



Bundesamt
für Sicherheit in der
Informationstechnik



Die Lage der IT-Sicherheit in Deutschland 2019

Vorwort

Verschiedene Cyber-Vorfälle der vergangenen Monate und Jahre haben uns nochmals vor Augen geführt, dass Cyber-Sicherheit eine wesentliche Voraussetzung für das Gelingen der Digitalisierung ist. Wenn wir die Chancen der Digitalisierung voll ausschöpfen wollen, müssen wir die mit ihr verbundenen Risiken beherrschbar machen. Die Bürgerinnen und Bürger erwarten von Staat und Politik zu Recht, dass sie den Gefahren der Digitalisierung entgegenreten. Hierbei kommt dem Bundesamt für Sicherheit in der Informationstechnik (BSI) eine immer bedeutendere Rolle zu.

Ein besonderes Anliegen ist mir der Verbraucherschutz. Mit dem IT-Sicherheitsgesetz 2.0 werden wir dem BSI den Verbraucherschutz als zusätzliche Aufgabe zuweisen.

Das BSI arbeitet in einem starken Verbund: Für einen effektiven Schutz der Bürgerinnen und Bürger, der Wirtschaft und des Staates sorgt die behördenübergreifende Zusammenarbeit im Nationalen Cyber-Abwehrzentrum (Cyber-AZ). Ende Juni 2019 haben wir beschlossen, das Cyber-AZ zur zentralen Informations-, Kooperations- und Koordinationsplattform der Behörden fortzuentwickeln. In einem nächsten Schritt werden wir das Cyber-Lagebild und die Risikobewertung zu Cyber-Gefahren weiter optimieren. Durch den verbesserten Informationsaustausch kann somit künftig noch schneller und koordinierter auf Cyber-Angriffe reagiert werden.

Starke Behörden können IT-Sicherheit nicht allein gewährleisten. Dies ist vielmehr eine gesamtgesellschaftliche Herausforderung. Erfolgreich können wird nur sein, wenn Zivilgesellschaft, Wirtschaft, Wissenschaft und Politik gemeinsam an Lösungen arbeiten. In Erfüllung des Koalitionsvertrags haben wir daher den „Nationalen Pakt Cybersicherheit“ ins Leben gerufen. Alle gesellschaftlich relevanten Gruppen, Hersteller, Anbieter, Anwender und die öffentliche Verwaltung sind eingebunden, um in gemeinsamer Verantwortung mehr Cyber-Sicherheit zu erreichen.

Unser besonderes Augenmerk gilt den Kritischen Infrastrukturen, also etwa der Versorgung mit Strom, Wasser und Wärme. Das gesamte gesellschaftliche Leben ist davon abhängig, dass die Kritischen Infrastrukturen durchgängig verfügbar sind. Ohne deren Systeme und Dienstleistungen ist ein reguliertes öffentliches Leben nicht vorstellbar. Dabei sind auch Kritische Infrastrukturen auf eine reibungslos funktionierende Informationstechnik angewiesen. Um dies sicherzustellen, arbeiten KRITIS-Betreiber, ihre Verbände und unsere Behörden in einer öffentlich-privaten Partnerschaft – dem UP KRITIS – vertrauensvoll zu-

sammen. Dort tauschen sich alle Beteiligten über aktuelle Vorkommnisse aus, bewerten die Cyber-Sicherheitslage, bauen Krisenmanagementstrukturen auf und koordinieren die Krisenreaktion. Ergänzt wird dieser Ansatz durch die im BSI-Gesetz geregelten Pflichten der Betreiber Kritischer Infrastrukturen, welche ebenfalls dafür sorgen, dass deren IT-Systeme höchsten Sicherheitsstandards genügen.

Neben den Kritischen Infrastrukturen sind weitere Teile der Wirtschaft von besonderer Sicherheitsrelevanz. Im IT-Sicherheitsgesetz 2.0 werden wir die Anforderungen für diese Bereiche regeln.

In einer vernetzten Welt profitieren wir unmittelbar von einem entsprechenden Sicherheitsniveau bei unseren europäischen und internationalen Partnern. Wir werden deshalb die Schritte der EU zur Steigerung der IT-Sicherheit ebenso unterstützen wie den verstärkten weltweiten Austausch hierzu.

Der Lagebericht zur IT-Sicherheit in Deutschland 2019 zeigt: Das BSI sorgt durch die Begleitung zahlreicher Digitalisierungsprojekte – nicht zuletzt der Einführung des Mobilfunkstandards 5G – dafür, dass IT-Sicherheit in diesen Projekten von Anfang an mitgedacht und umgesetzt wird. Das ist bei Digitalisierungsvorhaben dieser Größenordnung unabdingbar.

Der Bericht macht deutlich, dass die Herausforderungen für die IT-Sicherheit vielfältig und komplex sind. Ich setze mich mit aller Kraft dafür ein, dass wir diesen Herausforderungen gemeinsam gerecht werden. Staat und Politik tun alles, um die Digitalisierung in unser aller Sinn sicher zu gestalten. Dafür steht das BSI.



Horst Seehofer

Bundesminister des Innern, für Bau und Heimat

Vorwort

Der Grad der Vernetzung unserer Gesellschaft nimmt zu. Mittlerweile hat die Digitalisierung fast alle Bereiche unseres Lebens erreicht. Wir werden schneller, mobiler, smarter. Gleichzeitig nehmen potenzielle Risiken und Gefahren zu. Um die Digitalisierung unserer Gesellschaft zukunftsfähig und sicher zu gestalten, müssen wir Informationssicherheit von Beginn an mitdenken: sei es bei der Digitalisierung unseres Alltags, bei Prozessen in der staatlichen Verwaltung oder in der Wirtschaft.

Der vorliegende Lagebericht 2019 analysiert die aktuelle IT-Sicherheitslage unter Bezugnahme konkreter Vorfälle einschließlich einer Beschreibung der Methoden und Mittel der Angreifer. Es werden konkrete Lösungsansätze zur Verbesserung der IT-Sicherheit in Deutschland sowie Angebote und Maßnahmen des BSI dargestellt. Hierbei wird auf die Adressaten Staat, Wirtschaft, Gesellschaft und Internationales näher eingegangen.

Das BSI stellte im Berichtszeitraum wieder eine Vielzahl kritischer Schwachstellen fest, nicht zuletzt in aktueller Chip-Hardware. Es zeigt sich erneut, wie wichtig qualitativ hochwertige Soft- und Hardware ist und welche Bedeutung Security-by-Design und Security-by-Default einnehmen müssen: Beide Grundprinzipien sind sinnvolle und notwendige Vorbedingung, um Verbraucher zu schützen und das notwendige Maß an Sicherheit und Verlässlichkeit sicherzustellen.

Und noch etwas Anderes stellt das BSI fest. Entwicklungen, die im vorherigen Lagebericht bereits beschrieben und prognostiziert wurden, sind in diesem Berichtszeitraum eingetreten. Dies betrifft unter anderem die Häufigkeit und Auswirkungen von Ransomware-Angriffen sowie Umfang und Bedeutung von Identitätsdiebstählen.

Darüber hinaus verstärkt die fortschreitende Digitalisierung digitale Abhängigkeiten. Sich schnell und automatisiert ausbreitende Angriffe können in letzter Konsequenz auch weltweit zu massiven wirtschaftlichen Schäden oder sogar – z. B. im Zusammenhang mit autonomem Fahren oder Medizinsystemen – zu gesundheitlichen Schäden bei Menschen führen. Umso wichtiger ist es, IT-Sicherheit in Unternehmen und Organisationen strukturell umzusetzen. Hier ist unsere Allianz für Cyber-Sicherheit (ACS) für Unternehmen und Organisationen jeder Größe die richtige Anlaufstelle.

Als Cyber-Sicherheitsbehörde des Bundes gestaltet das BSI die Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft. Qualifizierte und motivierte Mitarbeiterinnen und Mitarbeiter setzen sich in Bonn und zukünftig auch in Sachsen dafür ein, die aktuelle IT-Sicherheitslage zu analysieren, Gefahren zu begegnen und das Niveau der Cyber-Sicherheit gesamtgesellschaftlich zu erhöhen. So ist das BSI zuständig für die IT-Sicher-

heit der Bundesregierung und als Kompetenzzentrum für Fragen der Cyber-Sicherheit national und international anerkannt.

Die zunehmende Digitalisierung spiegelt sich auch in Fragen der Cyber-Sicherheit wider. Damit erweitert sich auch das Themenspektrum des BSI auf Themen wie die neue Netzinfrastruktur 5G, Künstliche Intelligenz, den Digitalen Verbraucherschutz, den Ausbau der Beratung auf kommunaler und Länderebene sowie das BSI als zentrale Zertifizierungs- und Standardisierungsstelle. Mit der Einnahme einer neuen Organisationsstruktur und dem Aufbau von neuen Referaten, Abteilungen und damit Zuständigkeiten hat das BSI nicht nur dem erfolgreichen personellen Aufwuchs, sondern insbesondere auch den zahlreichen neuen Aufgaben Rechnung getragen.

Den Herausforderungen der Cyber-Sicherheit muss auf allen Ebenen und von den relevanten Akteuren gemeinsam begegnet werden: sei es mit Partnern in der EU und der NATO, auf Bundes-, Länder- und kommunaler Ebene, mit Betreibern Kritischer Infrastrukturen sowie kleinen und mittleren Unternehmen (KMU) und in vertrauensvoller Zusammenarbeit mit den zuständigen Ressorts und nachgeordneten Behörden.

Um den notwendigen gesamtstaatlichen Ansatz verfolgen zu können, arbeitet das BSI eng mit allen im kontinuierlich fortentwickelten Cyber-Abwehrzentrum beteiligten Behörden zusammen.

Cyber-Sicherheit ist eine gesamtgesellschaftliche Aufgabe und beginnt bei einer stärkeren Sensibilisierung zu einer selbstbestimmten und sicheren Nutzung des Internets: Mit dem umfangreichen Informations- und Beratungsangebot für Bürgerinnen

und Bürger einschließlich einer kostenfreien Hotline steht das BSI auch jedem Einzelnen als Dienstleister und Ansprechpartner zur Verfügung.

Das BSI bietet mit seinem ganzheitlichen, nationalen und herstellerneutralen Ansatz ein Kompetenzzentrum, das sich als Gestalter und Vordenker im digitalisierten Zeitalter greift.



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 Die Gefährdungslage

1.1 Zusammenfassung und Bewertung der Gefährdungslage	7
---	---

1.2 Angriffsmethoden und -mittel	8
----------------------------------	---

1.2.1 Identitätsdiebstahl	8
---------------------------	---

1.2.2 Schadprogramme	11
----------------------	----

1.2.3 Ransomware	15
------------------	----

1.2.4 Distributed Denial of Service (DDoS)	18
--	----

1.2.5 Botnetze	21
----------------	----

1.2.6 Spam	26
------------	----

1.2.7 Trends in APT-Angriffen	27
-------------------------------	----

1.2.8 Angriffsvektoren im Kontext Kryptografie	29
--	----

1.2.9 Angriffe durch Ausnutzung moderner Prozessorarchitektur	32
---	----

2 Zielgruppenspezifische Lösungen und Angebote

2.1 Staat/Verwaltung	37
----------------------	----

2.1.1 Gefährdungslage der Bundesverwaltung	37
--	----

2.1.2 Lösungen und Angebote des BSI für Bund, Länder und Kommunen	39
---	----

2.2 Wirtschaft/Kritische Infrastrukturen	46
--	----

2.2.1 Gefährdungslage Wirtschaft und Kritische Infrastrukturen	46
--	----

2.2.2 Lösungen und Angebote des BSI für die Wirtschaft und Kritische Infrastrukturen (KRITIS)	50
---	----

2.3 Gesellschaft/Bürger	63
-------------------------	----

2.3.1 Gefährdungslage Gesellschaft/Bürger	63
---	----

2.3.2 Lösungen und Angebote des BSI für Gesellschaft und Bürger	66
---	----

2.4 Internationales und Wissenschaft sowie ausgewählte neue Technologien	68
--	----

2.4.1 Internationales	69
-----------------------	----

2.4.2 Zusammenarbeit mit der Wissenschaft	71
---	----

2.4.3 Kryptografie	71
--------------------	----

2.4.4 Blockchain-Technologie	72
------------------------------	----

2.4.5 Künstliche Intelligenz	72
------------------------------	----

3 Gesamtbewertung und Fazit

4 Glossar/Impressum

1 Die Gefährdungslage

1 Die Gefährdungslage

Das BSI beobachtet die Gefährdungslage der IT-Sicherheit in Deutschland kontinuierlich und stellt in diesem Bericht die Erkenntnisse aus dem Zeitraum 01. Juni 2018 bis 31. Mai 2019 zusammen. Nach einer Zusammenfassung der Bedrohungslage werden die Methoden und Mittel der Angreifer sowie die Rahmenbedingungen und Ursachen im Detail beschrieben. Anhand zahlreicher Beispiele wird zudem erläutert, wie durch Angriffe auf die IT-Sicherheit das Leben in einer digitalisierten Gesellschaft beeinträchtigt werden kann.

1.1 Zusammenfassung und Bewertung der Gefährdungslage

Der Schwerpunkt der Cyber-Angriffe liegt aktuell im Bereich Cyber-Kriminalität. Ein typisches Beispiel dafür ist eine erneute intensive Ransomware-Kampagne Ende des Jahres 2018 und Anfang 2019. Als besonders schwerwiegender Cyber-Angriff ist der Vorfall bei einem norwegischen Aluminiumlieferanten zu verzeichnen. Am 19. März 2019 wurde der Konzern Opfer einer massiven Attacke mit der Ransomware LockerGoga. Betroffen waren die meisten Geschäftsfelder; die Produktion musste weitgehend auf manuellen Betrieb umgestellt werden. Allein dieses Beispiel zeigt: Ransomware stellt nach wie vor eine starke Gefährdung dar und verursacht große Schäden.

Wie bereits in den Vorjahren sind Infektionen durch Schadprogramme eine der größten IT-Bedrohungen für Privatanwender, Unternehmen und Behörden. Dies belegen z. B. die Ergebnisse aus den Cyber-Sicherheits-Umfragen der Jahre 2017 und 2018 der Allianz für Cyber-Sicherheit. 53 % der berichteten Angriffe im Jahr 2018 waren Malware-Infektionen, im Jahr 2017 waren es 57 %.

Eine im Berichtszeitraum besonders relevante Malware ist Emotet. Das schon seit 2010 bekannte Schadprogramm ist seit November 2018 wieder vermehrt mithilfe von schädlichen Office-Dokumenten verteilt worden – mit immer ausgefeilteren Mechanismen. Die Evolution von Emotet zeigt sich insbesondere an neuen Fähigkeiten wie dem „Outlook-Harvesting“, also der Analyse des Mailverlaufs infizierter Computer – dem Nachladen von beliebigen anderen Schadprogrammen im Kontext kooperierender und arbeitsteiliger Computerkriminalität sowie der Verwendung von Techniken, die bisher nur bei Advanced Persistent Threats (APTs) eingesetzt wurden.

Darüber hinaus sind Identitätsdiebstähle an der Tagesordnung, bei denen personenbezogene Daten in hoher Anzahl missbräuchlich durch Dritte genutzt werden. Identitätsdiebstähle von weniger großen Datenmengen bekommen dann einen hohen Stellenwert, wenn die Täter persönliche Daten der Opfer der breiten Öffentlichkeit zugänglich machen. Sensibilisierung und Eigenverantwortung im Umgang mit der Digitalisierung sind neben technischen Lösungen notwendige Antworten auf den zunehmenden Missbrauch digitaler Identitäten.

Die Bedrohungslage durch Botnetze (Verbünde von Rechnern oder Systemen, die von einem fernsteuerbaren Schadprogramm [Bot] befallen sind) ist wie in den Vorjahren anhaltend hoch. Wie die aktuellen Entwicklungen zeigen, ist das Risiko, Teil eines Botnetzes zu werden, vor allem bei mobilen Endgeräten und Internet-of-Things-Systemen (IoT-Systemen) hoch. Insbesondere deren Verbreitung und Verwendung in fast allen Bereichen des täglichen Lebens bieten eine stetig breiter werdende Angriffsfläche. Die vergleichsweise geringen Infektionszahlen von IoT-Geräten in Deutschland sind maßgeblich auf den Aufbau der typischen Internetanbindung deutscher Endkunden zurückzuführen, die über einen Router ins Internet gehen und im Regelfall keinen direkten Zugriff von außen zulassen.

Durch serverbasierte Botnetze lassen sich enorme Ressourcen für Distributed Denial of Service (DDoS)-Angriffe aktivieren. Die DDoS-Angriffsbandbreiten überschreiten immer wieder die Marke von 150 Gbit/s und erreichen Werte von bis zu 300 Gbit/s. Generell führt eine stetige Spezialisierung durch Anwendung neuer Angriffsvektoren, zielgerichtete Zusammensetzung von DDoS-Angriffen (Multivektor-Attacken), Einsatz neuer Angriffswerkzeuge (DDoS aus der Cloud) sowie von DDoS-Booterdiensten zu einer konstant angespannten Bedrohungslage (siehe Kapitel 1.3.4 DDoS).

Interessant ist die Entwicklung bei Schadprogramm-Spam. Obwohl die Zahl derartiger E-Mails stark abnimmt, verbleibt das Bedrohungspotenzial nach wie vor auf einem hohen Niveau. Die Qualität und somit die Effektivität von Schadprogramm-Spam steigt weiterhin. Das liegt unter anderem an Innovativität, technischem Sachverstand und starkem personellen Aufwand der Angreifer.

Als Trend bei APTs (Angriffe, die nicht finanziell oder opportunistisch motiviert sind, sondern strategische oder taktische Ziele verfolgen) sind folgende Phänomene festzustellen: mehr öffentlich verfügbare APT-Werkzeuge,

eine wachsende Zahl internationaler APT-Dienstleister, die Nutzung legitimer Dienste zur Verschleierung, das Erschweren von Schadsoftware-Analysen sowie die Übernahme von APT-Techniken in kriminellen Kampagnen. Auch wenn dieser Trend die Detektion von APT-Angriffen erschwert, so können durchgängige, konsequent umgesetzte IT-Sicherheitsmaßnahmen viele APT-Vorfälle verhindern.

1.2 Angriffsmethoden und -mittel

Um Cyber-Sicherheit erfolgreich gewährleisten zu können, ist die Abwehr von Angriffen der wesentliche Aspekt. Wirksamer Schutz ist aber nur möglich, wenn die allgemeine wie auch die konkrete Gefährdungslage zumindest im Überblick bekannt sind. Eine regelmäßige und gezielte Neubewertung der bestehenden Risiken ist aufgrund der dynamischen Entwicklung der Cyber-Sicherheitslage unabdingbar, um geeignete präventive und reaktive Maßnahmen auszuwählen.

Neueste Erkenntnisse über Schwachstellen bei Hard- und Software werden immer wieder bereits nach kurzer Zeit für Cyber-Angriffe genutzt. In der großen Anzahl unterschiedlicher Angriffsziele und möglicher Angriffsmethoden lassen sich Trends und Tendenzen erkennen, die beim Aufbau einer erfolgreichen Abwehr berücksichtigt werden sollten.

1.2.1 Identitätsdiebstahl

Unter einer Identität wird im Kontext der Informationssicherheit die Menge von Merkmalen verstanden, die die Echtheit einer Person oder Sache bildet. Die Identität einer Person oder Sache kann somit sowohl durch ein einzigartiges Merkmal oder auch durch die Kombination diverser Merkmale bestimmt werden. Im Internet wird auf die Identität einer Person meist aus Identifikations- und Authentisierungsdaten geschlossen, wie z. B. der Kombination aus Benutzername und Passwort. Als „Identitätsdiebstahl“ wird folglich die rechtswidrige Zueignung solcher Daten bezeichnet.

