem Fraunhofer-Institut für Angewandte Optik

und Feinmechanik (Fraunhofer IOF) durch Workshops und intensive Diskussionen die Grundlagen für die Sicherheitsevaluierungen solcher Generatoren.



Entwicklungsstand Quantencomputer

Um eine fundierte Einschätzung zum aktuellen Entwicklungsstand bzw. der potenziellen zukünftigen Verfügbarkeit von Quantencomputern zu erhalten, wurde vom BSI die Studie „Entwicklungsstand Quantencomputer“ bei Forschern der Universität des Saarlandes und der Florida Atlantic University in Auftrag gegeben. Die Studie beleuchtet aktuelle technologische Ansätze und quantenalgorithmische Innovationen und deren Implikationen im Kontext aktuell eingesetzter Kryptografie. Bei einer ersten Revision der Studie in 2019 hat sich gezeigt, dass algorithmische und technologische Fortschritte (u. a. bei der Fehlerkorrektur) die Anzahl der benötigten physikalischen Quantenbits (Qubits) für eine gegebene Aufgabe reduzieren können. Eine zweite Revision wird 2020 erscheinen. Die Studie und eine Zusammenfassung stehen auf der BSI Webseite unter www.bsi.bund.de/qcstudie zur Verfügung (vgl. *Quellenverzeichnis*⁴³: www.bsi.bund.de).

2.5.3 Blockchain-Technologie

Im Bereich der Informationssicherheit gehört *Blockchain* immer noch zu den häufig diskutierten Themen. Wie bei allen neuen Technologien sollte auch bei der *Blockchain*-Technologie Sicherheit von Anfang an mitberücksichtigt und *Security by Design* angestrebt werden. Das BSI hat daher Anfang 2018 Eckpunkte zur Sicherheit von *Blockchains* veröffentlicht und eine öffentliche Diskussion begonnen.

Im Frühjahr 2019 hat das BSI ein umfassendes Dokument mit dem Titel „*Blockchain* sicher gestalten. Konzepte, Anforderungen, Bewertungen“ veröffentlicht, das im Dezember 2019 auch auf Englisch erschienen ist. Es vertieft die Eckpunkte des BSI zur *Blockchain*-Technologie und unterstützt Entwickler und potenzielle Nutzerinnen und Nutzer von *Blockchain*-Lösungen dabei, Chancen und Risiken fundiert zu bewerten und IT-Sicherheit von Anfang an zu berücksichtigen. Dabei werden verschiedene Aspekte wie die Langzeitsicherheit beispielhaft diskutiert.

Wegen der besonderen Bedeutung des Datenschutzes im Zusammenhang mit der *Blockchain*-Technologie erfolgte

eine Zusammenarbeit mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. So werden die in der DSGVO formulierten Betroffenenrechte, wie beispielsweise die Rechte auf Berichtigung, Löschung und Datenübertragbarkeit, im Zusammenhang mit der *Blockchain*-Technologie diskutiert.

In einer begleitenden Studie hat das BSI parallel einen Marktüberblick zu *Blockchain*-Anwendungen erstellt

und danach ausgewählte Produkte aus verschiedenen Produktklassen exemplarisch evaluieren lassen. Die Hauptresultate der Studie wurden im Mai 2020 veröffentlicht (vgl. *Quellenverzeichnis*⁴⁴: www.bsi.bund.de).

Alle Veröffentlichungen des BSI zur *Blockchain*-Technologie stehen unter auf der Webseite des BSI (vgl. *Quellenverzeichnis*⁴⁵: www.bsi.bund.de) zum Download zur Verfügung.

3 Fazit



3 Fazit

Digitalisierungsschub nutzen – Informationssicherheit nachhaltig gestalten

Corona, Covid-19, SARS-CoV-2: Begriffe, die sich in den vergangenen Monaten eingepreßt haben. Die COVID-19-Pandemie hat das erste Halbjahr 2020 nachhaltig geprägt und ist auch bei Drucklegung dieses Berichts noch nicht beendet. Ihre vielschichtigen Auswirkungen haben nach wie vor erheblichen Einfluss auf Staat, Wirtschaft, Gesellschaft und jeden Einzelnen in Deutschland, Europa und weltweit. Abseits aller medizinischen und epidemiologischen Fragestellungen hat die Corona-Krise der Digitalisierung in Deutschland einen erheblichen Vorschub geleistet und eindrucksvoll gezeigt, dass funktionierende und sichere Informationstechnologie zur Lebensader der modernen Gesellschaft geworden ist. Ohne Home-Office, Online-Zusammenarbeit, Videokonferenzen und Chats, digitale Geschäftsprozesse, Online-Handel und Video-Streaming wären die Auswirkungen der Pandemie für Wirtschaft und Gesellschaft wohl noch schwerwiegender als sie es ohnehin schon sind.

Viele Menschen, aber auch viele Unternehmen, insbesondere im Mittelstand, mussten ihre gewohnten Abläufe innerhalb kürzester Zeit umstellen und neuen Rahmenbedingungen anpassen. Im privaten Bereich wurden Kontakte zu Familie und Freunden oft per Videochat aufrechterhalten. Viele Unternehmen nutzten innovativ und einfallreich die Möglichkeiten der Informations- und Kommunikationstechnologie, um Geschäftsprozesse zu digitalisieren und ihre Produkte und Dienstleistungen auf digitalem Wege anzubieten. Erfreulich ist, dass die Informationssicherheit bei vielen dieser Bemühungen nicht nur ein Randthema war. Auch aufgrund der jahrelangen Aufklärungs- und Sensibilisierungsarbeit des BSI ist vielen Anwendern in Wirtschaft und Gesellschaft daran gelegen, innovative Lösungen zu nutzen, die praxisingerecht, bedienbar und sicher sind. Exemplarisch hat die öffentliche Debatte um die Corona-Warn-App gezeigt, welche Bedeutung und welchen Einfluss die Datensicherheit hat – auch als notwendige Voraussetzung für einen wirksamen Datenschutz. Es gilt, diesen Entwicklungsschub der Digitalisierung zu nutzen und auch in der Nach-Corona-Zeit weiter voran zu treiben.

Funktionierende sichere IT ermöglicht Konzentration auf Kernaufgaben

Gerade im Gesundheitswesen hat die Digitalisierung in den letzten Jahren verstärkt Einzug gehalten. Auch

in den Zeiten vor Corona wurden immer mehr Abläufe im Gesundheitswesen digitalisiert. Viele Kliniken und Arztpraxen sind vernetzt und nutzen die Möglichkeiten moderner IT und Medizinprodukte, um Diagnosen und Therapien effektiver, effizienter und verträglicher für die Patientinnen und Patienten zu machen. Die Aufgabe von Ärztinnen, Ärzten und Pflegepersonal ist es dabei, Leben zu retten, kranke Menschen zu heilen und sich um ihre Patientinnen und Patienten zu kümmern. Sie sollten sich nicht damit auseinandersetzen müssen, ob die Stations-PCs funktionieren oder ob Sicherheitsupdates für ein medizinisches Gerät oder den Steuerungsrechner einer Herz-Lungenmaschine eingespielt werden müssen. Sichere, verfügbare, funktionierende Informationstechnologie ist die Voraussetzung dafür, dass das medizinische Personal seine Aufgabe erfüllen kann. Dies gilt sinngemäß ebenso für jedes andere Berufsfeld. Dass es bei der Absicherung dieser Technologien an einigen Stellen noch Nachholbedarf gibt, haben die teils erfolgreichen Cyber-Angriffe auf Krankenhäuser sowie auch die immer wieder bekannt gewordenen Schwachstellen in Medizinprodukten gezeigt. Gerade wenn es um Menschenleben geht wird deutlich, wie wichtig die Informationssicherheit als Voraussetzung einer erfolgreichen Digitalisierung ist. Man stelle sich vor, welche Folgen ein erfolgreicher Cyber-Angriff auf ein Krankenhaus haben könnte, wenn dieses durch die Pandemie ohnehin bereits einem enormen Stress-Test unterzogen wird. Das BSI hat daher – auch schon vor Corona – einige Initiativen und konkrete, praxisorientierte Unterstützungsmaßnahmen auf den Weg gebracht, die zur weiteren Absicherung des Gesundheitswesens beitragen (vgl. Kapitel *Gesellschaft*, Seite 39).