Eine prominente Form des Identitätsdiebstahls ist das sogenannte Phishing. Mit Hilfe hoch entwickelter Techniken des Social Engineerings versucht ein Angreifer, das Opfer zur Herausgabe sensibler Informationen zu bewegen. Eine weitere Möglichkeit, Identitätsdaten zu entwenden, besteht in dem Einsatz spezieller Schadsoftware. Aber auch ohne direkte Beteiligung des eigentlichen Opfers können Identitätsdaten entwendet werden, z. B. direkt bei einem Diensteanbieter (Daten-Leak).

Meldungen zu Datenabflüssen von Kundeninformationen wurden im Berichtszeitraum häufig beobachtet. Unter den Betroffenen befanden sich einige namhafte Unternehmen, zum Beispiel die Hotelkette Marriott oder die Social-Media-Plattform Facebook. Der medialen Resonanz sowie der betroffenen Zielgruppe nach zu urteilen, stach besonders die Veröffentlichung zusammengetragener deutscher Politikerdaten heraus und wurde in den Medien als „Doxing“ bekannt (siehe Vorfall: Doxing auf Seite 9).

Das BSI erfährt von Datenabflüssen im Rahmen der Lagebeobachtung oder durch direkte Meldungen, beispielsweise durch Strafverfolgungsbehörden. Allein auf Basis der Meldungen ist nicht unmittelbar erkennbar, ob es sich bei den Daten um qualitativ hochwertige Daten (Gültigkeit, Aktualität etc.) handelt. Oftmals kann die Qualität der in Umlauf gebrachten oder zum Verkauf angebotenen Datensätze auch bei längerer Analyse nicht zweifelsfrei geprüft werden. Wenn ein betroffener Dienstleister den Datenabfluss nicht bestätigt, ist zudem fraglich, ob die Daten tatsächlich aus dem vermeintlichen Abfluss stammen. In diesen Fällen ist es z. B. auch möglich, dass die Daten lediglich generiert oder aus öffentlichen Informationen zusammengetragen wurden, um diese zu verkaufen. Auch hat die Vergangenheit gezeigt, dass zwischen dem eigentlichen Daten-Leak und dem öffentlichen Bekanntwerden des Leaks Jahre liegen können. So befinden sich aktuell große Datensammlungen im Umlauf, die sich meist mehr durch ihren Umfang als durch ihre Qualität auszeichnen. Die Anfang des Jahres vom BSI analysierten Datensammlungen unterstreichen dies (siehe Kasten Seite 9, Analyse von Datensammlung bigDB, Collection#1 - Collection#5, Zabagur sowie Anti Public).

Der Identitätsdiebstahl wird den Tätern nach Beobachtungen des BSI zum Teil leicht gemacht, z. B. durch die Nutzung von ungeschützten, öffentlichen Cloud-Speichern oder Fehlkonfigurationen. Aber auch unzureichend gepatchte Systeme oder Zero-Day-Exploits bieten Angreifern die Möglichkeit, Daten auszulesen. Auch mit öffentlich verfügbaren Tools (z. B. sqlmap, Software zum Erkennen und Ausnutzen von Datenbankschwachstellen) können Datenbanken von Systemen automatisch abgerufen, kopiert oder manipuliert werden. Weil viele Online-Shops dieselbe Software verwenden, ist es den Angreifern ein Leichtes, vorgefertigte Skripte ohne großen manuellen Aufwand auf eine Vielzahl ausgewählter Plattformen anzuwenden. Dabei werden auch Skripte angewandt, die automatisiert verwundbare Ziele über Webcrawler oder Suchmaschinen identifizieren (z. B. Google Dorker). Hierdurch gelangen Angreifer an immer neue Datensätze. Diese werden mit weiteren bereits



Doxing

Sachverhalt

Der mutmaßliche Täter hatte unter den Pseudonymen @_Orbit und @_Orbiter auf dem Kurznachrichtendienst Twitter Verlinkungen zum Herunterladen größerer Datensammlungen veröffentlicht. Die Veröffentlichungen wurden wie ein Adventskalender inszeniert. Bis zum 24. Dezember 2018 öffnete er täglich ein weiteres „Türchen“ und pries über Twitter neue private Daten unter namentlicher Nennung der betroffenen Person an. Neben bekannten Personen des öffentlichen Lebens waren vor allem deutsche Politikerinnen und Politiker aller politischen Ebenen von den Veröffentlichungen betroffen. Die veröffentlichten Datensätze enthielten sowohl öffentlich zugängliche Informationen, zum Beispiel die dienstliche Partei-E-Mail-Adresse, wie auch private, nicht öffentlich einsehbare Daten. In Einzelfällen wurden private Kommunikationsinhalte, wie zum Beispiel Familienchats und -bilder, zum Download bereitgestellt.

Reaktion

Das BSI richtete eine besondere Aufbauorganisation ein. Das Nationale Cyber-Abwehrzentrum übernahm die zentrale Koordinierung der Fallbearbeitung der beteiligten Bundesbehörden. Die Geschäftsstellen der Parteien der jeweils Betroffenen wurden vom BSI benachrichtigt. Seitdem stand das BSI in dauerhaftem Kontakt zu den Parteien und Abgeordneten und beriet, wo gewünscht und möglich, individuell. Die Datenpakete wurden vom Täter auf einer Vielzahl von Downloadportalen hinterlegt. Über 50 dieser sogenannten Hoster, teilweise aus dem Ausland, ersuchte das BSI umgehend um Löschung der Daten und erschwerte damit deren Weiterverbreitung. Ebenfalls wurden die verwendeten Twitteraccounts gesperrt.

Für die Betroffenen bedeutet der Vorfall große Unsicherheit in mehreren Bereichen: Neben der eigentlichen Veröffentlichung privater Inhalte stellt sich für viele Betroffene die Frage, über welchen Weg der Täter die Daten erlangt hat und ob auch dienstliche Informationen veröffentlicht wurden.

Empfehlung

Der beschriebene Vorfall veranschaulicht zweierlei: Er zeigt, dass unterschiedliche Motivationslagen für eine solche Tat infrage kommen. Nicht immer muss ein fremder Staat hinter aufsehenerregenden Cyber-Angriffen stehen. Auch Einzeltäter können großen Schaden anrichten. Des Weiteren wird bewusst, wie umfangreich die Menge an frei einsehbaren persönlichen Daten im Netz ist.

BSI für Bürger gibt umfangreiche Empfehlungen zum Schutz persönlicher Daten im Internet (https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/empfehlungen_node.html).

geleakten Daten angereichert, um einen möglichst großen Datensatz zu generieren und diesen entsprechend lukrativ zu veräußern. In Kombination mit der Problematik der Wiederverwendung von Passwörtern bei unterschiedlichen Diensten eröffnet die enorme Summe offengelegter Identitätsdaten folglich die Möglichkeit, unmittelbar Angriffe auch gegen immer weitere Online-Konten durchzuführen: Beim Credential-Stuffing werden geleakte Kombinationen aus Benutzername und Passwort automatisiert gegen Serviceanbieter gerichtet. Beim Thema Phishing-Angriffe stehen nach Erkenntnissen des BSI in Deutschland neben Bankkunden insbesondere auch Kunden von Online-Händlern wie Amazon oder Bezahl-systemen wie PayPal im Fokus.

Nach wie vor orientieren sich aktuelle Phishing-Kampagnen an gesellschaftlichen Ereignissen und aktuellen

Themen. Im aktuellen Berichtszeitraum haben sich Angreifer so immer wieder die Popularität um das Thema Blockchain, die Steuerrückzahlung sowie die Unsicherheit rund um das Thema Datenschutzgrundverordnung (DSGVO) zunutze gemacht, um möglichst viele Nutzer zur Herausgabe persönlicher Daten zu verleiten. Im Nachgang zu erfolgreichen Identitätsdiebstählen wurden vermehrt Erpressungsversuche via E-Mail beobachtet. Hierbei schickten Angreifer in den E-Mails beispielsweise Passwörter der Opfer mit oder gaben vor, das Opfer bei dem Besuch von Internetseiten mit pornografischen Inhalten beobachtet und aufgezeichnet zu haben (Sextortion).

Die schiere Menge an öffentlich zugänglichen Identitätsdaten (z. B. frei verfügbar durch Social-Media oder Daten-Leaks) ermöglicht es den Angreifern, personalisierte Phishing-Angriffe durchzuführen, die sich zudem durch

immer besser werdende Formulierungen auszeichnen. Gemeinsame Analysen der Verbraucherzentrale Nordrhein-Westfalen (VZ-NRW) sowie des BSI haben aufgrund der zur Verfügung stehenden Datenbasis (Meldungen ans Phishing-Radar) ergeben, dass bei Phishing-E-Mails in Deutschland anstatt rein auf Text basierenden E-Mails (28 %) größtenteils E-Mails mit Links (72 %) versendet werden, die schließlich auf eine Phishing-Seite zeigen. Diese Internetseiten sind rein optisch kaum von den Originalseiten zu unterscheiden und verleiten somit den Nutzer durch eine vorgetäuschte Seriosität dazu, seine Identitätsdaten preiszugeben. Um diese Seriosität weiter zu untermauern, setzen Angreifer bei den erstellten Phishing-Seiten vermehrt auf das Secure Hypertext Transfer Protocol (HTTPS), was für eine abhörsichere und nicht manipulierbare Datenübertragung steht. Eine solche Verschlüsselung sagt jedoch nichts über den eigentlichen Inhalt einer Seite aus. Auch Phishing-Seiten können ein

HTTPS-Zertifikat erhalten und den Datenverkehr zwischen dem Opfer und der Seite verschlüsseln. Den oben genannten Analysen zufolge kann für Phishing-Angriffe in Deutschland von einem Verhältnis von ca. 55 % HTTP zu 45 % HTTPS ausgegangen werden. Eine entsprechende Entwicklung hin zur vermehrten Verwendung von HTTPS ist seit Mitte 2017 verstärkt zu beobachten. Kostenlose Zertifikate sind aktuell das Mittel der Wahl für Angreifer und werden meist von Let's Encrypt oder Sectigo bezogen. Um die Seriosität einer URL neben der Verwendung von HTTPS weiter zu untermauern, verwenden Angreifer in der URL immer wieder prägnante Begriffe (z. B. Security-218309sad.de), bekannte Abkürzungen (z. B. AWS-anmeldungs-seite.de) oder den Anbieternamen (z. B. facebook-142.de oder gotrock.org/facebook). Die Nennung des Anbieternamens in der Domain, erweitert mit unüblichen Zusätzen wie Zahlen, wird hierbei auch als Combosquatting bezeichnet.



Analyse der Datensammlungen bigDB, Collection#1 - Collection#5, Zabagur sowie Anti Public

Sachverhalt

Im Januar 2019 hat das Lagezentrum des BSI Kenntnis von einer öffentlich zugänglichen Zusammenstellung personenbezogener Daten erhalten. Diese wurde von den Medien unter der Bezeichnung Collection#1 aufgegriffen. Kurze Zeit später wurde bekannt, dass neben der Collection#1 noch weitere Datensammlungen existieren, die mit der ersten Veröffentlichung in Verbindung stehen: bigDB, Collection#2 - Collection#5, Zabagur sowie Anti Public.

Ursache/Schadenswirkung

Die Daten stammen aus diversen Datenabflüssen unterschiedlicher Webseiten und Onlinedienste der vergangenen Jahre (beispielsweise aus den Datenleaks bei Yahoo, LinkedIn, Adobe und MySpace). Es kann davon ausgegangen werden, dass die Daten über einen längeren Zeitraum zusammengetragen wurden. So befinden sich in der Gesamtkollektion fast ausschließlich veraltete Datensätze sowie Datendubletten.

In Kombination mit der Problematik der Wiederverwendung von Passwörtern lassen sich solche Listen vor allem für Credential Stuffing verwenden. Beim Credential Stuffing werden geleakte oder generierte Kombinationen aus Benutzernamen und Passwörtern automatisiert gegen den Login-Mechanismus von Serviceanbietern gerichtet. Ein weiteres Problem besteht darin, dass Phishing-Angriffe durch solche Informationen immer gezielter und personalisierter gestaltet werden können.

Reaktion

Das BSI hat die Sicherung und Analyse der Daten durchgeführt, mit dem Ziel, die Betroffenheit der Bundesverwaltung festzustellen und weitere notwendige Schritte einzuleiten. Alle betroffenen Bundesbehörden und Bundesländer, die eindeutig zuordenbar waren, wurden informiert. Die Rückmeldungen konnten bestätigen, dass es sich zum größten Teil um sehr alte und nicht mehr in aktueller Verwendung befindliche Daten handelt.

Empfehlung

Eine Betroffenheit durch diese Veröffentlichung von personenbezogenen Daten insbesondere für private E-Mail-Adressen können über den Leakchecker der Uni Bonn (<https://leakchecker.uni-bonn.de/>) sowie den HPI Identity Leak Checker (<https://sec.hpi.de/ilc/>) festgestellt werden. Auch können Angebote der ISP oder internationalen Sicherheitsforscher genutzt werden. Weitere Informationen zu den Projekten sind auf den jeweiligen Webseiten der Anbieter zu finden. Empfehlungen für den Schutz gegen Identitätsdiebstahl und was Betroffene tun können, stellt das BSI im Internet zur Verfügung (https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/ID-Diebstahl/Schutzmassnahmen/id-dieb_schutz_node.html und https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/ID-Diebstahl/Hilfe/Hilfe_Betroffene_node.html).

Zusätzlich zu den genannten Punkten werden die folgenden Verschleierungstechniken eingesetzt:

1. Erweiterungen durch Subdomains (z. B. aus wikipedia.org wird wikipedia.weitere.verschachtelte.domain.org).
2. Einbringen von Tippfehlern (z. B. wikiepedia.org anstatt wikipedia.org).
3. Einbringen von Zahlen anstelle von ähnlich aussehenden Buchstaben (z. B. w1kipedia.org).
4. Verwenden von Unicode-Zeichen, die denen in lateinischer Schrift ähneln
(kyrillisch <https://www.apple.com/> (Punycode <https://www.xn--80ak6aa92e.com>) sieht dann aus wie <https://www.apple.com/>). (IDN Homograph Attack).
5. Laden einer Phishing-Seite über Google-Translate (z. B. <https://translate.google.com/translate?hl=de&sl=en&u=https://Phishingseite.de/&prev=search>).

Eine weitere Form der Verschleierung ist das Einbinden realistischer aussehender Anmeldefenster in Form von Pop-Ups. Hierbei wird das Ziel verfolgt, Nutzerinformationen von weiteren Diensten zu erlangen.

Alternativ zum klassischen Phishing werden immer wieder legitime Webseiten mit korrekten Zertifikaten unter die Kontrolle eines Angreifers gebracht und entsprechend durch das Einbringen von Code in eine „Phishing-Seite“ umgestaltet. Dies erfolgt beispielsweise durch das direkte Kompromittieren eines Webserver oder das Einschleusen von JavaScript-Code. Eine bestimmte Gruppierung von Angreifern, die mit dieser Methode arbeitet, ist Magecart. Bei den Angriffen wurde maliziöses JavaScript eingebunden, das den Abfluss von Kreditkarteninformationen sowie Liefer-/Zahlungsadressen aus Einkaufskörben zur Folge hatte.

Insgesamt sind Meldungen zum Datenabfluss von ganzen Datenbanken mit Kundeninformationen an der Tagesordnung und lassen Diensteanbietern eine große Verantwortung zuteilwerden. Die aktuell bestätigten Daten-Leaks zeigen, dass digitale Eigenverantwortung eines jeden ein wesentlicher Bestandteil für nachhaltige Informations- und Cyber-Sicherheit darstellt. Sie zeigen zugleich die Sicherheitsgrenzen des Benutzername-Passwort-Verfahrens auf. Das BSI empfiehlt daher die Verwendung einer Zwei-Faktor-Authentisierung, sobald ein Online-Dienst dies ermöglicht. Viele Dienste haben die Funktion der Zwei-Faktor-Authentisierung standardmäßig deaktiviert, bieten diese jedoch in den Einstellungen an. Deshalb sollten Nutzerinnen und Nutzer die jeweils angebotenen Log-In-Verfahren aufmerksam prüfen. Bei Verwendung

einer Zwei- oder Mehr-Faktor-Authentisierung führt ein gestohlenes Passwort nicht unmittelbar zur Offenlegung weiterer sensibler Daten.

Die Datenschutzgrundverordnung (DSGVO) sieht für verantwortliche Betreiber seit dem 25. Mai 2018 unter bestimmten Voraussetzungen eine Meldepflicht für den Verlust und die unbefugte Offenlegung von personenbezogenen Daten gegenüber der zuständigen Datenschutzbehörde und ggf. auch gegenüber den jeweiligen Betroffenen vor. Hierdurch werden Nutzerinnen und Nutzer besser über mögliche Datenabflüsse informiert.

1.2.2 Schadprogramme

Der Begriff Schadprogramme (engl. Malware) umfasst alle Arten von Computerprogrammen, die unerwünschte oder schädliche Funktionen auf einem Computersystem ausführen können. Die Begriffe Trojaner, Viren, Würmer etc. werden in der Presse und den Medien oft synonym für alle Arten von Schadprogrammen genutzt. Schadprogramme sind fester Bestandteil der meisten Angriffsszenarien: z. B. bei der Infektion eines Clients durch Ransomware, bei der Kommunikation von Botnetzen aber auch bei APT-Angriffen.

Im vorliegenden Berichtszeitraum wurden von dem IT-Sicherheits-Unternehmen AV-Test (seit Jahren Zulieferer des BSI mit einer der größten Malware-Datenbanken, <https://www.av-test.org/de/>) insgesamt rund 114 Millionen neue Schadprogramm-Varianten registriert. Davon entfallen ca. 65 Millionen auf das Betriebssystem Windows, ca. 3,4 Millionen auf Android, ca. 0,09 Millionen auf MacOS und mehr als 39 Millionen in die Kategorie Sonstiges (dazu zählen u. a. betriebssystem-unabhängige Scripte, maliziöse Dokumente, Java-Malware usw).

Dies bedeutet im Durchschnitt fast 320.000 neue Schadprogramme pro Tag - etwas weniger als im vorherigen Berichtszeitraum. Hierbei ist anzumerken, dass die Zahlen nicht 1:1 vergleichbar mit den bisher veröffentlichten Zahlen sind. Grund dafür sind die neuen, detailreicheren Möglichkeiten der Datenerhebung, wodurch es möglich wurde, PUA (Potentially unwanted application: Anwendungssoftware, die nicht eindeutig als Malware klassifiziert werden kann) aus der Gesamtzahl herauszurechnen..

So bleiben Infektionen durch Schadprogramme wie bereits in den Vorjahren auch im aktuellen Berichtszeitraum eine der größten Bedrohungen für Privatanwender, Unternehmen und Behörden. Wie schon bei der Cyber-Sicherheits-Umfrage 2017 der Allianz für Cyber-Sicherheit, bestätigte sich dies erneut in der zuletzt durchgeführten Cyber-Sicherheits-Umfrage 2018. In 53 % der 2018 berichteten Angriffsfälle handelte es sich um Malware-Infektionen,

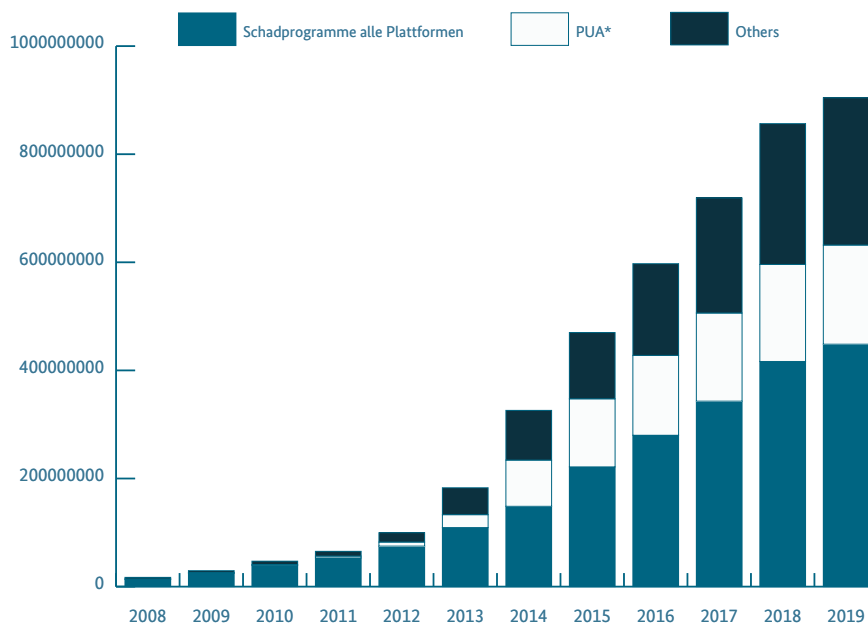


Abbildung 01 Bekannte Malware-Varianten insgesamt, Quelle: AV-Test



APT28 modifiziert Diebstahlsicherungssoftware LoJack

Sachverhalt

Mehrere Sicherheitsfirmen veröffentlichten 2018 Analysen über eine selten genutzte Schadsoftware der Tätergruppe APT28. Demnach wurde die legitime Diebstahlsicherungssoftware LoJack von den Tätern durch minimale Änderungen zu einem Rootkit umfunktioniert. Statt sich bei einem Server des Software-Herstellers zu melden, nahm die modifizierte Variante Kontakte zu Servern der Täter auf. Dadurch konnte APT28 Befehle an infizierte Rechner senden. Die Verwendung der prinzipiell legitimen Software LoJack hatte für die Täter den Vorteil, dass die Erkennungswahrscheinlichkeit durch Sicherheitsprodukte sehr gering war.

Ursache/Schadenswirkung

Die Auswirkungen der Manipulation von LoJack waren begrenzt. Die Täter manipulierten nicht bereits vorhandene LoJack-Installationen. Stattdessen installierten sie manipulierte Varianten auf Rechnern, die bisher keine Diebstahlsicherungssoftware besaßen. Dafür benötigten sie aber bereits administrativen Zugang zu den Zielsystemen. LoJack ist also kein neuer Angriffsvektor, sondern nur eine Methode, eine bereits bestehende Kompromittierung weiterzutreiben.

APT28 setzte diese Schadsoftware zudem nur sehr begrenzt ein. Sie wurde zum einen nur in bestimmten Sektoren installiert, vorrangig in militärischen Einrichtungen, und auch dort nur auf einzelnen Systemen. Die manipulierten LoJack-Varianten wurden nicht für die tägliche Arbeit der Täter im Zielnetzwerk verwendet, sondern fungierten als Rückfalloption, falls die anderen (teilweise öffentlich bekannten) Schadprogramme entdeckt und bereinigt werden sollten.

Reaktion

Dieser LoJack-Fall ist ein gutes Beispiel für Themen, die trotz großer Medienaufmerksamkeit keine grundlegend neuen oder zusätzlichen Reaktionen oder Handlungsempfehlungen bedürfen. Zum einen ist der Kreis der potenziellen Betroffenen wegen des sparsamen Einsatzes durch die Täter sehr begrenzt. Zum anderen wurde LoJack erst in nachgelagerten Phasen eines Angriffs eingesetzt und nur als ein Werkzeug von vielen. Die BSI-Empfehlungen, die sicherzustellen helfen, dass die Täter erst gar nicht Zugriff auf Systeme erhalten, blieben nach wie vor gültig.

Empfehlung

Eine Detektion des Rootkits LoJack ist deutlich schwieriger als die der anderen Tools von APT28. Daher empfiehlt das BSI, im Normalbetrieb gängige Methoden zur Erkennung von Schadsoftware und Täteraktivität zu nutzen. Erst im Fall einer Kompromittierung durch APT28 mit anderen Schadprogrammen, ist es ratsam, im Zuge der Vorfallsbewältigung auch auf die Existenz des Rootkits zu prüfen.

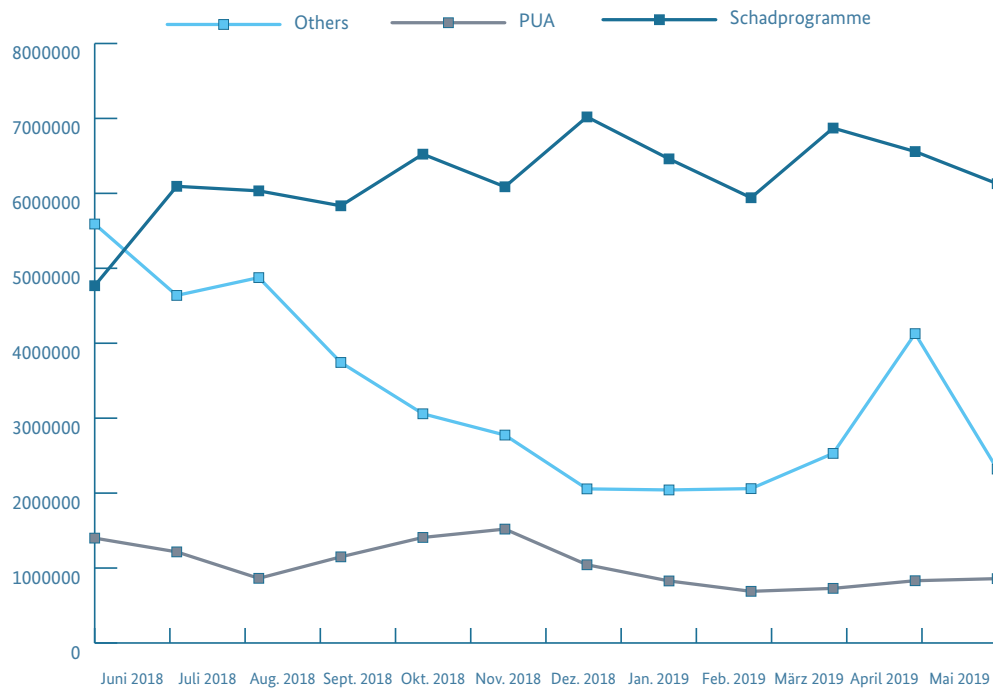


Abbildung 02 Verlauf der neuen Malware-Varianten pro Monat

*PUA: Potentially unwanted application. Bezeichnet Anwendungssoftware (oft als „Bundled“-Software vertrieben), die nicht eindeutig als Malware klassifiziert werden kann und daher unter dem Begriff „grayware“ subsumiert wird. PUA zeichnet sich insbesondere dadurch aus, dass sie i. d. R. vom Anwender 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 etc.

**Andere: u. a. betriebssystem-unabhängige Skripte, maliziöse Dokumente, Java-Malware usw.

***Schadprogramme: Betriebssystemabhängige Malware

bei denen Schadprogramme in betriebliche IT-Systeme eindringen, um schädliche Operationen durchzuführen. 87 % der Betroffenen gaben zudem an, dass die Cyber-Angriffe erhebliche Konsequenzen in Form von Betriebsstörungen und Betriebsausfällen verursachten (siehe Kapitel: 2.2.1.3 Erkenntnisse und Ergebnisse aus der Cyber-Sicherheitsumfrage der Allianz für Cyber-Sicherheit).

Auch bei den Top 10 Bedrohungen und Gegenmaßnahmen 2019 (Version 1.3, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_005.pdf) im Bereich der Systeme zur Fertigungs- und Prozessautomatisierung (Industrial Control Systems, ICS) wurden das „Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware“ sowie die „Infektion mit Schadsoftware über Internet und Intranet“ als Top-Risiken mit zunehmendem Trend identifiziert.

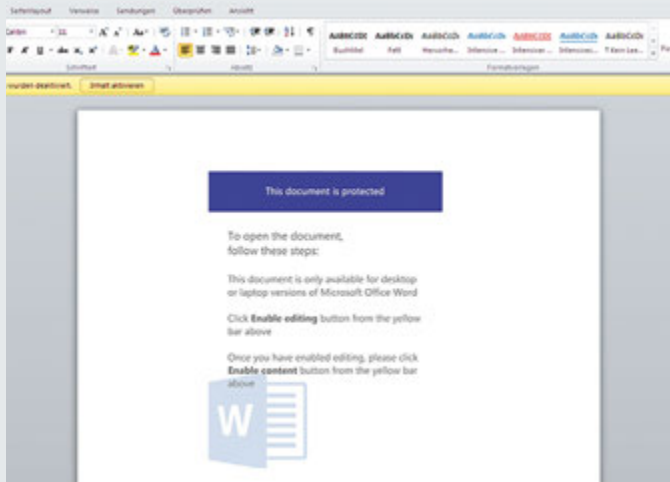


Warnung vor Schadsoftware Emotet

Sachverhalt

Emotet (auch bekannt als Feodo, Bugat) wurde erstmals 2010 als Banking-Trojaner bekannt. Spätere Varianten des Schadprogramms wurden auch als Geodo und Heodo bezeichnet. *Emotet* enthält verschiedene Module zum Ausspähen von Informationen auf infizierten Systemen sowie zum Spam-Versand und zur Verbreitung des Schadprogramms. Spam-Kampagnen mit gefälschten Rechnungen zur Verbreitung von *Emotet* sorgten bereits in den Jahren 2013 bis 2015 für zahlreiche Infektionen. Ab November 2018 wurde eine zunehmende Verbreitung der Schadsoftware *Emotet* mittels schädlicher Office-Dokumente registriert. Neu war ab Ende Oktober 2018, dass das Outlook-Harvesting-Modul nicht nur die Kontaktbeziehungen, sondern auch E-Mail-Inhalte ausgespäht hat. Diese wurden aber erst im April 2019 verwendet, um noch authentischer aussehenden Spam zu versenden. Sobald ein Rechner durch *Emotet* infiziert ist, verwendet die Schadsoftware Kontaktbeziehungen und E-Mail-Inhalte aus den Outlook-Postfächern des infizierten Systems. Diese Informationen nutzen die Täter zur weiteren Verbreitung des Schadprogramms in nachfolgenden Spam-Kampagnen, so dass die Empfänger authentisch aussehende E-Mails von Absendern erhalten, mit denen sie kürzlich in Kontakt standen.

Ab November 2018 wurde eine zunehmende Verbreitung der Schadsoftware *Emotet* durch maliziöse Office-Dokumente registriert. Mit Social-Engineering-Methoden werden potenzielle Opfer dazu gebracht, Microsoft Office-Makros (VBA-Skripte) auszuführen, die als Downloader für beliebige Schadprogramme fungieren.



Angreifer machen sich das Verhalten von Windows zur Dateityp-Erkennung zunutze, um schädliche Office-Dokumente an Sicherheitssystemen vorbei zu schleusen. Zunächst wird ein Office-Dokument als Office-2003-XML-Datei abgespeichert und erhält die Dateiendung *.xml*. Anschließend wird diese Datei umbenannt und die Endung *.xml* wird in *.doc* geändert. Gängige Datentyp-Erkennungs-Bibliotheken wie z. B. „libfile“ erkennen diese Datei folglich als *.xml* und stuften diese als weniger gefährlich ein. Windows hingegen erkennt diese Datei anhand der Dateiendung als *.doc* und öffnet diese standardmäßig mit dem installierten Office-Programm.

Abbildung 03 Screenshot eines maliziösen Office-Dokumentes, das den Nutzer auffordert, Office-Makros zu aktivieren. (Quelle: BSI)

Hinsichtlich der Kommunikation von Schadsoftware mit den dazugehörigen Command-and-Control-Servern ist ein deutlicher Zuwachs an HTTPS-Kommunikation zu beobachten. Das Verhältnis von verschlüsselter zu unverschlüsselter Kommunikation von Schadsoftware mit ihren Command-and-Control-Servern liegt für den Berichtszeitraum bei circa 15 % (HTTPS) zu 85 % (HTTP).

Ursache/Schadenswirkung

Schädliche Office-Dokumente und Skripte fungieren als Downloader und versuchen mit Social-Engineering-Methoden, die potenziellen Opfer dazu zu bringen, Office-Macros (VBA-Skripte) auszuführen. Die Office-Dokumente sind abwärts-kompatibel bis Microsoft Office 2003. Dadurch ist die Malware auf unterschiedlichen Office-Versionen lauffähig, was die Anzahl der potenziellen Opfersysteme deutlich erhöht. Das BSI rechnet künftig mit einer weiteren Zunahme an gut umgesetzten, automatisierten Social-Engineering-Angriffen dieser Art, die für die Empfänger kaum noch als solche zu identifizieren sind.

Ein Merkmal von *Emotet* ist es, dass beliebiger Schadcode nachgeladen werden kann. Ähnlich einem Baukastensystem lädt *Emotet* bisher hauptsächlich Trickbot, QBot, IcedID oder Ursnif/Gozi nach, teilweise auch Dridex, Gootkit oder Azoruit. Es ergeben sich somit für die Täter weitere Angriffsmöglichkeiten. Die Erweiterungen und Folgen von *Emotet* sind u. a.:

- Adaption von Techniken, die bisher vor allem bei APT-Angriffen beobachtet wurden
 - „Outlook-Harvesting“ auf infizierten Systemen
 - Diebstahl der Historie und gespeicherter Zugangsdaten aus Webbrowsern
 - Nachladen beliebiger Schadsoftware
 - Ausnutzung alter, nicht-gepatchter Schwachstellen
 - Schäden durch Produktionsausfälle
- Die Entwickler von in der Breite verteilter Schadsoftware wie *Emotet* oder *Trickbot* adaptieren zunehmend Methoden zur Weiterverbreitung in lokalen Netzwerken (lateral movement), die bisher vor allem bei APT-Angriffen beobachtet wurden. Sie nutzen zunächst eine sehr breit angelegte Kampagne, wählen dann aber opportunistisch sehr selektiv Ziele aus, bei denen sie sich weiter ausbreiten und weitere Malware nachladen. Die Ausbreitung im Netzwerk dient auch dazu, Backups zu finden und zu manipulieren bzw. zu löschen. Die folgende Abbildung visualisiert die neue Vorgehensweise:

Mehrstufiger Schadprogrammangriff mit APT-artiger Vorgehensweise

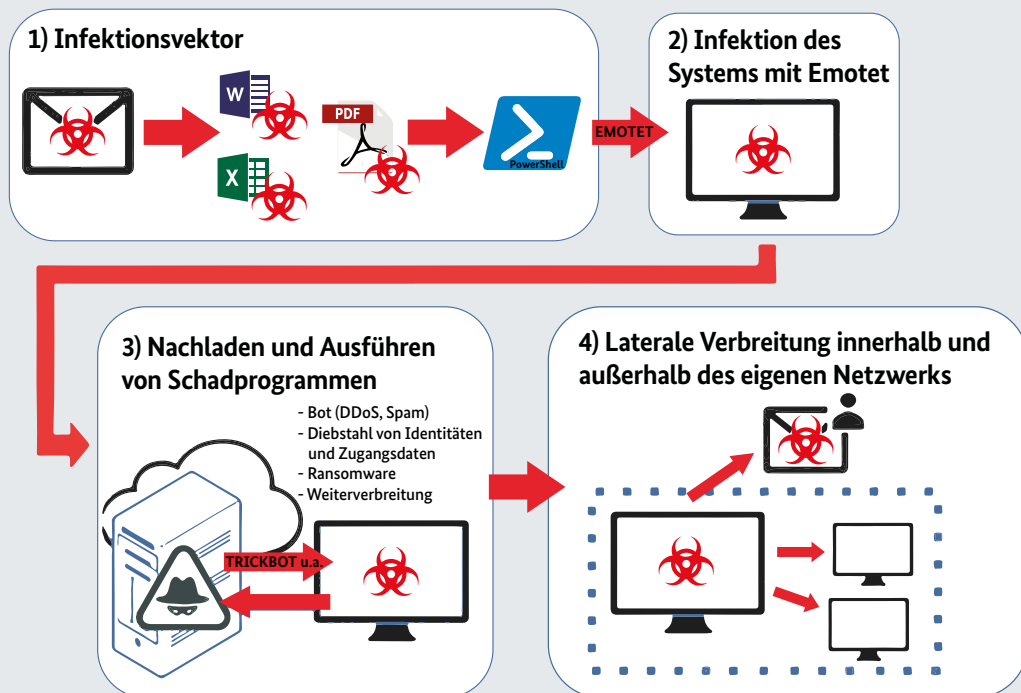


Abbildung 04 Grafiken: <https://www.fortinet.com/resources/icon-library.html>, Microsoft, Adobe

Dem BSI sind mehrere Fälle bekannt, in denen Ransomware nachgeladen und Unternehmensdaten verschlüsselt wurden. Die Folge waren Produktionsausfälle, ganze Unternehmensnetzwerke mussten neu aufgebaut werden. Für Privatanwender kann eine Infektion den Verlust von Daten, insbesondere wichtiger Zugangsdaten, bedeuten.

Reaktion

Auch „kleinere“ Infektionen durch eine in der Fläche verteilte Malware wie Emotet müssen unmittelbar behandelt werden und Zugangsdaten geändert werden, weil anderenfalls über diesen Eintrittsweg noch weitaus größere Schäden entstehen können.

Empfehlung

Folgende Maßnahmen erhöhen generell die Sicherheit gegen Emotet: zeitnah Sicherheitsupdates für Betriebssystem und Anwendungen installieren, regelmäßig Offline-Backups ausführen, Monitoring von Logdaten implementieren, nachhaltige Sensibilisierung von Nutzern gegen Social-Engineering durchführen sowie eine Netzsegmentierung von Produktions- und Büronetzwerken realisieren. Weitere Informationen zu Emotet gibt es auf der Webseite „BSI für Bürger“:

<https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/emotet.html>.

1.2.3 Ransomware

Ransomware ist mit dem Angriff von WannaCry im Jahr 2017 der breiten Öffentlichkeit bekannt geworden und bezeichnet Schadsoftware, die den Zugriff auf den eigenen Rechner oder die eigenen Dateien verwehrt oder einschränkt. Dies

wird normalerweise durch eine am Bildschirm eingeblendete Nachricht mitgeteilt. Manchmal ist die Mitteilung nur vorge-täuscht oder sind Einschränkungen leicht zu umgehen.

Das Ziel von Ransomware ist, die Zahlung eines Lösegelds (englisch: Ransom) oder andere Handlungen zu fordern, bevor die Ressourcen wieder freigegeben werden. In den meisten Fällen wird die Zahlung mit einer Krypto-Währung wie Bitcoin oder Ethereum gefordert, um die Anonymität der Täter zu wahren. Inzwischen sind die Zahlungsströme dieser Währungen besser zu beobachten, so dass teilweise

Erkenntnisse über geleistete Lösegeldzahlungen einzelner Ransomware-Varianten bestehen. Es wird deutlich, dass die Zahlung von Lösegeld den Opfern in vielen Fällen keinen Vorteil bringt. So konnte z. B. beobachtet werden, dass Täter nach der Zahlung nicht in der Lage waren, die Daten zu entschlüsseln, keine Entschlüsselungsmöglichkeit anboten, weitere Forderungen stellten oder gar nicht reagierten.