Der Grundsatz der Informationssicherheit als Voraussetzung einer erfolgreichen Digitalisierung gilt nicht nur im Gesundheitswesen, sondern auch in anderen Bereichen der Wirtschaft und der Kritischen Infrastrukturen (KRITIS). Durch das IT-Sicherheitsgesetz von 2015 sowie durch zahlreiche Umsetzungshilfen und Empfehlungen des BSI hat der Bund die Voraussetzungen geschaffen und Rahmenbedingungen gesetzt, die für einen sicheren Betrieb Kritischer Infrastrukturen notwendig sind. KRITIS-Betreiber müssen angemessene Sicherheitsmaßnahmen zum Schutz ihrer IT-Systeme, Komponenten und Prozesse nach Stand der Technik umsetzen und dies alle zwei Jahre gegenüber dem BSI nachweisen. Die Auswertung der dem BSI vorliegenden Nachweise ergibt ein heterogenes Bild: einige KRITIS-Bereiche sind gut aufgestellt, in anderen gibt es Nachholbedarf (vgl. Kapitel *Gefährdungslage Wirtschaft mit besonderer Betrachtung Kritischer Infrastrukturen*, Seite 52). Insgesamt jedoch

zeigt sich, dass das IT-Sicherheitsgesetz erfolgreich dazu beiträgt, die Informationssicherheit in den für das Gemeinwohl so bedeutsamen KRITIS-Bereichen zu verbessern.

Dynamische Gefährdungslage – flexible Reaktion

Wie wichtig Flexibilität und Praxisorientierung im Bereich der Cyber-Sicherheit sind, wird auch am Beispiel der Corona-Krise deutlich. Denn diese hat gezeigt, wie adaptionsfähig auch Cyber-Kriminelle sind und welche Bedrohungslage daraus entstehen kann. Das BSI beobachtete eine Zunahme von Cyber-Angriffen mit Bezug zur Corona-Thematik auf Unternehmen ebenso wie auf Bürgerinnen und Bürger. Es gab etwa breit gestreute E-Mail-Spamwellen mit vermeintlichen Corona-Informationen. Unternehmen wurden per E-Mail aufgefordert, persönliche oder unternehmensbezogene Daten auf gefälschten Webseiten preiszugeben. Die Cyber-Kriminellen geben sich dabei als vermeintliche (staatliche) Institutionen zur Beantragung von Soforthilfegeldern aus. Mit betrügerischen Online-Shops machten sich Kriminelle zudem die erhöhte Nachfrage nach Schutzbekleidung oder Atemmasken zunutze.

Diese Methoden und Vorgehensweisen sind an sich nicht neu. Auch vor Corona wurden diese Angriffsmethoden angewandt, mit anderen aktuellen Themen als Aufhänger. Die Angriffe im Kontext Corona zeigen jedoch, wie wichtig es ist, Anwender immer wieder darauf aufmerksam zu machen und ihnen im Rahmen des digitalen Verbraucherschutzes das Rüstzeug an die Hand zu geben, sich selbst besser zu schützen. Dies ist jedoch nur die halbe Miete, denn gleichzeitig gilt es, auf Seiten der Digital-Industrie dafür zu sorgen, dass neue Technologien, Produkte und Dienstleistungen schon in der Entwicklung sicher gestaltet werden und sicher auf den Markt kommen. Aktuell können Verbraucherinnen und Verbraucher nicht erkennen, wie cyber-sicher ein Produkt ist. Damit sie das zukünftig können, entwickelt das BSI gemeinsam mit anderen Stellen des Bundes und der Wirtschaft das IT-Sicherheitskennzeichen (vgl. Kapitel *Das IT-Sicherheitskennzeichen – Transparenz für Verbraucherinnen und Verbraucher*, Seite 41)