Cyber-Angriff auf Aluminiumkonzern

Sachverhalt

Ein norwegischer Aluminiumkonzern ist in der Nacht zum 19. März 2019 Opfer eines Cyber-Angriffs durch die Ransomware LockerGoga geworden. Das Unternehmen hat weltweit nach eigenen Angaben 35.000 Mitarbeiter in 40 Ländern und erwirtschaftete 2017 einen Umsatz von ca. 11 Mrd. Euro. Das Kerngeschäft ist die Aluminiumproduktion, daneben gehört das Unternehmen zu den drei größten Stromerzeugern Norwegens.

Es wurde festgestellt, dass die IT-Systeme in den meisten Geschäftsfeldern betroffen sind. Die Anlagen wurden zunächst als erste Reaktion vom Netz genommen und die Produktion wurde weitestgehend auf manuellen Betrieb umgestellt. Es wurde Lösegeld in unbekannter Höhe gefordert, aber vom Unternehmen nicht gezahlt. Es nutzte stattdessen die vorhandenen Backups, um den Betrieb wiederherzustellen. Die Webseite war als Folge der Angriffe zeitweise nicht mehr erreichbar. Noch vier Wochen nach dem Vorfall wurden viele Bereiche manuell betrieben.

Ursache/Schadenswirkung

Beim Angriff kam die Ransomware LockerGoga zum Einsatz. Pressemitteilungen zufolge gab es im Vorfeld Manipulationen des Active Directory und den Austausch von Admin-Passwörtern, Abmeldungen eingeloggter Nutzer und die Deaktivierung von Netzwerkgeräten. Damit kann von einem gezielten Angriff mit individueller Vorbereitung auf das konkrete Opfer ausgegangen werden. LockerGoga war erstmals Anfang des Jahres bei einem französischen Unternehmen eingesetzt worden und kurz nach der Attacke auf den Aluminiumkonzern noch bei zwei US-Unternehmen der chemischen Industrie zum Einsatz gekommen.

Dem Unternehmen ist nach eigenen Angaben alleine in der ersten Woche nach dem Cyber-Angriff ein wirtschaftlicher Schaden in Höhe von ca. 35 bis 43 Millionen US-Dollar entstanden. Während dieser Woche stand die Produktion in den am stärksten betroffenen Bereichen nahezu still.

Der Aluminiumpreis stieg in den ersten beiden Tagen nach dem Vorfall deutlich an. Der Aktienkurs selbst nahm keinen Schaden und stieg in der Folge sogar.

Reaktion

Der Konzern informierte die Öffentlichkeit und Börse umgehend (u. a. über Facebook) über den Cyber-Angriff. Am Tag nach der Attacke gab es eine Pressekonferenz und auch in den folgenden Wochen wurde die Öffentlichkeit über den Stand der Maßnahmen informiert. Das Unternehmen wurde für sein Vorgehen (keine Lösegeldzahlung, Backup-Nutzung, Informationspolitik) gelobt. Dieses Verhalten entspricht auch den Empfehlungen des BSI.

Empfehlung

Der Fall zeigt, dass der Schutz vor Ransomware weiterhin in einer überprüften Backup-Strategie besteht, die eine erfolgreiche Wiederherstellung der Daten sicherstellt. Die zunehmende Fokussierung auf größere Ziele wie Unternehmen (mit erwartbarer hoher Motivation zur Zahlung von Lösegeldern) lassen jedoch weitere Empfehlungen sinnvoll erscheinen. Dazu gehören z. B. das unternehmensweite Managen von Makros, der Ausschluss des Zugriffs auf Dokumentenverzeichnisse für ausführbare Dateien, die Deaktivierung standardmäßig automatisierbarer Systemteile wie z. B. des Scriptinghosts. Um die Verbreitung von Schadsoftware im Unternehmens-Netzwerk unabhängig von seiner Ausdehnung über einen oder mehrere (nationale oder internationale) Standorte zu unterbinden, ist zudem eine kleinteiligere Segmentierung des Netzwerks von Vorteil. Der Fernzugriff von außen sollte weitestgehend vermieden werden und wo nötig, jede Zugriffsmöglichkeit mit Passwortschutz ausgestattet sein, die strikte Passwortrichtlinien verfolgt (vorgeschriebene Zeichenbereiche und Länge).

Um dieser Konstellation zu entgehen und den Tätern keine Anreize zu bieten, empfiehlt das BSI auch weiterhin, kein Lösegeld zu zahlen.

Ransomware verbreitet sich über diverse Angriffsvektoren. Alle Zielgruppen können von folgenden Angriffsvektoren betroffen sein:

- Spam-E-Mails mit Schadsoftware, die sich im Anhang befindet oder über URLs referenziert wird.
- Drive-By-Exploits (Schwachstellen in Browsern, Browser-Plug-Ins oder Betriebssystemen), die durch den Aufruf einer infizierenden Webseite oder darauf platzierter Werbung (potenziell ohne weitere Interaktion durch den Nutzer) ausgenutzt werden.
- Exploit-Kits verwalten verschiedene Schwachstellen in unterschiedlichen Produkten und stellen sowohl die Angriffsart als auch den Transport der Schadsoftware dem Täter auf Knopfdruck zur Verfügung.

Unternehmen und andere Einrichtungen mit komplexerer IT-Infrastruktur können zudem von folgenden Angriffswegen betroffen sein:

- Ausnutzung von Schwachstellen oder Erraten von schwachen Passwörtern in öffentlich zugänglichen Webservern. Für das Ausspähen weiterer Passwörter im internen Netz gibt es ebenfalls weit verbreitete Schadsoftware.
- Schwachstellen in Fernwartungs-Werkzeugen (Remote Administration Tools, RAT) werden verwendet, um auf die zu wartenden Systeme zuzugreifen. Dies führt oft bereits im ersten Schritt dazu, dass der Angreifer mit weitgehenden Rechten ausgestattet ist.
- Nach der Infektion des Zielsystems nutzt die Schadsoftware u. a. Schwachstellen im Betriebssystem, um als scheinbar legitimer Prozess nicht frühzeitig entdeckt zu werden.

Seit dem Jahr 2016 ist ein starker Anstieg der Gefährdung durch Ransomware festzustellen. Auf starke mediale Resonanz stießen hauptsächlich WannaCry und NotPetya/ExPetr im Jahr 2017. Teilweise dauern rechtliche Auseinandersetzungen zu Leistungsansprüchen bei Versicherungen bis heute an. Hintergrund ist, dass es sich bei NotPetya vermutlich um einen Sabotageakt und nicht um Ransomware mit dem Ziel einer Erpressung handelte. Die Schäden können durchaus weit über die Höhe des geforderten Lösegelds hinausgehen. Dies wird besonders deutlich, wenn größere Firmen zum Opfer werden.

Neuere Vorfälle aus dem Jahr 2019 hatten nicht die gleiche mediale Aufmerksamkeit wie die zuvor genannten, zeigen aber verschiedene Entwicklungen auf. Die seit 2018 bekannte Ransomware namens GandCrab zeigt eine agile Entwicklung, die sogar eine Versionsnummer beinhaltet, was für eine gute Organisation der Angreifer spricht. GandCrab stellt ein Beispiel für Ransomware-as-a-Service (Personalisierte Ransomware wird als Dienstleistung angeboten) dar und attackiert tendenziell in der Fläche. Andere Ransomware-Varianten scheinen sich dagegen auf gezieltere Angriffe zu fokussieren:

- SamSam ist eine der aktiveren Ransomware-Varianten und wurde durch den Angriff auf die Stadt Atlanta bekannt. Dieser Angriff markierte eine stärkere Hinwendung zu gezielten Angriffen auf Organisationen.
- SamSam, BitPaymer und CrySIS zeigten, dass aktive Fernwartungswerkzeuge ein beliebtes Einfallstor sind. Diese werden individuell z. B. mit veröffentlichten Zugangsdaten oder erratenen Passwörtern, aber auch über Schwachstellen attackiert.
- Während des letzten Jahres wurden verschiedene Ransomware-Attacken auf Häfen und Flughäfen, Unternehmen im Logistikbereich (Container), Zeitungen und Restaurantketten gemeldet. Diese trafen zwar zum größten Teil Unternehmen außerhalb Deutschlands, aber auch innerhalb Deutschlands wurden z. B. Krankenhäuser angegriffen.
- Die andauernde Gefahr wird auch durch die Ransomware-Variante Ryuk illustriert. Gezielte Beobachtung von verwendeten Bitcoin-Adressen lassen auf ein erbeutetes Lösegeld von mindestens 600.000 US-Dollar schließen. Weiterhin tritt Ryuk seit dem Jahreswechsel 2018/2019 vermehrt in Verbindung mit Emotet/Trickbot-Kampagnen auf, was die erhöhte Modularität bei Schadsoftware allgemein, insbesondere aber bei Ransomware zeigt (siehe Vorfall: Warnung vor Schadsoftware Emotet auf Seite 13).

Wie groß der Schaden durch Ransomware werden kann, selbst wenn ein Unternehmen eine gute Backup- und Incident-Response-Strategie hat, zeigt sich am Beispiel eines norwegischen Aluminiumkonzerns (siehe Vorfall: Cyber-Angriff auf Aluminiumkonzern auf Seite 16). Das norwegische Unternehmen wurde im März 2019 Opfer eines Ransomware-Angriffs und stellte, ohne ein Lösegeld gezahlt zu haben nach einer Woche laut eigener Angabe bereits einen Verlust von ca. 40 Millionen Euro fest, obwohl es versuchte, alle Daten aus den Backups zu rekonstruieren. Zum Einsatz kam die relativ neue Ransomware-Variante LockerGoga, die augenscheinlich zunächst an einer

Organisation ausprobiert wurde und dann gleich mehrere Unternehmen in kurzem zeitlichen Abstand traf, was auf ein sehr geplantes Vorgehen schließen lässt.

Auch in mehreren anderen Fällen waren die Folgen von Ransomware-Angriffen schwerwiegend. Berichtet wurde von Komplettausfällen von Rechnern und Netzwerken bis hin zu Ausfällen ganzer Produktionsanlagen. Neben der Industrie waren auch immer wieder Einrichtungen des Gemeinwesens Ziel solcher Angriffe, wie zum Beispiel Krankenhäuser in Deutschland oder Kommunalverwaltungen in den USA. Dabei konnte Folgendes beobachtet werden: Die Angriffe richteten sich gezielt auf zentrale Dienstleister. War der Angriff erfolgreich, konnten dann die Systeme der Kunden oder angeschlossene Netzwerke infiziert werden. Daher zeigt sich, dass bei der Digitalisierung vieler Institutionen die Gefährdung durch eine hohe Konnektivität in vielen Fällen unterschätzt wurde und zunächst nur die Funktionalität und die Bedienung möglichst vieler Nutzer im Vordergrund stand.

Zusammenfassend sind folgende Entwicklungen im Bereich Ransomware festzustellen:

- Wie kommerzielle Software auch, wird Ransomware modular entwickelt, um in Zielsysteme einzudringen und sich zu verteilen. Nur noch das Modul der eigentlichen Verschlüsselung/Blockierung unterscheidet sie von anderen Malware-Arten. Beim Geschäftsmodell Ransomware-as-a-Service wird teilweise sogar die Gewinnbeteiligung vorab ausgehandelt.
- Ransomware richtet sich mehr und mehr auf größere Unternehmen als Opfer, die eher bereit sind, ein hohes Lösegeld zu zahlen. Dabei werden Methoden für das Eindringen verwendet, die an das jeweilige Unternehmen angepasst sind.
- Wird eine flächendeckende Angriffsart gewählt, so ist zumindest eine hohe Agilität erforderlich, um sich vorhandenen Schutzmechanismen (freie Entschlüsselungswerkzeuge, frühzeitige Entdeckung) zu entziehen. Dies führt zu einer ständigen Anpassung der Angriffsvektoren (Schwachstellen, Social-Engineering) und Verschlüsselungsalgorithmen.

Daher sollten folgende Überlegungen beachtet werden:

- Basis für das Überstehen eines erfolgreichen Ransomware-Angriffs ist immer noch die Vorsorge durch ein funktionierendes Backup der wertvollen bzw. kritischen Daten. Das genannte Beispiel macht jedoch deutlich, dass es auch trotz guter Backup- und Incident-Response-Strategie zu großen Schäden kommen kann.

- Die durch Systemerneuerung und Einspielen der Backups verlorene Arbeitszeit verursacht in Unternehmen zwar in allen Fällen Kosten. Je nachdem, welche kritischen Workflows eines Unternehmens von der durch die Ransomware eingeschränkte IT abhängen, entstehen noch wesentlich größere Kosten durch den temporären Ausfall: Schäden an Betriebsanlagen, Beschaffung von teuren Übergangslösungen, Unsicherheit bei Personal und Kunden sowie mangelndes Vertrauen in den Geschäftspartner.
- Die Angriffsfläche ist so gering wie möglich zu halten: Dazu gehören die Minimierung der Zahl und Variabilität der von außen zugänglichen Rechner, eine möglichst zeitnahe Aktualisierung der Betriebssysteme, Server- und Anwendungssoftware sowie eine kluge und restriktive Auswahl der Personen, die einen Zugang zum System über das Internet benötigen. Bei den nötigen Zugängen sind hohe Anforderungen an die Passwortrichtlinien und die verwendeten Protokolle zu stellen.
- Sollte es trotz aller Vorsorge zu einer Infektion kommen, wird eine sachgerechte interne Segmentierung der Netze helfen, das Ausmaß der Schäden zu begrenzen.

1.2.4 Distributed Denial of Service (DDoS)

Wenn eine Webseite nicht mehr erreichbar ist, Netzwerkdienste ausfallen oder kritische Geschäftsprozesse wegen Überlastung blockiert werden, ist oftmals ein DDoS-Angriff die Ursache. Diese DDoS-Angriffe werden von Cyber-Kriminellen meist genutzt, um gezielt Schaden anzurichten, ihre Opfer zu erpressen, oder Aufmerksamkeit für eine eigene Sache zu erregen, aber auch, um andere Attacken zu verschleiern oder erst zu ermöglichen. Dabei werden die Angriffe häufig mittels einer großen Anzahl von Computern, ggf. Servern, parallel durchgeführt.

Die Auswirkungen von DDoS-Angriffen können beträchtlich sein. Sie können für die betroffenen Institutionen einen großen wirtschaftlichen Schaden verursachen und auch einen Reputationsverlust nach sich ziehen. Deutsche Unternehmen mussten laut einer Studie des Unternehmens Netscout 2018 einen DDoS-Gesamtschaden von rund vier Milliarden Euro verzeichnen (<https://www.internetworld.de/technik/hacker/ddos-attacken-verursachen-schaeden-in-milliardenhoehe-1700104.html>, <https://www.netscout.com/report/>).

Ziele von DDoS-Angriffen sind in der Regel aus dem Internet erreichbare Dienste. Insbesondere Systeme, deren Ausfall auf Kundenseite deutlich wahrgenommen wird, stehen im Fokus von Angreifern.

Die Lage im Bereich von DDoS-Angriffen ist gekennzeichnet durch mehrere, sich überschneidende Entwicklungen:

- die stetige Spezialisierung bei der Ausführung von Angriffen durch Anwendung neuer Angriffsvektoren (z. B. „Memcached“ aus dem vergangenen Berichtszeitraum – vgl. „Die Lage der IT-Sicherheit in Deutschland 2018“), durch zielgerichteten Zusammensetzung von DDoS-Angriffen (Multivektor-Angriffen) oder durch den Einsatz neuer Angriffswerkzeuge (DDoS aus der Cloud),
- die Existenz von DDoS-Booterdiensten (z. B. der mittlerweile vom Netz genommene „webstresser.org“), die es Angreifern ohne technische Kenntnisse immer leichter macht, großvolumige Attacken zu starten, sowie
- anlassbezogene DDoS-Aktivitäten zu besonderen Ereignissen im E-Commerce-Umfeld oder im Gaming-Umfeld.

Multivektor-Angriffen machten im vierten Quartal 2018 den Großteil aller DDoS-Angriffe aus. Auf sie entfielen 59 % der Attacken. Im Vorjahreszeitraum lag der Wert noch bei 45 %. Bei diesen Angriffen konnten zugleich bis zu neun verschiedene Angriffsvektoren beobachtet werden. Die wichtigsten Vektoren waren NTP Monlist, CLDAP, DNS Reflection und SSDP Reflection (<https://www.link11.com/de/blog/link11-ddos-statistiken-fuer-q4-2018-veroeffentlicht/>).

Mit der Zusammenstellung unterschiedlicher Angriffsvektoren kann sowohl auf der

- Netzwerkebene (Angriffe auf den OSI-Layern 3 [Network Layer] und 4 [Transport Layer] wie z. B. SYN-Flooding, TCP-Connection-Flooding, DNS Amplification Attacks, Tribe Flood Network [TFN], Ping of Death) als auch auf der
- Anwendungsebene (Angriffe auf dem OSI-Layer 7 [Application Layer] wie z. B. HTTP-Floods, Slow Attacks, SMTP-Floods)

gleichzeitig die Wirkung im Angriffsziel entfaltet werden. Anstatt die Wirkung des Angriffs alleine durch eine Überlastung herbeizuführen, können zusätzlich parallel Schwachstellen auf Anwendungs- und Netzwerkebene attackiert werden.

Der Missbrauch von modernen Cloud-Lösungen ist insbesondere bei der Ausführung von DDoS-Attacken durch Cyber-Kriminelle in der Vergangenheit stetig gestiegen.

Damit Angreifer das technische Potenzial der Clouds für ihre Angriffe nutzen können, müssen sie die Kontrolle über einzelne Serversysteme oder Segmente der Cloud-Infrastruktur erlangen. Hierzu setzen Angreifer Schadsoftware zur Kompromittierung von Cloud-Servern ein oder mieten für sie geeignete Public-Cloud-Dienstleistungen an, um dadurch die hohe Anbindungsbandbreite der Cloud-Services für ihre Angriffe ausnutzen zu können.

Auswertungen auf Basis von Daten von Link 11 (www.link11.com) zeigen, dass im Winter 2018 der bisherige Höchststand erreicht wurde: Mit 59 % wurde mehr als jede zweite Attacke über kompromittierte oder missbräuchlich angemietete Cloud-Server ausgeführt. Im Sommer 2018 lag der Anteil von Cloud-basierten DDoS-Attacken in Mitteleuropa bei 52 %, im Januar 2016 noch bei 2 %.