Das BSI nimmt somit Einfluss auf beiden Seiten. Verbraucherinnen und Verbraucher profitieren von den Informationsangeboten und praxisgerechten Empfehlungen des BSI. Den Unternehmen macht das BSI passende Angebote etwa durch die Definition von Mindestanforderungen, durch Technische Richtlinien oder durch die Möglichkeiten der Zertifizierung. Allein im Bereich der Common Criteria hat das BSI im aktuellen Berichtszeitraum knapp 100 Zertifizierungen von Produkten und Standorten durchgeführt.

Das BSI passt sich dynamischen Gefährdungslagen an und unterstützt Anwender in Staat, Wirtschaft und Gesellschaft dabei, schnell und adäquat zu reagieren. So hat das BSI beispielsweise im Kontext der COVID-19-Pandemie schnell und umfassend zielgruppengerechte Informationen und Empfehlungen veröffentlicht, mit denen sich Internetnutzerinnen und -nutzer und Unternehmen gut gegen Cyber-Angriffe und Betrugsversuche wappnen können.

Diese Empfehlungen werden auch „nach Corona“ gelten. Denn auch dann wird es immer wieder neue Angriffsversuche geben, gegen die es sich flexibel aufzustellen gilt. Cyber-Angriffe mit *Ransomware* etwa haben auch zu Corona-Zeiten stattgefunden und werden auch danach weiterhin eine Bedrohung insbesondere für viele Unternehmen und Behörden sein. Mehrstufige Angriffe mit der Schadsoftware Emotet beispielsweise haben insbesondere bis Ende 2019 für teils erhebliche Schäden in Wirtschaft und Verwaltung gesorgt. Mit Beginn des Jahres 2020 kamen auch andere Schadprogramme zum Einsatz, mit nicht weniger einschneidenden Folgen für die Betroffenen. So lange dieses kriminelle Geschäftsmodell für Angreifer lukrativ ist, so lange wird es diese Bedrohungslage geben, und so lange wird das BSI sachgerechte Maßnahmen im Bereich der Prävention, Detektion und Reaktion ergreifen und Betroffene unterstützen.

Digitalisierung „Made in Germany“

Auch andere Themen der Informationssicherheit werden „nach Corona“ wieder und weiter im Fokus der öffentlichen Debatte stehen, beispielsweise Künstliche Intelligenz, 5G, das vernetzte, autonome Fahren oder das sichere Smart Home.

Die Herausforderung in der schnell voranschreitenden Digitalisierung ist es, mit eben dieser Dynamik Schritt zu halten und sie im Sinne der Informationssicherheit mitzugestalten. Das BSI verfolgt dabei einen kooperativen Ansatz und stellt seine Kompetenz und Erkenntnisse allen Akteuren in Staat, Wirtschaft und Gesellschaft – regional, national und international – zur Verfügung. Der partnerschaftliche Ansatz in der Kooperation darf jedoch keine Einbahnstraße sein. Erkenntnisse, in welcher Institution oder Organisation auch immer sie anfallen, müssen verantwortlich geteilt werden, um die Cyber-Abwehr zu stärken und die Gesellschaft weiter für die Gefahren aus dem Cyber-Raum zu sensibilisieren. Informationssicherheit wird so zu einem Qualitätsmerkmal der Digitalisierung „Made in Germany“, durch die Deutschland – gerade auch während und nach der Corona-Krise – seine Position auf den internationalen Märkten stärken und ausbauen kann.