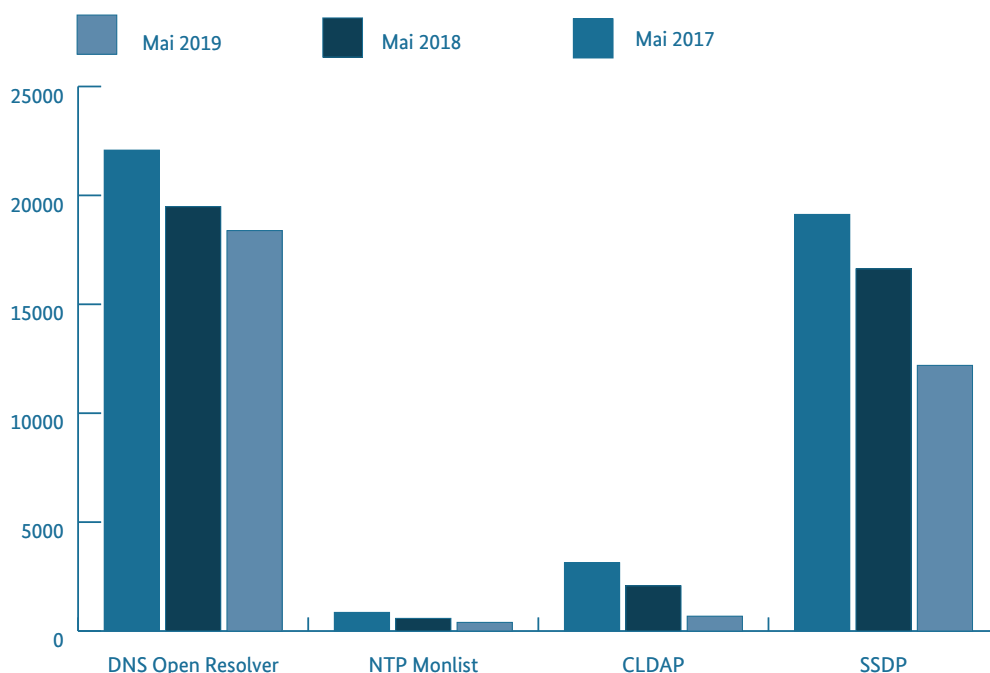


Abbildung 05 BSI, europol, security-insider

Fast jeder Cloud-Dienstleister wurde bereits von Kriminellen zur Durchführung von DDoS-Attacken missbraucht, wobei einige Cloud-Anbieter von der rechtswidrigen Nutzung öfter betroffen waren als andere. Für Kriminelle stehen besonders Cloud-Server im Fokus, auf denen Memcached- oder SSDP-Dienste installiert sind. Public-Cloud-Server von Microsoft Azure, Amazon Web Services und Alibaba werden am häufigsten zur Durchführung von DDoS-Angriffen ausgewählt. Die Cloud-Lösung von Google wird hingegen deutlich seltener für kriminelle Zwecke genutzt. (Link11 DDoS Report Q3/18)

Angreifern auch ohne technische Kenntnisse wird es immer leichter gemacht, wirksame DDoS-Angriffe durchzuführen. Dahinter steht im Wesentlichen eine wachsende „Dienstleistungsindustrie“ für „Cybercrime-as-a-Service“. Insbesondere im Bereich DDoS werden Angriffe als Booterdienste angeboten. Der Aufbau eines Booterdienstes ist vergleichsweise einfach und kostengünstig. Er basiert auf dem Missbrauch offen aus dem Internet erreichbarer Serverdienste und dem Aufbau einer Infrastruktur, um auf diese Dienste zugreifen zu können. Einer der bekanntesten Anbieter „webstresser.org“ offerierte Multi-Gigabit-DDoS-Angriffe im „Abo“ für nur 15 US-Dollar pro Monat, bis die Seite schließlich Ende April 2018 in der Operation „Power Off“ durch internationale Strafverfolgungsbehörden vom Netz genommen wurde. Allerdings traten bereits kurze Zeit nach dem Takedown neue Dienstleister an dessen Stelle.

Durch die Nutzung von DDoS-Diensten werden Angreifer Werkzeuge an die Hand gegeben, mit denen sie in die Lage versetzt werden, mit sehr wenig Geld und wenig bis gar keinem technischen Fachwissen hochwirksame DDoS-Angriffe auszulösen. Auf das Konto der Webstresser-Dienstleistungen gingen im Jahr 2018 überaus erfolgreiche Attacken gegen mehrere niederländische Banken und zahlreiche andere Finanz- und Regierungsdienstleister in den Niederlanden, bei denen eine Vielzahl von Kunden tagelang keinen Zugang zu ihren Bankkonten hatten.

CERT-Bund erhält täglich aus verschiedenen Quellen Informationen zu IP-Adressen, unter denen sich mit Schadprogrammen infizierte Systeme befinden. Dabei kann es sich zum Beispiel um Infektionen mit Online-Banking-Trojern oder auch Spam-Bots handeln. Diese Informationen werden auf Basis der IP-Adressen an die jeweils zuständigen deutschen Netzbetreiber und Provider übermittelt. Da sich insbesondere die IP-Adressen von privaten Internetanschlüssen häufig (meist täglich) ändern (sog. dynamische IP-Adressen), können die IP-Adressen nur von dem jeweils zuständigen Provider seinen einzelnen Kunden zugeordnet werden, um diesen zu benachrichtigen. Daher werden täglich alle jeweils betroffenen IP-Adressen an die zuständigen Netzbetreiber gemeldet. Im Berichtszeitraum wurden rund 11,5 Millionen solcher Meldungen übermittelt.

Hinweis: Die Zahlen für NTP Monlist sind vergleichsweise gering. Der Missbrauch dieses Dienstes ermöglicht jedoch weitaus höhere Verstärkungsfaktoren (Amplification).

Analysen des BSI zu Vorfällen am „Black Friday“ und „Cyber Monday“ zeigen, dass an umsatzstarken Tagen im Bereich E-Commerce die Gefahren, die von DDoS-Angriffen ausgehen, besonders groß sind. Die Angriffe können dabei mehrere Stunden anhalten. Der entstehende Umsatzeinbruch ist an solchen konsumstarken Tagen besonders gravierend (siehe Vorfall DDoS-Angriffe zum Black Friday und Cyber Monday auf Seite 22 und 23).

Alles in allem lässt sich die Bedrohungslage im Bereich DDoS als konstant hoch beschreiben. Dabei wird der Erfolg eines DDoS-Angriffs nicht mehr davon abhängig gemacht, ob die Angriffsbandbreite ausreicht, um ein Zielsystem mehr oder weniger lange vom Netz zu nehmen. Das Spektrum der DDoS-Angriffstechnologie erweitert sich permanent um neue Angriffsvektoren, Angriffsmethoden (z. B. Multivektor-Attacken) und Angriffswerkzeuge (z. B. DDoS aus der Cloud). Die DDoS-Dienstleistungsindustrie fungiert dabei als „Distributionssystem“ für DDoS-Angriffstechnologie und rollt die aktuellen Entwicklungen im DDoS-Segment in der Breite aus.

Bei den Multivektor-Attacken wird das Überlasten mit Attacken auf Schwachstellen auf der Anwendungs- und Netzwerkebene kombiniert, wogegen man sich nur schwer schützen kann.

Durch die serverbasierten Botnetze (Angriffe aus der Cloud) lassen sich enorme Ressourcen aktivieren. Während einzelne Systeme wie IoT-Geräte, Bots oder PC-Systeme in der Regel mit nur wenigen Mbit/s an das Netz angebunden sind, bieten die Cloud-Provider Anbindungen von 1 bis 10 Gbit/s. Nach Messungen von Link11 erreichten die Peaks im Angriffsbandbreite über die Cloud in den vergangenen Monaten immer wieder Werte von über 150 Gbit/s, in Spitzenfällen sogar Werte von bis zu 300 Gbit/s.

Angreifer ohne technische Kenntnisse können wie beschrieben auf Booterdienste zurückgreifen. Eine Untersuchung des BSI von Mitte 2017 und aktuelle Analysen von Angriffen zeigen, dass die betrachteten Booterdienste eine Vielzahl der aktuellen Angriffsvektoren zur Zusammenstellung von Angriffen nach dem Baukastenprinzip anbieten. Statt individuelle Schutzmaßnahmen gegen die Vielzahl von DDoS-Angriffsvektoren zu implementieren, sind Abwehrmaßnahmen erfolgversprechender, die bereits vor der Anbindung des Betreibers dynamisch Angriffe erkennen und individuelle Maßnahmen zur Bereinigung des Datenstroms einleiten. Als Service für Unternehmen als auch Betreiber größerer Webseiten hat das BSI am 20. September 2018 eine Übersicht qualifizierter DDoS-Mitigations-Dienstleister veröffentlicht.

1.2.5 Botnetze

Durch die Nutzung von Botsoftware haben Cyber-Kriminelle Zugriff auf eine große Zahl von fremden Systemen (Computer, Smartphones, Router, IoT-Geräte etc.) und können diese für eigene Zwecke missbrauchen. Neben dem Abgreifen persönlicher Daten des Anwenders und Betrug beim Onlinebanking können auch die Ressourcen des gekaperten Systems von einem Angreifer missbraucht werden, um beispielsweise Kryptowährungen zu berechnen oder DDoS-Angriffe durchzuführen. Aufgrund eines modularen Aufbaus ist aktuelle Schadsoftware in der Lage, ihre Funktionalitäten durch das Nachladen von Erweiterungen dynamisch anzupassen oder zu erweitern. Somit können die Betreiber eines Botnetzes flexibel dessen Einsatzzweck verändern und an aktuelle Gegebenheiten individuell anpassen.

Im Zeitraum dieses Berichts wurden Botnetze hauptsächlich zum Informationsdiebstahl, zum Betrug beim Onlinebanking sowie zur Verteilung von Schadprogrammen genutzt. Auch wenn die Anzahl der DDoS-Bot-Netze auf Mirai-Basis stieg, konnte keine Zunahme botnetzbasierter DDoS-Angriffe beobachtet werden. Die Beobachtungen des BSI legen nahe, dass Botnetze im Vergleich zu anderen Angriffsmethoden seltener für DDoS-Angriffe genutzt werden, da Angreifern kostengünstige und leicht zugängliche Alternativen zur Verfügung stehen wie z. B. DDoS-Booterdienste (siehe 1.2.4 DDoS). Viele neue Mirai-Varianten ergänzten die ursprüngliche Version um neue Infektionsmechanismen und erweiterten damit das Portfolio möglicher infizierter Systeme um zusätzliche Rechnerarchitekturen oder Geräteklassen wie beispielsweise Webserver oder Enterprise-Systeme. Wie bereits im Vorjahr konnte im Berichtszeitraum ein genereller Anstieg an IoT-Botnetzen festgestellt werden, die auf Basis internetfähiger Heimelektronik aufgebaut wurden. Medienberichten und BSI-eigenen Recherchen zufolge fand der Großteil der Infektionen jedoch im nicht-europäischen Ausland statt.

Ebenso wurden verstärkt mit Botsoftware infizierte Android-Systeme beobachtet, hier jedoch mit einer vergleichsweise hohen Infektionsrate in Deutschland. Auffällig war, dass die betroffenen Geräte in einigen Fällen bereits ab Werk mit einer Infektion ausgeliefert wurden (siehe Vorfall: Vorinstallierte Schadsoftware auf Android-Geräten auf Seite 24). Die Schadsoftware ging dabei über reinen Informationsdiebstahl hinaus und ermöglichte einen Vollzugriff auf die betroffenen Geräte. Die Mehrzahl der beobachteten Android-Botnetze hatte den Abfluss von persönlichen Daten zum Ziel, war aber auch in der Lage, weitere Module nachzuladen, um zusätzliche Schadfunktionalitäten hinzuzufügen.

Im Bereich der Windows-basierten Botnetze ist Emotet hervorzuheben, ein Schadprogramm, das bereits seit mehreren Jahren aktiv ist und insbesondere in diesem Berichtszeitraum größere Infektionen in Deutschland verursacht hat. Neben einer Vielzahl von Privatanwendern wurden auch größere Unternehmen befallen und durch nachgeladene Schadsoftware wie beispielsweise Trickbot teilweise vollständig lahmgelegt (siehe Vorfall: Warnung vor Schadsoftware Emotet auf Seite 13).

Im Berichtszeitraum wurden täglich bis zu 110.000 Botinfektionen deutscher Systeme registriert und über das BSI an die deutschen Internet-Provider gemeldet. Die Provider benachrichtigen ihrerseits die betroffenen Kunden über die Infektion und stellen teilweise weiterführende Informationen zur Bereinigung der Systeme bereit. Zur Erkennung von Botnetzinfektionen werden Sinkhole-Systeme verwendet, die anstelle der regulären Command-and-Control-Server die Kontaktanfragen von Bots entgegennehmen (eine Beschreibung des Sinkholing-Verfahrens findet sich unter https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/BotNetze/Avalanche/FAQ/botnetz_faq_node.html#faq8606246).

Die Bedrohungslage durch Botnetze ist wie auch in den Vorjahren anhaltend hoch. Abhängig von der Auswahl der beobachteten Botnetze und der verwendeten Domänen der Steuerungsserver können die Zahlen der sichtbaren Infektionen stark schwanken. Weil eine vollständige Erfassung aller existierenden Botnetzinfektion nicht möglich ist, bilden die aus dem Sinkholing ermittelten Zahlen stets eine Untergrenze. Erfahrungen aus Botnetzabschaltungen haben gezeigt, dass die Dunkelziffer deutlich höher liegt. Insbesondere im privaten Bereich lässt sich digitale Sorglosigkeit feststellen, ausgedrückt zum Beispiel durch täglich neue Botnetz-Infektionsmeldungen, die sich mit einfachen Basismaßnahmen verhindern ließen.

Wie die aktuellen Entwicklungen zeigen, liegt der Fokus der Angreifer inzwischen auf mobilen Endgeräten und IoT-Systemen. Weil insbesondere diese zunehmende Verbreitung finden und auch kontinuierlich weitere Bereiche des täglichen Lebens erschließen, bieten sie eine stetig breiter werdende Angriffsfläche. Erschwerend kommt hinzu, dass insbesondere IoT-Geräte primär für den Massenmarkt produziert werden und zur Minimierung der Herstellungskosten oft die Funktionalität gegenüber der Sicherheit in den Vordergrund gestellt wird. So werden viele Systeme in einem unsicheren Zustand ausgeliefert und erhalten wenig bis gar keinen Herstellersupport in Form von Sicherheitsupdates oder Fehlerbehebungen. Aufgrund dieser Faktoren sind IoT-Geräte prädestiniert für Angriffe. Hier ist es notwendig, die Hersteller in die Pflicht zu nehmen, sicherere Produkte auf den Markt zu bringen.



DDoS-Angriffe zum Black Friday und Cyber Monday

Black Friday

Am Black Friday (23. November 2018) verzeichnete Link11, ein deutscher DDoS-Mitigations-Dienstleister, einen Anstieg von Angriffen auf spezielle E-Commerce-Anbieter um über 70 % gegenüber dem Monatsdurchschnitt.

Von den Top 40 der Angriffe mit den höchsten Angriffsdauern aller von Link11 im November 2018 gemeldeten Angriffe fanden 28 Angriffe am Black Friday statt. Die BSI-Analyse der Top 55 der längsten DDoS-Angriffe am Black Friday ist im Folgenden dargestellt:

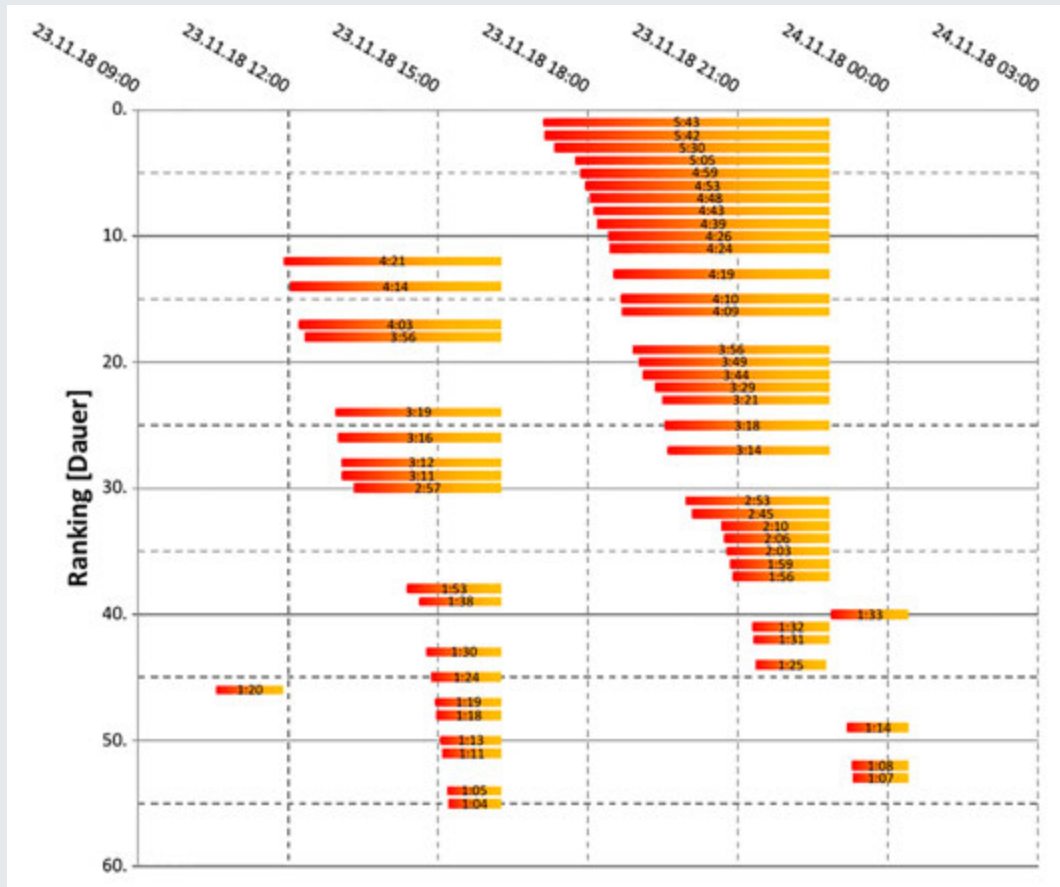


Abbildung 06 Top 55 der längsten DDoS-Angriffe am 23. November 2018 (Black Friday)

Zu sehen sind im Wesentlichen zwei Angriffswellen mit definierten Angriffsenden. Die zeitgleiche Beendigung der Angriffe um ca. 16.15 Uhr MESZ bzw. um ca. 23.00 Uhr MESZ hat ihre Ursache darin, dass zu diesen Zeitpunkten Mitigationsmaßnahmen ergriffen wurden, mit denen die Angriffe beendet werden konnten. Die Analyse der Metadaten der Angriffe zeigt auffällige Ähnlichkeiten, die Hinweis darauf geben, dass die Angriffe aus derselben Quelle (z. B. DDoS-Booster-Dienste) stammen.

Die Attribution zu einer konkreten Person/Organisation ist nicht möglich. Die Durchführung der Angriffe in zwei Angriffswellen und der zeitlich strukturiert durchgeführte Ablauf der Angriffsfolgen sind Indizien dafür, dass die Anzahl der beteiligten Angreifer begrenzt ist und die Angreifer im Informationsaustausch standen. Die Angreifer verfolgten mit hoher Wahrscheinlichkeit wirtschaftliche Interessen durch

- die Erpressung einzelner Unternehmen (Beendigung des Angriffs gegen Bezahlung) oder
- die Erlangung von Wettbewerbsvorteilen (Ausgrenzen von Mitbewerbern).

Zur Maximierung des Schadens griffen die Täter gezielt in zwei Zeitfenstern an, als E-Commerce-Plattformen, On-line-Services, Web-Anwendungen und Apps besonders intensiv genutzt wurden.