Das BSI leistet einen entscheidenden Beitrag dazu, den Weg in die digitalisierte Gesellschaft für jeden Einzelnen sicher zu gestalten. Durch eine Vielzahl an konkreten operativen Maßnahmen, unterstützenden Kooperationen, richtungsweisenden Vorgaben und sensibilisierenden Empfehlungen des BSI ist Deutschland in den vergangenen Monaten wieder ein Stück cyber-sicherer geworden. Gleichwohl ist dies kein Grund, sich zurückzulehnen. Die Gefährdungslage bleibt aufgrund täglich neuer Schwachstellen, neuer Angriffsmethoden und steigender Komplexität in der IT-Landschaft dynamisch und angespannt, mit zum Teil dramatischen Auswir-

kungen auf Unternehmen, Behörden und Einzelpersonen. Dynamische Lagen erfordern dynamisches Handeln. Deutschland steht dieser Herausforderung nicht hilflos gegenüber. So wie bei einem modernen Hochleistungsrechner effiziente Mehrkernprozessoren, schnelle SSD-Speicher und passgenaue Software zu einem leistungsstarken Werkzeug werden, so arbeiten auch im BSI Expertinnen und Experten aus unterschiedlichsten Fachrichtungen an den wichtigsten Digitalthemen unserer Zeit zusammen. Gemeinsam gestalten wir im BSI die sichere Digitalisierung für Deutschland.

4 Glossar

Advanced Persistent Threats

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

Adversarialer Angriff

Szenarium, in dem das Eingangsbild von einem potentiellen Angreifer bewusst verändert wird, um das jeweilige neuronale Netzwerk zu täuschen. Adversarial Images sind Bilder und Gegenstände, die die Computer-Wahrnehmung bewusst täuschen sollen. Sie haben bestimmte über das eigentliche Bild oder den Gegenstand gelegte Strukturen und Muster, die das System überlisten. Für das menschliche Auge sind diese Muster jedoch nicht sichtbar. Wo Menschen beispielsweise eine Schildkröte sehen, erkennt das KI-System z. B. ein Haus.

Angriffsvektor

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

Applikation / App

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

Authentifizierung

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

Authentisierung

Authentisierung bezeichnet den Nachweis der Authentizität. Die Authentisierung einer Identität kann u. a. durch Passwordeingabe, 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

Bitcoins (BTC) sind 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 hashverknüpfte Liste von Datenblöcken geführt, die mit Hilfe eines Konsensverfahrens aktualisiert wird. Blockchain ist die technologische Grundlage für Kryptowährungen wie Bitcoin.

Bot / Botnetz

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

CEO-Fraud

Als CEO-Fraud werden gezielte Social-Engineering-Angriffe auf Mitarbeiter von Unternehmen bezeichnet. Der Angreifer nutzt hierbei zuvor erbeutete Identitätsdaten (z. B. Telefonnummern, Passwörter, E-Mail-Adressen etc), um sich als Vorstandsvorsitzender (CEO), Präsident o. Ä. auszugeben 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 Schnitt-

stellen 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.

Digital Nudging

Digital Nudging“ (dt. „Digitales Anstupfen“) ist eine subtile und zwanglose Einflussnahme auf das Verhalten von Menschen, mit dem Versuch, Verbraucher zu einem für sie und das Gemeinwohl vorteilhaften Verhalten „anzustupsen“. Dabei sollen die Verbraucher in Richtung besserer Entscheidungen beeinflusst werden, ohne ihnen dabei Wahl- oder Entscheidungsfreiheiten wegzunehmen oder ihnen ein bestimmtes Verhalten zu diktieren. Ziel ist, Verbrauchern dabei zu helfen, bessere und bewusste Entscheidungen zu treffen, zum Beispiel für Produkte mit besseren Informationssicherheitseigenschaften.

DoS / DDoS-Angriffe

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

Drive-by-Download / Drive-by-Exploits

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

Exploit

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

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.

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.

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 Computer-Viren, Würmer und Trojanische Pferde. Schadsoftware ist üblicherweise für eine bestimmte Betriebssystemvariante konzipiert und wird daher meist für verbreitete Systeme und Anwendungen geschrieben.