Die Analyse der Angriffsmetadaten zeigen, dass den Angriffen eine Angriffsvorbereitung vorausging. In Hinblick auf die Angriffsbandbreiten und die Paketzahlen lagen die Werte dieser Angriffe im unteren Drittel der beobachteten DDoS-Attacken des Monats November 2018. Doch statt per „hit and hope“ mit hoher Angriffsbandbreite einzelne Ziele anzugreifen, haben die Angreifer die ihnen zur Verfügung stehende Bandbreite dazu genutzt, möglichst viele Ziele zeitgleich anzugreifen. Um dies zu erreichen wurden vermutlich Ziele ausgewählt, von denen die Angreifer ausgingen, dass sie trotz des verringerten technischen Potenzials der einzelnen Angriffe dennoch die gewünschte Wirkung erzielen konnten.

Die Angriffe erfolgten mit Bezug auf einen konkreten Anlass (Black Friday). Es kann davon ausgegangen werden, dass sich ähnliche Angriffe zu prägnanten Online-Ereignissen (z. B. große E-Sports-Turniere, Sonderveranstaltungen von großen Online-Unternehmen usw.) wiederholen können.

Cyber Monday

Auch am „Cyber Monday“ (26.11.2018) verzeichnet Link11 einen massiven Anstieg von Angriffen auf spezielle E-Commerce-Anbieter. Mit einem Anstieg um 109 % gegenüber dem Monatsdurchschnitt wurde der Zuwachs am „Black Friday“ sogar weit überboten.

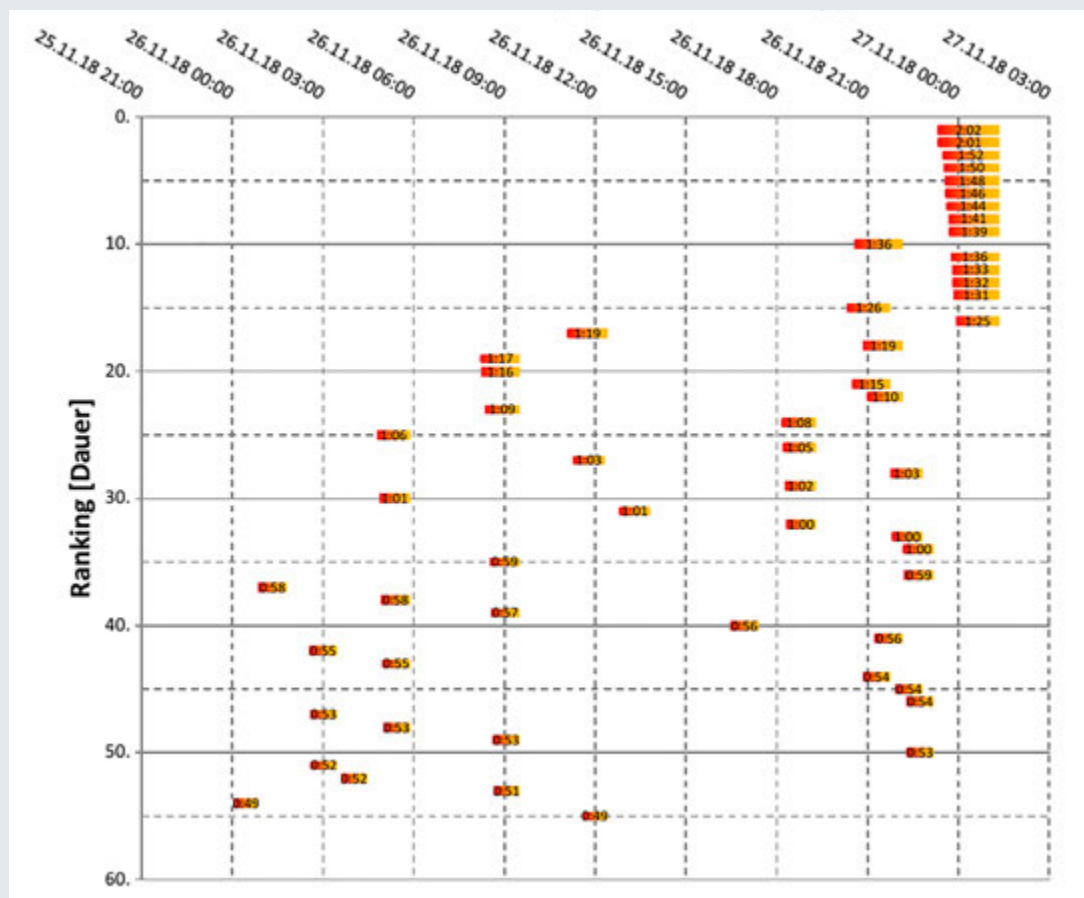


Abbildung 07 Top 55 der längsten DDoS-Angriffe am 26. November 2018 (Cyber Monday)

Im Gegensatz zu den Angriffen am Black Friday ist die zeitliche Verteilung der 55 längsten Angriffe am Cyber Monday jedoch nahezu homogen. Eine Gruppierung von Angriffen ist nur in einem Zeitfenster in der Stunde vor 24.00 Uhr MESZ feststellbar. Diese Angriffe endeten alle nach 00.00 Uhr des Folgetages. Die Angriffsdauern zwischen 49 Minuten und 122 Minuten erreichen die Werte vom Black Friday nicht. Doch liegen Sie wesentlich über dem Mittelwert des Monats November 2018 von ca. 25 Minuten pro Angriff.

Die Analyse der Metadaten der Angriffe zeigt auch hier Auffälligkeiten, wie sie bereits bei den Angriffen am Black Friday beobachtet werden konnten, die darauf hindeuten, dass die Angriffe aus derselben Quelle (z. B. DDoS-Booter-Dienste) stammen.

Wie bereits am Black Friday ist auch hier die Attribution zu einer konkreten Person/Organisation nicht möglich. Durch die nahezu homogene Verteilung der Angriffe fehlen Hinweise, die Rückschlüsse auf die Anzahl der Angreifer oder über Verbindungen der Angreifer untereinander zulassen.

Die vergleichsweise geringen Infektionszahlen von IoT-Geräten in Deutschland sind maßgeblich auf den Aufbau der typischen Internetanbindung deutscher Endkunden zurückzuführen. So sind diese klassischerweise über einen Router an das Internet angebunden, der im Regelfall keinen direkten Zugriff von außen auf Systeme im Netz des Endkunden zulässt, falls dies nicht explizit konfiguriert wurde. Dies ist anders als im nicht-europäischen Ausland, wo Geräte des internen Netzes oft direkt im Internet exponiert sind. Die besondere Sicherheitsrelevanz des Routers für das Heimnetzwerk spiegelt sich in der Technischen Richtlinie für Breitband-Router wider, die im November 2018 vom

BSI veröffentlicht wurde und Sicherheitsanforderungen an Router formuliert. Ähnliche Anforderungsdokumente sind für IoT-Geräte geplant (siehe 2.3.1.2 Smart Home und das Internet der Dinge).

Auch im Fall von Android-Geräten ist die fehlende Verfügbarkeit von Sicherheitsaktualisierungen und Fehlerbehebungen insbesondere im Niedrigpreissegment ein Problem, wie der Fall von Andr/Xgen2-CY eindrucksvoll gezeigt hat. Werden Geräte bereits ab Werk mit Infektionen ausgeliefert und erhalten keine infektionsbehebende Aktualisierung, sollten diese auf keinen Fall eingesetzt werden. Im Berichts-



Vorinstallierte Schadsoftware auf IT-Geräten

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat im Juni auf mehreren Smartphones vorinstallierte Schadsoftware nachgewiesen. Die Geräte wurden auf unterschiedlichen Online-Marktplätzen gekauft und auf eine bereits im Februar nachgewiesene Schadsoftware-Variante überprüft. Auf Grundlage von § 7 des BSI-Gesetzes warnte das BSI daher vor dem Einsatz der Geräte Doogee BL 7000 und M Horse Pure 1 und riet Anwenderinnen und Anwendern zu besonderer Vorsicht (<https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2019/bsi-warnung-smartphones-060619.html>). Auch auf dem Gerät Keecoo P11 wurde die Schadsoftware in der Firmware-Version V3.02 nachgewiesen. Für dieses Gerät stand aber eine Firmware V3.04 ohne diese Schadsoftware über die Updatefunktion „Wireless Update“ des Herstellers zur Verfügung. Daneben hat das BSI auf dem Gerät VKworld Mix Plus in den Firmware-Versionen V3.05 und V3.07 die gleiche Schadsoftware nachweisen können, diese wurde allerdings nicht aktiv. Einzelne Handelsplattformen nahmen die von der BSI-Warnung betroffenen Geräte aus dem Sortiment.

Bereits Ende Februar 2019 hatte das BSI vor Android-Geräten mit vorinstallierter Schadsoftware gewarnt, die über Online-Plattformen in Deutschland vertrieben wurden (https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2019/Warnung_vorinst_Schadsoftware_260219.html). Zunächst hatte das BSI die Infektion an einem konkreten Tablet nachgewiesen, stieß aber im Zuge der Untersuchungen auf weitere Geräte unterschiedlicher Hersteller, die ebenfalls betroffen waren. Auch wenn für einzelne Modelle zwischenzeitlich korrigierte Softwarestände ausgeliefert wurden, enthielten die auf den jeweiligen Hersteller-Webseiten bereitgestellten alten Firmware-Versionen weiterhin die entdeckte Schadsoftware. Somit war davon auszugehen, dass frühere Gerätelieferungen mit der veralteten infizierten Firmware erfolgt sind.

Auslöser für die Untersuchungen war das Auftreten hoher Infektionszahlen in Deutschland einer neu ins Sinkholing aufgenommenen Schadsoftwarefamilie, die erstmals vom Sicherheitsunternehmen Sophos auf einem Ulefone S8 Pro Smartphone entdeckt wurde. Das BSI verzeichnete täglich bis zu 20.000 Infektionen unterschiedlicher deutscher IP-Adressen und ging daher von einer größeren Verbreitung dieser Schadsoftwarevariante in Deutschland aus. Die von Sophos als „Andr/Xgen2-CY“ bezeichnete Schadsoftware (<https://news.sophos.com/en-us/2018/10/02/the-price-of-a-cheap-mobile-phone-may-include-your-privacy/>) befand sich in der Firmware des Gerätes und übertrug regelmäßig charakteristische Gerätedaten an einen Steuerungsserver. Zusätzlich verfügte sie über eine Nachladefunktion, um dynamisch weitere Funktionserweiterungen von einem Command-and-Control-Server zu empfangen. Über diesen Mechanismus ist beispielsweise die Platzierung und Ausführung eines Banking-Trojaners auf dem Gerät möglich. Aufgrund der Verankerung des Schadprogramms in der Gerätefirmware ist eine manuelle Bereinigung nicht umsetzbar.

Das BSI hat insgesamt für mehrere Geräte (fünf Smartphones und ein Tablet), die in Deutschland erworben werden konnten, eine Infektion mit „Andr/Xgen2-CY“ nachgewiesen und die betroffenen Hersteller informiert. Ein Teil von diesen hat daraufhin korrigierte Firmwareversionen zum Download bereitgestellt. Seit dem ersten Auftreten von Infektionen in den Sinkhole-Daten wurden die deutschen Netzbetreiber mittels Reports von CERT-Bund (<https://reports.cert-bund.de/schadprogramme>) bereits zu infizierten Geräten in ihren jeweiligen Netzen informiert. Die Provider wurden gebeten, ihre betroffenen Kunden entsprechend zu benachrichtigen. Was Käuferinnen und Käufer betroffener Geräte tun sollten und worauf alle IT-Nutzerinnen und IT-Nutzer beim Kauf von IT-Geräten achten sollten, hat das BSI unter <https://bsi-fuer-buerger.de> zusammengefasst.

zeitraum entfiel jedoch der Großteil der Android-Infektionen auf bösartige Apps, die im Wesentlichen aus Drittquellen stammten und von den Nutzern aktiv installiert wurden.

Aufgrund dieser Beobachtungen ist davon auszugehen, dass die Trends anhalten und die Vielzahl und Größe von Botnetzen weiterhin zunehmen. Maßnahmen zur Präven-

tion und Detektion sind zwingend erforderlich. Auch wenn der Schwerpunkt von IoT-Infektionen im Ausland zu finden ist, stellen infizierte Geräte eine Bedrohung für deutsche Systeme dar, weil diese beispielsweise zur Durchführung von internationalen DDoS-Angriffen oder zur Verbreitung von Schadprogrammen oder Spam missbraucht werden können.

i AVALANCHE: VERLÄNGERUNG DER SCHUTZMASSNAHMEN

Am 30. November 2016 hat die Staatsanwaltschaft Verden in Zusammenarbeit mit der Zentralen Kriminalinspektion (ZKI) Lüneburg und internationalen Partnern die weltweit größte Botnetzinfrastruktur Avalanche ausgehoben. Das BSI ist dabei unterstützend tätig gewesen. Im Rahmen der Zerschlagung wurden sogenannte Sinkhole-Server aufgesetzt, mit deren Hilfe IP-Adressen von infizierten Systemen identifiziert werden. Mit ihnen können die Internetprovider die betroffenen Anwender informieren und warnen. Die ursprünglich auf ein Jahr ausgelegten Schutz- und Informationsmaßnahmen wurden im November 2017 um ein weiteres Jahr verlängert, weil Analysen gezeigt hatten, dass trotz positiver Entwicklung der Infektionszahlen viele betroffene Anwender ihre Systeme nicht bereinigt haben. Zusätzlich wurde das im Zuge der Avalanche-Abschaltung aufgesetzte Sinkholing-System um Domänen des Andromeda-Botnetzes erweitert und für den Monat Oktober eine erhöhte Sichtbarkeit

der Infektionen mit dem Trojaner Goznmym erreicht.

Im November 2018 wurde eine erneute Verlängerung dieser Maßnahmen beschlossen und umgesetzt. Hierzu wurden ca. 850.000 Domänen geprüft und blockiert, um eine Übernahme der Botnetze durch Kriminelle zu unterbinden. Dadurch wurde eine Sichtbarkeit der Aktivität der Botnetze für weitere zwölf Monate sichergestellt. Als Resultat werden wieder täglich allein bei Avalanche weltweit mehr als 1,9 Millionen Rechner (unique IPs) erkannt, davon 3.900 in Deutschland. Durch die Weitergabe dieser Daten durch das BSI an Provider und andere, auch internationale Partner, wird eine rasche Bereinigung der betroffenen Systeme möglich. Eine kooperative Mitwirkung von Providern und Domaininhabern ist jedoch für einen Erfolg erforderlich. Den Erfolg zeigen die folgenden Zahlen: Am 28. November 2018 wurden weltweit ca. 1,3 Millionen Infektionen erkannt und gemeldet, davon ca. 3.300 in Deutschland.

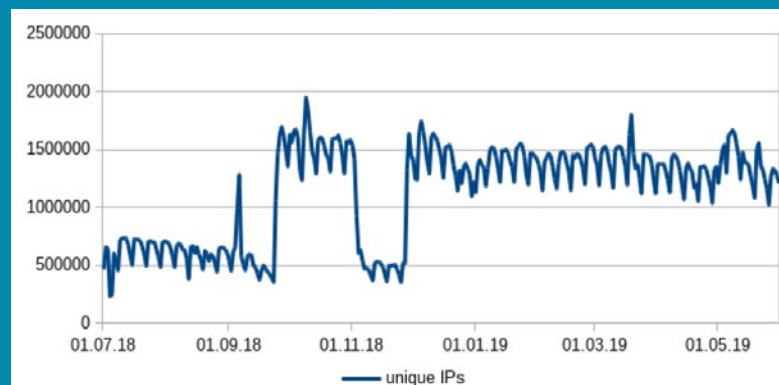


Abbildung 08 Infizierte Systeme weltweit

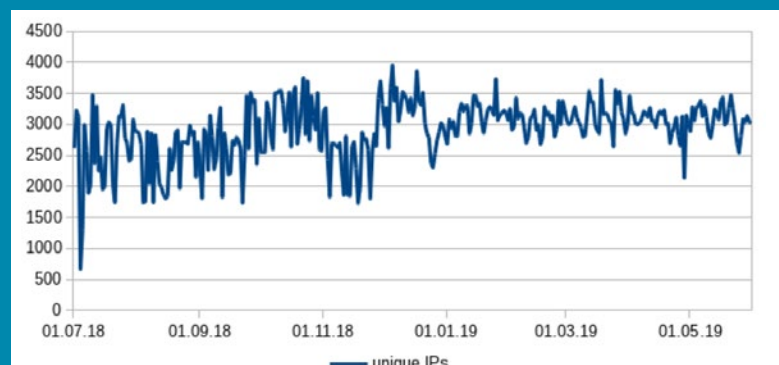


Abbildung 09 Infizierte Systeme Deutschland

1.2.6 Spam

Unerwünscht zugesandte E-Mails werden generell als Spam bezeichnet. Dieser lässt sich grob in drei Formen unterteilen:

- Klassischer Spam wird häufig für Produkt-, Wertpapier- oder Dienstleistungswerbung benutzt und zudem für Betrugsversuche wie Vorschussbetrug eingesetzt. Beim Vorschussbetrug soll das Opfer z. B. dazu animiert werden, Geld für eine Dienstleistung oder Ware vorab zu überweisen, die später nicht geliefert wird.
- Mit Schadprogramm-Spam (Malware-Spam) wollen Angreifer Systeme der Empfänger mit Schadprogrammen infizieren. Dies kann direkt durch ein Schadprogramm im E-Mail-Anhang oder indirekt durch einen Link im E-Mail-Text oder im Anhang erfolgen, der auf ein Schadprogramm oder eine Webseite mit Drive-by-Exploits verweist (siehe Kapitel 1.2.2 Schadprogramme).

- Mit Phishing-Nachrichten werden Benutzer dazu bewogen, ihre Zugangsdaten (z. B. zu Internet-Banking, Bezahldiensten, sozialen Netzwerken, Einkaufsportalen etc.) auf Webseiten unter der Kontrolle der Angreifer einzugeben (siehe 1.2.1 Identitätsdiebstahl).

Der Spam-Versand erfolgt in den meisten Fällen entweder über kompromittierte Server, infizierte Client-Systeme oder mithilfe ausgespähter Zugangsdaten über legitime E-Mail-Konten. Häufig sind die Spam versendenden Systeme zu einem Botnetz (siehe Kapitel 1.2.5 Botnetze) zusammengeschlossen, was die Vermarktung von Spam als Dienstleistung durch Cyber-Kriminelle erleichtert.

Ein weiterer Aspekt, der derzeit in den Spam-E-Mails beobachtet werden kann, ist die missbräuchliche Verwendung persönlicher Daten aus Daten-Leaks oder anderweitig unrechtmäßig erworbener Identitätsdaten (bspw. von infizierten E-Mail-Clients oder recherchierte Daten). Dadurch wird die Wahrscheinlichkeit einer Infektion in erheblichem Maße gesteigert.

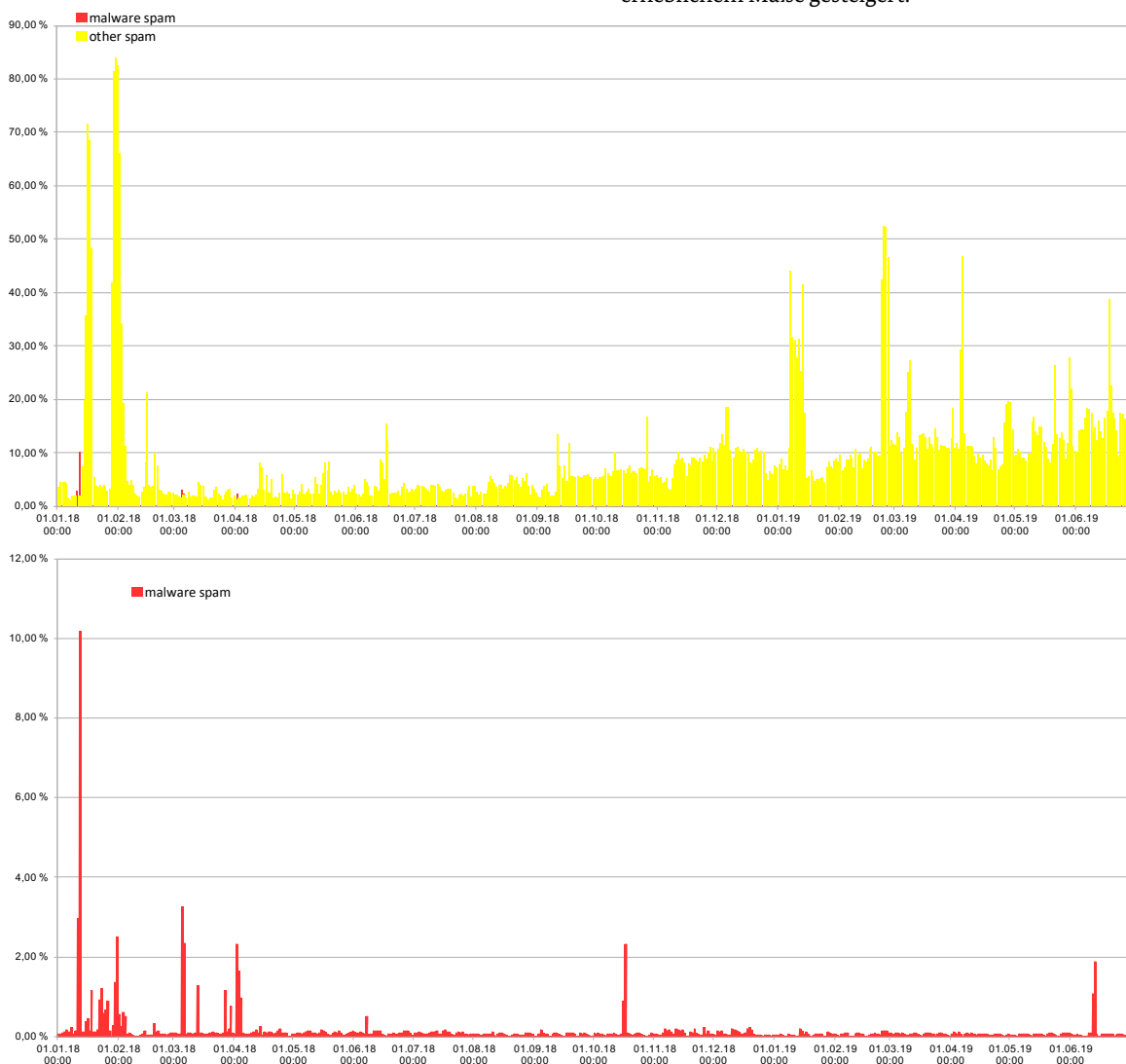


Abbildung 10 Malware-Spam- und Spamverlauf seit 01.01.20018 in Prozent des bisherig Tagesmaximums des Gesamtspamvolumens von Mitte Dezember 2016 (höchstes bislang gemessener Tagesspamvolumen) als gestapelte Flächen. Untere Grafik zeigt nochmal vergrößert den Malware-Spam-Verlauf.

Der Versand von Spam ist im Vergleich zum letzten Berichtszeitraum um ca. 40 % zurückgegangen. Noch stärker war mit ca. 97 % der Rückgang von Malware-Spam.

Obwohl das Volumen von Malware-Spam so stark abgenommen hat, ist – nach Beobachtungen des BSI – das Schadenspotenzial durch eine deutlich gezieltere Versandweise gleich geblieben, in einigen Fällen sogar gestiegen. Hervorzuheben ist in diesem Zusammenhang das Emotet-Botnetz (siehe Vorfall: Warnung vor Schadsoftware Emotet auf Seite 13). Durch die Benutzung von Kontaktbeziehungen aus aktuellen E-Mails auf infizierten Clients wurde der Versand von bekannten Kommunikationspartnern vorgetäuscht. Dieser Modus Operandi gepaart mit der Nutzung von erbeuteten E-Mail-Accounts zum Versand der E-Mails trug deutlich zu einer größeren Schadwirkung bei.

Ferner wurden die versendeten Anhänge (vor allem MS-Office-Dokumente und JS-Dateien) stetig angepasst, um die Erkennung durch Antiviren-Software zu unterlaufen. Anfang April 2019 wurden z. B. Dokumente als verschlüsselte ZIP-Dateien versendet und das Passwort in der E-Mail genannt. Der fingierte Inhalt der E-Mail war häufig in gutem Deutsch verfasst und sollte dem Adressaten eine dringende Angelegenheit suggerieren (Rechnung, Auftragsbestätigung etc.).

Über Emotet hinaus wurden auch weitere kleine Wellen beobachtet. Gehäuft war der Versand von ungewöhnlichen Dateiformaten wie z. B. ACE, ISO und UDF zu beobachten, die dann die entsprechenden Schadcodes zumeist in Form einer ausführbaren Datei (EXE) enthielten. Diese E-Mail-Texte waren allerdings meist auf Englisch formuliert. Hervorzuheben ist auch der Versand von RTF- und teilweise auch MS-Word-Dokumenten, die die MS-Equation-Schwachstelle (CVE-2017-11882) ausgenutzt haben. Ein weiterer Trend ist der Versand von MS-Office-Dokumenten, die keinen Schadcode enthalten, diesen jedoch über MS-Office-Mechanismen nach dem Öffnen des Anhangs aus dem Internet nachladen. Vereinzelt werden auch sehr alte Softwarekomponenten für Angriffe ausgenutzt, die aus Kompatibilitätsgründen weiterhin in moderner Software eingebettet sind wie z. B. Excel-4.0-Makros.

Im Gegensatz zum letzten Berichtszeitraum lässt sich beim klassischen Spam keine besonders ausgeprägte Kategorie feststellen, sondern eine breitere Verteilung auf mehrere Angriffsvektoren.

Wie die Beobachtungen gezeigt haben, steigen die Qualität und somit die Effektivität von Malware-Spam weiterhin. Daher ist das Bedrohungspotenzial trotz der stark reduzierten Menge konstant geblieben oder in einigen

Bereichen sogar gestiegen. Die Angreifer zeigen ein hohes Maß an Innovation und technischem Sachverstand. Hier scheint auch ein erheblicher personeller Aufwand erbracht zu werden, um mit stets neuen Techniken den Antiviren-Schutz zu überwinden und mit neuen Social-Engineering-Ansätzen den Benutzer zum Starten des Schadcodes zu bewegen. Die Ausnutzung von Features oder Schwachstellen von veralteten Softwarekomponenten oder Dateiformaten läuft oft zuerst unbemerkt, da diese weitgehend unbekannt sind.

Teilweise wurden Emotet-Vorfälle – auch durch IT-Fachpersonal – als „gezielte Angriffe“ wahrgenommen und dem BSI als solche gemeldet. Dies zeigt die Effektivität der verwendeten Vorgehensweisen.

Dass nicht alle technisch ausgeklügelten Ansätze der Angreifer in der Praxis erfolgreich sind, zeigt sich an den passwortgeschützten ZIP-Dateien. Diese haben zwar die Perimeter-Antiviren-Lösungen leicht überwunden, scheitern aber an den Nutzern gescheitert zu sein, die nicht gewillt oder nicht in der Lage waren, Passwörter beim Öffnen des Anhangs einzugeben.

Eine restriktive Behandlung von Anhängen (Dateityp-Whitelist-Ansatz) verbunden mit einer restriktiven Content-Policy für Dokumente (indem z. B. Dokumente mit Makros oder Nachladefunktionalität oder Office-Nachladeanfragen am zentralen HTTP-Gateway gefiltert werden) könnte die meisten neuen Ansätze der Angreifer ins Leere laufen lassen.

1.2.7 Trends in APT-Angriffen

APT-Angriffe (Advanced Persistent Threats, deutsch: „fortgeschrittene, andauernde Bedrohungen“) unterscheiden sich in ihren technischen Möglichkeiten, Zielen und den Organisationen, von denen sie ausgeführt werden. Somit stellt sich die Lage in diesem Bereich sehr heterogen dar. Als Trend werden im Folgenden daher Phänomene beschrieben, die nicht auf einzelne Gruppen oder vermutete Ursprungsländer beschränkt sind.

Öffentlich verfügbare Werkzeuge: Ein klarer Trend, der sich bei APT-Gruppen mit sehr unterschiedlichen technischen Möglichkeiten und Hintergründen durchsetzt, ist die Verwendung öffentlich verfügbarer Penetrationstest-Werkzeuge, die dieselbe Funktionalität wie Spionageprogramme bieten. Beispiele sind die Frameworks „Cobalt Strike“, „Meterpreter“, „Kodiak“ oder „Powershell Empire“. Diese wurden zum Einsatz von Penetrationstest professionell entwickelt, bieten einen großen Funktionsumfang und sind in der Regel komfortabel verwendbar.

Für Täter hat deren Verwendung mehrere Vorteile. Zum einen wird Entwicklungsaufwand gespart. Zum anderen erschwert deren Verwendung für die Sicherheitsteams die Zuordnung eines konkreten Angriffs zu Kampagnen oder APT-Gruppen.

Für Sicherheitsteams bieten sich aber auch Chancen. Logdaten und Netzwerkverkehr können auf typische Eigenschaften der bekannten und gut analysierten Angriffswerkzeuge geprüft werden, wodurch die Detektion einer größeren Zahl an Tätergruppen ermöglicht werden könnte. Zwar bieten die Frameworks viele Möglichkeiten der Konfiguration, um die Detektion zu erschweren, insbesondere unerfahrene Tätergruppen nutzen aber oft Voreinstellungen. Ein Beispiel ist, dass die Kontrollserver von Cobalt Beacon bis Januar 2019 im Vergleich zu anderen Webservern auf bestimmte Anfragen mit einem zusätzlichen Leerzeichen antworteten. Über diesen Mechanismus war es möglich, weltweit nach allen erreichbaren Cobalt Strike Servern zu scannen, um diese anschließend als Netzwerk-Signatur zu verwenden.

Generell ist durch die Verfügbarkeit dieser öffentlichen Werkzeuge eine leichte Nivellierung der technischen Komplexität von APT-Angriffen zu beobachten, allerdings nur im unteren und mittleren Bereich. Für unerfahrene Gruppen sinkt die Anfangshürde und sie können (zumindest im Bereich Schadprogramme) auf einem höheren Niveau beginnen. Erfahrene und technisch fortgeschrittene Gruppen entwickeln jedoch parallel zur Nutzung dieser öffentlichen Frameworks ihr eigenes Schadprogramm-Arsenal weiter. Beispiele sind APT28, Snake und APT10. Die Gründe hierfür sind noch unklar. Plausibel ist, dass eigenentwickelte Schadprogramme von IT-Sicherheitsfirmen noch nicht so gut analysiert sind wie die öffentlich verfügbaren, bekannten Frameworks und Täter sich dadurch niedrigere Detektionsraten versprechen. Zudem werden mitunter neue Funktionen benötigt, die in den öffentlichen Frameworks nicht enthalten sind.

Internationale Dienstleister: Berichte von IT-Sicherheitsfirmen legen nahe, dass es eine wachsende Zahl von Dienstleistern gibt, die Spähsoftware und Exploits anbieten, oder sogar selbst Cyber-Angriffe operativ durchführen. Diese Dienstleistungen werden teilweise nicht nur im eigenen Heimatland, sondern international angeboten. Dadurch sind nun auch Staaten, die bisher wenig Know-how in der Entwicklung von Spionageprogrammen hatten, in der Lage, hochprofessionelle Werkzeuge zu besitzen oder für Angriffe zu nutzen. Diese Entwicklung führt nicht nur zu einer erweiterten Bedrohungslage, sondern erschwert auch das Zusammenfassen von Angriffen derselben Täter (Attribution), da

verschiedene Auftraggeber dieselben Dienstleister (und damit beobachtbare Techniken) verwenden. Andererseits bieten sich für Netzwerkverteidiger Chancen. Fehler von unerfahrenen Tätern können dazu führen, dass Spionageprogramme detektiert und dadurch die Operationen von weiteren Akteuren aufgedeckt werden können.

Nutzung legitimer Dienste: Eine weitere Entwicklung, die bei so unterschiedlichen Gruppen wie APT28, Mud-dyWater oder DarkHydrus beobachtet werden kann, ist die Verwendung legitimer Dienste als Verschleierung für die Steuerung von Schadprogrammen. Diese als Dead-Drop-Resolver („Toter-Briefkasten“) bezeichnete Methode bedeutet, dass Schadprogramme nach einer erfolgreichen Infektion zunächst eine Adresse bei legitimen Diensten wie Dropbox, Github, Google Groups oder anderen Foren kontaktieren. Diese Dienste werden über TLS verschlüsselt, sodass Netzwerk-Monitoring-Systeme die Schadsoftware-Kommunikation nicht von legitimer Nutzung unterscheiden können. Dort sind die eigentlichen Adressen der Kontrollserver hinterlegt, zu denen sich das Schadprogramm dann verbindet. Über diesen Weg können die Täter die Adressen von Kontrollservern sehr flexibel ändern und die Detektionswahrscheinlichkeit verringern.

Technisch können Sicherheitsteams diesem Phänomen begegnen, indem sie verschlüsselten TLS-Verkehr in Unternehmens- oder Behördennetzen aufbrechen und ihn bestehenden Sicherheitsprodukten zuführen. Diese Maßnahme berührt jedoch Datenschutzaspekte und bedeutet bei der Einführung einen großen organisatorischen Aufwand. Die Nutzung von solchen TLS-Proxies bietet jedoch auch Detektionsmöglichkeiten für weitere Phänomene wie Exploits oder Schadsoftware auf Webseiten, die mit leicht zu erlangenden TLS-Zertifikaten von kostenlosen Stellen wie Let's Encrypt verschlüsselt werden.

Erschweren von Schadsoftware-Analysen: Technisch fortgeschrittene Gruppen betreiben zunehmend Aufwand, um die systematische Analyse ihrer Schadsoftware durch Sicherheitsfirmen zu erschweren. Eine gängige Praxis der Firmen ist das Sammeln von Schadprogrammen auf Kundensystemen oder aus webbasierten Diensten, mit denen Nutzer Dateien auf Schadcode prüfen lassen können. Anschließend werden die sogenannten Samples analysiert und Detektionssignaturen entwickelt. Mehrere APT-Gruppen unterlaufen diese Sammelpraxis nun, indem sie dafür sorgen, dass ihre Haupt-Schadprogramme erst zugreifbar werden, wenn eine Kette von sogenannten Droppern und Downloadern durchlaufen wurde. Teilweise werden auf kompromittierten Systemen zunächst Informationen gesammelt, um zu prüfen, ob es sich um ein lohnenswertes Ziel handelt oder um ein

Analyse-System einer Sicherheitsfirma, das absichtlich als zu infizierend aufgebaut wurde. Erlangt eine Sicherheitsfirma nur einen Downloader der ersten Stufe, kann sie das Haupt-Schadprogramm nicht unbedingt daraus erhalten, weil es ggf. nicht mehr von dem Angriffsserver herunterladbar ist oder spezifische Konfigurationen benötigt, die nur die Täter kennen. Diese Vorgehensweise ist grundsätzlich seit Jahren gängige Praxis, wird aber derzeit stärker beobachtet.

Übernahme von APT-Techniken in kriminellen Kampagnen: Wie schon im letzten Jahr berichtet machen sich verschiedene kriminelle Gruppen Techniken zu eigen, die vor einiger Zeit noch als charakteristisch für APT-Angriffe galten. Hierzu gehört das Lateral Movement, bei dem sich Täter manuell in einem kompromittierten internen Netzwerk ausbreiten. Im Berichtszeitraum wurden mehrere Fälle beobachtet, in denen nach einer anfänglichen Kompromittierung durch Massenschadsoftware wie Emotet andere Angriffsarten folgten. Vermutlich mit den via Emotet erbeuteten Zugängen brachten Täter in mehreren Fällen Ransomware aus, die sie offenbar manuell und gezielt auf Servern in internen Unternehmensnetzwerken platzierten (siehe Vorfall: Warnung vor Schadsoftware Emotet auf Seite 13).

Technische Zuordnung zu APT-Gruppen: Ein wichtiger Aspekt bei der technischen Prävention und Detektion von APT-Angriffen ist das Zusammenfassen ähnlicher Vorfälle zu abstrakten APT-Gruppen, die als Intrusion Sets bezeichnet werden. Diese Kategorisierung erlaubt es, Ressourcen von Sicherheitsabteilungen zu priorisieren und bei Vorfällen aufgrund von Erfahrungen effizienter nach möglichen Vorgehensweisen der Täter zu suchen. Die oben erwähnten Phänomene, wie öffentlich angebotene Werkzeuge und Dienstleister, führen jedoch zu Unschärfen in früheren Phasen bei der Zuordnung von Angriffen zu Intrusion Sets. Trotzdem empfiehlt das BSI weiterhin, für die Risiko-Einschätzung der eigenen Organisation auch die Aktivität von APT-Gruppen zu berücksichtigen.

Angriffsanalyse und Priorisierung von Maßnahmen:

Eine Methodik zur strukturierten Auswertung von Vorfallsinformationen über APT-Angriffe ist das MITRE ATT&CK-Framework (<https://attack.mitre.org/>). Eine BSI-interne Auswertung von Vorfallsberichten anhand dieser Methodik zeigt, dass die folgenden Angriffstechniken bei APT-Angriffen besonders häufig zum Einsatz kommen:

- Spearphishing: E-Mails mit Schadprogrammen im Anhang (Phase: Initial Access)
- Genereller Einsatz von Skripten, spezifisch von PowerShell-Skripten sowie Ausführung durch den Nutzer (Phase: Execution)

- Verankerung über Autostart-Mechanismen in der Registry oder als neuer Dienst (Phase: Persistence)
- Sammeln von Systeminformationen oder laufenden Prozessen (Phase: Discovery)
- Standard-Protokolle wie HTTP(S) (Phase: Command & Control)

Auch wenn diese Erkenntnisse nicht neu sind oder überraschen, so helfen sie, die Abwehr von APT-Angriffen zu priorisieren: Die Fokussierung von Präventions- und Detektionsmaßnahmen auf die oben genannten Angriffstechniken führt zu einem signifikant höheren Absicherungsniveau gegen APT-Angriffe.

Die aufgezeigten Trends ändern nichts an der Tatsache, dass viele APT-Angriffe durch gängige IT-Sicherheitsmaßnahmen (vgl. https://www.bsi-fuer-buerger.de/Basischutz_PC) verhindert werden können, wenn diese konsequent umgesetzt werden. Umgekehrt machen fehlende Sicherheitsmaßnahmen den Tätern die Arbeit leichter und führen dazu, dass sie weniger Ressourcen einsetzen müssen. Im Zweifelsfall ist es ratsam, sich zunächst auf grundlegende und erprobte IT-Sicherheitsmaßnahmen zu konzentrieren. Im Anschluss umzusetzende APT-spezifische Maßnahmen sind besonders wirksam, wenn zuerst eine organisationsspezifische Risikobewertung vorgenommen wurde: Sicherheitsverantwortliche sollten das für ihre Organisation relevante Threat-Model kennen und daraus ableiten, welche Angriffstechniken (ggf. durch Analyse der jeweils relevanten APT-Gruppen) noch nicht durch die eigenen Sicherheitsmaßnahmen abgedeckt werden.