Morphing

Morphing ist eine digitale Bildbearbeitungstechnik, um mehrere Bilder zu einem Bild zu fusionieren. Diese Technik können Angreifer nutzen, um Gesichtsbilder von mehreren Personen so zu kombinieren, dass ein neues Gesichtsbild (Morph) mit einer Mischung der Gesichtsmkmale aller zum Morph beitragenden Personen entsteht. Diese gemorphten Bilder können Angreifer z. B. als Referenzbild bei der Beantragung eines Ausweisdokuments (wie z. B. eines Reisepasses) nutzen. Ausweisdokumente, die ein gemorphtes Bild als Referenzbild enthalten, können dann i. d. R. von allen zum Morph beitragenden Personen zur Authentifizierung genutzt werden.

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.

Phishing

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

Phishing-Radar der Verbraucherzentrale NRW

Seit 2010 wertet die Verbraucherzentrale NRW betrügerische E-Mails aus, die Verbraucher an das Phishing-Radar weiterleiten (phishing@verbraucherzentrale.nrw). Auf Basis der täglich eingehenden 200-300 E-Mails - bei denen es sich um Phishing, sonstigen Cyber-Crime 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 Netzwerk-Bereitstellung hinausgehende Dienstleistungen erbringt, beispielsweise den Netzbetrieb einer Organisation oder die Bereitstellung von Sozialen Medien.

Potenziell unerwünschte Anwendung (PUA)

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

Public-Key-Kryptografie

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

Ransomware

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

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 Präventiv-Maßnahmen wie zum Beispiel Fachpersonal, IT-Sicherheitsbudget, verfügbare technische Infrastrukturen u. Ä..

Security by Default

Ein Produkt, das nach Security by Default ausgeliefert wird, ist ohne zusätzliche notwendige Maßnahmen bereits in einem sicher vorkonfiguriertem 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 informativ-verarbeitender Systeme von hoher Relevanz.

Sinkhole

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

Social Engineering

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

Spam

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

UP KRITIS

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

VPN

Ein Virtuelles Privates Netz (VPN) ist ein Netz, das physisch innerhalb eines anderen Netzes (oft des Internets) betrieben wird, jedoch logisch von diesem Netz getrennt wird. In VPNs können unter Zuhilfenahme kryptografischer Verfahren die Integrität und Vertraulichkeit von Daten geschützt und die Kommunikationspartner sicher authentisiert werden, auch dann, wenn mehrere Netze oder Rechner über gemietete Leitungen oder öffentliche Netze miteinander verbunden sind.

Der Begriff VPN wird oft als Bezeichnung für verschlüsselte Verbindungen verwendet, zur Absicherung des Transportkanals können jedoch auch andere Methoden eingesetzt werden, beispielsweise spezielle Funktionen des genutzten Transportprotokolls.

Zwei- bzw. Mehr-Faktor-Authentisierung

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

5 Quellenverzeichnis

- ¹ <https://www.bsi.bund.de/ransomware>
- ² https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html
- ³ https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/BotNetze/Avalanche/FAQ/botnetz_faq_node.html#faq8606246
- ⁴ <https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar>
- ⁵ <https://www.heise.de/newsticker/meldung/Microsoft-leakt-250-Millionen-Eintraege-aus-Kundendatenbank-4644161.html>
- ⁶ https://www.greenbone.net/wp-content/uploads/CyberResilienceReport_DE.pdf
- ⁷ <https://www.trustedsec.com/blog/netscaler-honeypot/>
- ⁸ <https://deyda.net/index.php/en/2020/01/15/checklist-for-citrix-adc-cve-2019-19781/>
- ⁹ https://blog.dcs0.de/a-curious-case-of-cve-2019-19781-palware-remove_bds/
- ¹⁰ <https://www.fireeye.com/blog/threat-research/2020/01/vigilante-deploying-mitigation-for-citrix-netscaler-vulnerability-while-maintaining-backdoor.html>
- ¹¹ <https://msrc-blog.microsoft.com/2019/08/13/patch-new-wormable-vulnerabilities-in-remote-desktop-services-cve-2019-1181-1182/>
- ¹² https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2019/DejaBlue-Schwachstelle_140819.html
- ¹³ <https://www.link11.com/de/blog/bedrohungslage/ddos-report-von-link11-bestaetigt-steigende-komplexitaet-und-volumen-der-attacken/>
- ¹⁴ https://www.cl.cam.ac.uk/~sp849/files/RAID_2018.pdf
- ¹⁵ <https://www.datensicherheit.de/netscout-cybersicherheits-report-herausforderungen-unternehmen>
- ¹⁶ https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Dienstleistungen/Qualifizierte_Dienstleister/QDL_node.html
- ¹⁷ <https://shattered.io>
- ¹⁸ <https://sha-mbles.github.io>
- ¹⁹ <https://minerva.crocs.fi.muni.cz>
- ²⁰ <https://tpm.fail>
- ²¹ https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Checklisten/checklisten_node.html
- ²² <https://www.bundesregierung.de/breg-de/themen/wirksam-regieren/schutz-von-online-konten-1732360>
- ²³ <https://www.bsi.bund.de/gesellschaftlicherDialog>
- ²⁴ <https://www.bsi-fuer-buerger.de>
- ²⁵ https://www.bsi.bund.de/DE/Themen/KRITIS/IT-SiG/Was_tun/Stand_der_Technik/B3S/B3S.html
- ²⁶ https://www.bsi.bund.de/DE/Themen/KRITIS/IT-SiG/Was_tun/Nachweise/Orientierungshilfe/Orientierungshilfe_node.html
- ²⁷ <https://www.upkritis.de>
- ²⁸ <https://www.bsi.bund.de/zertifizierung>
- ²⁹ <https://www.commoncriteriaportal.org>
- ³⁰ https://www.bsi.bund.de/DE/Presse/Kurzmeldungen/Meldungen/Empfehlungen_mobiles_Arbeiten_180320.html
- ³¹ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/empfehlung_home_office.pdf
- ³² https://www.bsi.bund.de/DE/Presse/Kurzmeldungen/Meldungen/KoViKo_140420.html
- ³³ <https://www.allianz-fuer-cybersicherheit.de/ACS/29CST>
- ³⁴ https://www.bsi.bund.de/DE/Themen/Sicherheitsberatung/ZugelasseneProdukte/Zulassung_node.html
- ³⁵ https://www.bsi.bund.de/DE/Themen/Sicherheitsberatung/ZugelasseneProdukte/VS-Anforderungsprofile/VS-Anforderungsprofile_node.html
- ³⁶ <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf> (S. 44)
- ³⁷ <https://arxiv.org/pdf/2003.08837.pdf>
- ³⁸ <https://www.plattform-lernende-systeme.de>
- ³⁹ <https://www.etsi.org/committee/1640-sai>
- ⁴⁰ https://www.plattform-lernende-systeme.de/files/Downloads/Publikationen/AG3_6_Whitepaper_07042020.pdf
- ⁴¹ https://link.springer.com/chapter/10.1007/978-3-030-26951-7_6
- ⁴² <https://eprint.iacr.org/2020/165>
- ⁴³ <https://www.bsi.bund.de/qcstudie>
- ⁴⁴ <https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2019/Blockchain-Sicherheit-230519.html>
- ⁴⁵ www.bsi.bund.de/Blockchain

Impressum

Herausgeber

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Bezugsquelle

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185–189
53175 Bonn

E-Mail

bsi@bsi.bund.de

Telefon

+49 (0) 22899 9582-0

Telefax

+49 (0) 22899 9582-5400

Stand

September 2020

Druck

Appel & Klinger Druck und Medien GmbH, Schneckenlohe

Gestaltung

Faktor 3 AG

Texte und Redaktion

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Bildnachweis

Titel: GettyImages ©perihelio; S. 3: BMI; S. 4: BSI; S. 8, 38, 78:
GettyImages ©perihelio; S. 36: GettyImages ©mattjeacock;
S. 51: GettyImages ©Morsa Images

Grafiken

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Artikelnummer

BSI-LB20/509

Diese Broschüre ist Teil der Öffentlichkeitsarbeit des BSI.
Sie wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt.