1.2.8 Angriffsvektoren im Kontext Kryptografie

Die Sicherheitsfunktionalität vieler IT-Produkte basiert auf kryptografischen Mechanismen. Dem Stand der Technik entsprechende Kryptoalgorithmen wie das symmetrische Verschlüsselungsverfahren Advanced Encryption Standard (AES) oder der asymmetrische Diffie-Hellman-Schlüsselaustausch über elliptischen Kurven 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. Die Sicherheit dieser Verfahren ist jedoch in der Regel an gewisse Voraussetzungen geknüpft. Alternativ müssen zusätzliche Absicherungsmaßnahmen getroffen werden.

Folgende Aspekte können dazu beitragen, dass ein Kryptosystem in der Praxis versagt:

- Schwächen in kryptografischen Mechanismen oder Protokollen
- Implementierungsfehler
- Unzureichend abgesicherte Seitenkanäle
- Hardware-Schwachstellen (z. B. Spectre, siehe Kapitel 1.2.9)
- Schwache Zufallszahlen

Ein verbreitetes Beispiel sind Geräte, die in einer sicheren Umgebung betrieben werden und über ein offenes Netzwerk mit anderen IT-Produkten kommunizieren. Für die gegenseitige Authentisierung sowie die vertrauliche und integritätsgeschützte Kommunikation stehen kryptografische Protokolle wie TLS, IKEv2/IPsec oder SSH zur Verfügung, für die gemeinhin angenommen wird, dass ein Angreifer mit Netzwerkzugriff weder die geheimen Schlüssel in Erfahrung bringen noch Nachrichten entschlüsseln oder unbemerkt verändern kann. Für die Wirksamkeit der kryptografischen Protokolle muss sichergestellt sein, dass diese korrekt implementiert werden. Insbesondere dürfen wichtige kryptografische Prüfungen nicht ausgelassen werden, selbst wenn diese aus funktionaler Sicht nicht benötigt werden (siehe z. B. Info-Kasten „Invalid-Curve-Angriffe“ auf Seite 31). Darüber hinaus muss verhindert werden, dass durch das an der Netzwerkschnittstelle beobachtbare Verhalten der Geräte (zB. Fehlermeldungen, Antwortzeit) Informationen über verarbeitete Geheimnisse abfließen (siehe z. B. Info-Kasten „CBC-Padding-Orakel-Angriffe“).

Bei der Absicherung von Kryptosystemen, die selbst Angreifen in räumlicher Nähe standhalten sollen, müssen neben der Laufzeit noch weitere für Seitenkanalangriffe nutzbare Informationen wie Stromverbrauch oder elektromagnetische Abstrahlung der Geräte berücksichtigt werden. Intensive Forschung auf diesem Gebiet hat neben Gegenmaßnahmen auch neue Angriffsvektoren hervorgebracht.

Die aktuellste Entwicklung in der Seitenkanalanalyse ist der Einsatz von Methoden der Künstlichen Intelligenz (KI), um Muster in Messdaten zu erkennen. Darüber hinaus gibt es erste Ansätze, mit Hilfe der KI Werkzeuge zur Kryptoanalyse zu entwickeln. Das BSI baut praktische Expertise in diesen Gebieten auf (siehe Kapitel 2.4.5).

Eine wesentliche Voraussetzung für den sicheren Einsatz von Kryptografie ist die Erzeugung von Zufallszahlen, die gewisse Gütekriterien erfüllen. Das BSI definiert hierfür in den AIS 20 und AIS 31 (Anwendungshinweise und Interpretationen zum Schema) Funktionalitätsklassen von Zufallszahlengeneratoren für verschiedene Einsatzzwecke. Dabei ist positiv hervorzuheben, dass mittlerweile

viele Produkte über einen nach dem deutschen Common-Criteria-Schema (CC-Schema) zertifizierten physikalischen Zufallszahlengenerator verfügen. Aufgrund der Strukturverkleinerung von Halbleiterprodukten bzw. der immer größeren Leistungsfähigkeit bei geringem Stromverbrauch verfügen neuere Produkte zudem über eine integrierte kryptografische Nachbearbeitung der Zufallszahlen, die die theoretische Ausnutzbarkeit der bereits sehr kleinen verbleibenden statistischen Schwächen physikalischer Rauschquellen vollends verhindert.

Für die Blockverschlüsselung (z. B. mit AES) im CBC-Modus müssen Nachrichten durch sogenannte Padding-Verfahren auf ein Vielfaches der Blocklänge aufgefüllt werden. Wegen der ungünstigen Verwendung des CBC-Modus innerhalb des TLS-Protokolls (Transport Layer Security) können sogenannte CBC-Padding-Orakel entstehen, falls eine Implementierung durch Antwortzeit oder anderes Verhalten Informationen über das Ergebnis einer Padding-Prüfung preisgibt. Ein CBC-Padding-Orakel kann es einem Angreifer ermöglichen, TLS-Nachrichten zu entschlüsseln. Das Grundprinzip dieser Angriffe geht auf eine Publikation von Serge Vaudenay aus dem Jahr 2002 zurück. Seitdem haben Sicherheitsforscher trotz mehrfach angepasster TLS-Standards immer wieder Schwachstellen in diesem Zusammenhang aufgedeckt. Zuletzt wurden im März 2019 die neuen Angriffsvarianten „Zombie POODLE“ und „GOLDENDOODLE“ von Sicherheitsforscher Craig Young auf der Black Hat Asia Konferenz vorgestellt.

Im neuen Standard TLS 1.3, der im August 2018 von der Internet Engineering Task Force (IETF) verabschiedet wurde, sind CBC-Padding-Orakel-Angriffe nicht mehr möglich, da der CBC-Modus dort entfernt wurde. Das BSI hat die Verwendung von TLS 1.3 als Empfehlung in die Technische Richtlinie TR-02102-2 aufgenommen.

Unter Invalid-Curve-Angriffen versteht man Attacken gegen Elliptische-Kurven-Kryptografie, bei denen ein Angreifer durch Manipulation von Kurvenpunkten implizit die Verwendung schwacher Kurvenparameter durchsetzt. Solche Angriffe wurden erstmals 2000 in einer Arbeit von Biehl, Meyer und Müller (Ingrid Biehl, Bernd Meyer, Volker Müller: Differential Fault Attacks on Elliptic Curve Cryptosystems) beschrieben und lassen sich grundsätzlich leicht durch Punktvalidierung verhindern. Im Berichtszeitraum gab es gleich zwei Vorfälle, bei denen diese wichtige Prüfung ausgelassen oder nur unzureichend durchgeführt wurde.

Im Juli 2018 haben Biham und Neumann (Eli Biham, Lior Neumann: Breaking the Bluetooth Pairing: Fixed Coordinate Invalid Curve Attack) einen neuartigen Invalid-Curve-Angriff gegen aktuelle Bluetooth Pairing-Protokolle vorgestellt,

i CBC-PADDING-ORAKEL-ANGRIFFE

Für die Blockverschlüsselung (z. B. mit AES) im CBC-Modus müssen Nachrichten durch sogenannte Padding-Verfahren auf ein Vielfaches der Blocklänge aufgefüllt werden. Wegen der ungünstigen Verwendung des CBC-Modus innerhalb des TLS-Protokolls (Transport Layer Security) können sogenannte CBC-Padding-Orakel entstehen, falls eine Implementierung durch Antwortzeit oder anderes Verhalten Informationen über das Ergebnis einer Padding-Prüfung preisgibt. Ein CBC-Padding-Orakel kann es einem Angreifer ermöglichen, TLS-Nachrichten zu entschlüsseln. Das Grundprinzip dieser Angriffe geht auf eine Publikation von Serge Vaudenay aus dem Jahr 2002 zurück. Seitdem haben Sicherheitsforscher trotz mehrfach

angepasster TLS-Standards immer wieder Schwachstellen in diesem Zusammenhang aufgedeckt. Zuletzt wurden im März 2019 die neuen Angriffsvarianten „Zombie POODLE“ und „GOLDENDOODLE“ von Sicherheitsforscher Craig Young auf der Black Hat Asia Konferenz vorgestellt.

Im neuen Standard TLS 1.3, der im August 2018 von der Internet Engineering Task Force (IETF) verabschiedet wurde, sind CBC-Padding-Orakel-Angriffe nicht mehr möglich, da der CBC-Modus dort entfernt wurde. Das BSI hat die Verwendung von TLS 1.3 als Empfehlung in die Technische Richtlinie TR-02102-2 aufgenommen.

i INVALID-CURVE-ANGRIFFE

Unter Invalid-Curve-Angriffen versteht man Attacken gegen Elliptische-Kurven-Kryptografie, bei denen ein Angreifer durch Manipulation von Kurvenpunkten implizit die Verwendung schwacher Kurvenparameter durchsetzt. Solche Angriffe wurden erstmals 2000 in einer Arbeit von Biehl, Meyer und Müller (Ingrid Biehl, Bernd Meyer, Volker Müller: Differential Fault Attacks on Elliptic Curve Cryptosystems) beschrieben und lassen sich grundsätzlich leicht durch Punktvalidierung verhindern. Im Berichtszeitraum gab es gleich zwei Vorfälle, bei denen diese wichtige Prüfung ausgelassen oder nur unzureichend durchgeführt wurde. Im Juli 2018 haben Biham und Neumann (Eli Biham, Lior Neumann: Breaking the Bluetooth Pairing: Fixed Coordinate Invalid

Curve Attack) einen neuartigen Invalid-Curve-Angriff gegen aktuelle Bluetooth Pairing-Protokolle vorgestellt, mit dem Bluetooth-Nachrichten entschlüsselt und gefälscht werden können. Die Bluetooth-Spezifikation wurde daraufhin korrigiert. Die Sicherheitsforscher Ronen und Vanhoef (Mathy Vanhoef, Eyal Ronen: Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd.) haben im April 2019 bei mehreren Implementierungen des passwortbasierten Authentisierungsprotokolls EAP-pwd fehlende Punktvalidierung festgestellt, wodurch einem Angreifer die Authentisierung ohne Passwort ermöglicht werden kann. EAP-pwd wird u. a. als Authentisierungsmethode für die WLAN-Verschlüsselung WPA2 eingesetzt.

i POST-QUANTEN-KRYPTOGRAPHIE

Die Sicherheitsgarantien der heute eingesetzten kryptografischen Mechanismen gelten allerdings nur, bis ein hinreichend leistungstarker Quantencomputer zur Verfügung steht. Schon seit den 1990er Jahren sind Quantenalgorithmen bekannt, die das Sicherheitsniveau klassischer Verfahren erheblich reduzieren (Grover-Algorithmus für symmetrische Kryptoverfahren) oder diese Verfahren vollständig brechen (Shor-Algorithmus für asymmetrische Kryptoverfahren).

Einen Ausweg bietet die sogenannte Post-Quanten-Kryptografie. Darunter versteht man kryptografische Verfahren, die auf mathematischen Problemen beruhen, die vermutlich auch mit einem Quantencomputer nicht effizient gelöst werden können. In Folge der zunehmenden Wahrscheinlichkeit, dass ein Quantencomputer hinreichender Größe realisiert werden kann, haben sich die Forschungs- und Standardisierungsaktivitäten im Bereich Post-Quanten-Kryptografie in den letzten Jahren massiv verstärkt (siehe Kapitel 3.4.2). Eine wichtige Aufgabe des BSI wird es in den

nächsten Jahren sein, diese Aktivitäten aktiv zu begleiten und eigene Projekte umzusetzen.

Um eine fundierte Einschätzung zum aktuellen Entwicklungsstand und der potenziellen zukünftigen Verfügbarkeit eines Quantencomputers zu erhalten, wurde vom BSI die Studie „Entwicklungsstand Quantencomputer“ bei Forschern der Universität des Saarlandes und der Florida Atlantic University in Auftrag gegeben. In dem Ergebnisbericht werden aktuelle technologische Ansätze und quantenalgorithmenische Innovationen beleuchtet und deren Implikationen im Kontext aktuell eingesetzter Public-Key-Verfahren erörtert. Bei einer ersten Revision der Studie hat sich angedeutet, dass Fortschritte (u. a. bei der Fehlerkorrektur) die Anzahl der benötigten Quantenbits (Qubits) für eine gegebene Aufgabe reduzieren könnten. Eine zweite Revision ist für Ende 2019 geplant. Die Studie und eine Zusammenfassung stehen auf der Webseite des BSI unter <https://www.bsi.bund.de/qcstudie> zur Verfügung.

mit dem Bluetooth-Nachrichten entschlüsselt und gefälscht werden können. Die Bluetooth-Spezifikation wurde daraufhin korrigiert.

Die Sicherheitsforscher Ronen und Vanhoef (Mathy Vanhoef, Eyal Ronen: Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd) haben im April 2019 bei mehreren Implementierungen des passwortbasierten Authentisierungsprotokolls EAP-pwd fehlende Punktvalidierung festgestellt, wodurch einem Angreifer die Authentisierung ohne Passwort ermöglicht werden kann. EAP-pwd wird u.a. als Authentisierungsmethode für die WLAN-Verschlüsselung WPA2 eingesetzt.

1.2.9 Angriffe durch Ausnutzung moderner Prozessorarchitektur

Die im Januar 2018 veröffentlichten Sicherheitslücken im Design performanter Central-Processing-Unit Mikroarchitekturen (CPU-Mikroarchitektur) wurden insbesondere im akademischen Umfeld ausführlich charakterisiert und weiterentwickelt. Diese Klasse von Angriffen wird als transiente Ausführungsangriffe beschrieben und umfasst neben den Spectre-Varianten Spectre V1, Spectre V2, Spectre V3a und Spectre V4 auch Meltdown, Foreshadow, LazyFP und SPOILER. Grundsätzlich anfällig für diese Art von Angriffen sind nahezu alle aktuellen Prozessoren, die auf hohe Performance abzielen. Der Fokus richtet sich aber auf die großen Hersteller Intel, AMD und ARM.

Transiente Ausführungsangriffe nutzen Details der CPU-Mikroarchitektur aus, um Informationen aus eigentlich geschützten Speicherbereichen auszulesen. Ein großer Teil der in den letzten 20 Jahren erzielten Leistungssteigerungen von Prozessoren geht darauf zurück, dass auch innerhalb eines Rechenkerns Befehle auf mikroarchitektureller Ebene nicht streng seriell abgearbeitet werden (Out-of-Order-Ausführung). So versucht beispielsweise moderne Hardware, das Ergebnis (Sprungziel) einer bedingten Verzweigung vorherzusagen und führt Code entsprechend spekulativ aus, noch bevor das korrekte Ziel bekannt ist. Ergebnisse aus falschen Vorhersagen oder unberechtigten Zugriffen werden zwar verworfen und nicht weitergegeben (transient ausgeführt), führen aber zu einer Änderung des mikroarchitekturellen Zustands der CPU, etwa dem Inhalt der Caches. Diese Veränderung ist unter bestimmten Voraussetzungen von einem Angreifer wahrnehmbar, etwa durch Messung der Cachezugriffszeiten, und führt somit mittelbar zur Offenlegung von geschützten Inhalten.

Im Laufe des Jahres wurden mehr als 20 konkrete Methoden dieser mikroarchitekturellen Seitenkanalangriffe vornehmlich aus dem akademischen Umfeld bekannt.

Die teils sehr spezifisch auf eine (Mikro-)Architektur abgestimmten Methoden und der allgemein probabilistische Ansatz der Angriffe erschweren es erheblich, diese Angriffsklasse großflächig auszunutzen. Gezielte Angriffe, insbesondere im Umfeld der Cloud-Virtualisierung, erscheinen aber plausibel.

Eine als SPOILER bekannt gewordene Methode zielt z. B. darauf ab, die in Intel CPUs implementierte Zuordnung von virtuellen zu physischen Speicheradressen zu rekonstruieren. Die so gewonnenen Informationen können insbesondere genutzt werden, um ein als Rowhammer bekanntes Fehlverhalten von als Hauptspeicher genutzten DRAM-Zellen gezielter auszunutzen. Bei Letzterem handelt es sich um die versuchte gezielte Veränderung einzelner Bits durch hochfrequent wiederholtes Auslesen benachbarter Speicherzeilen.

Bisher konnten jedoch keine Anzeichen dafür beobachtet werden, dass transiente Ausführungsangriffe aktiv im Feld ausgenutzt werden.

Seitens der CPU-Hersteller wurden für die ursprünglichen Angriffsvarianten Gegenmaßnahmen entwickelt und bereitgestellt, welche die Ausnutzung erschweren oder verhindern sollen. Intel CPUs sind seit den ab Herbst 2018 erschienenen Prozessorarchitekturen („Whiskey Lake“ Mobile, „Cascade Lake“ Server) nach Herstellerangabe hardwareseitig gegen die besonders kritischen Angriffstypen *Meltdown* und *Foreshadow* geschützt. Für ältere Prozessoren sind Sicherheitsupdates auf Ebene des Betriebssystems verfügbar.

Für die Angriffstypen Spectre V1 und V2 wurden ebenfalls Schutzmaßnahmen auf Betriebssystemebene sowie als Microcode-Update (Spectre V2) entwickelt. Diese sind jedoch oft nur gegen bestimmte konkrete Angriffsvarianten wirksam. Die verfügbaren Maßnahmen gehen mit teils signifikanten Leistungseinbußen einher, welche erst mit kommenden Prozessorgenerationen hardwareseitig entschärft werden können. Insbesondere gegen den Angriffstyp Spectre V1 sind keine Lösungen erkennbar, die ausschließlich auf hardwareseitigen Gegenmaßnahmen basieren.

Die Erfahrungen in diesem noch eher jungen Feld der transienten Angriffe auf CPU-Mikroarchitekturen sprechen dafür, dass diese eine auf Dauer angelegte Beobachtung und Analyse erfordern. Die sich daraus ergebenden Bedrohungssannahmen sind Bestandteil aktueller Sicherheitsanalysen und finden verstärkt Berücksichtigung in der Evaluation der Sicherheitseigenschaften von Systemplattformen.

Die Auswirkungen der Klasse transienter Ausführungsangriffe auf bestehende Systeme lassen sich durch die Installation von verfügbaren Updates für Anwendungen

(insbesondere Browsern), Betriebssysteme und Microcode abmildern. Inwiefern Anwendungen aber tatsächlich über konkrete Schutzmechanismen passend zum eingesetzten Prozessor verfügen, ist in der Regel für den Anwender nicht ersichtlich.

Aufgrund der Vielzahl an betroffenen Prozessorarchitekturen ergibt sich ein äußerst unübersichtliches Bild über den tatsächlichen Stand potenziell anfälliger Systeme. Zudem werden grundsätzlich verfügbare sicherheitskritische Updates zum Teil nicht automatisch eingespielt oder sind aufgrund der starken Fragmentierung des Marktes nicht für jedes Gerät erhältlich (z. B. bei Smartphones, insbesondere bei Android-basierten Systemen). Potenziell signifikante Leistungseinbußen bei Installation aller verfügbaren Gegenmaßnahmen sind ebenfalls zu erwarten, was eine Installation unattraktiv macht.

Im Vergleich zu Bedrohungen durch sonstige Schadsoftware und Exploits erscheinen transiente Angriffe – außerhalb virtualisierter Cloud-Anwendungen – als untergeordnetes Problem. Die Infiltration eines Systems über klassische Wege, etwa Schadprogramme oder Spear-Phishing-Angriffe, scheinen auch langfristig die vielversprechenderen Angriffsvektoren zu sein.

Es ist nicht abzusehen, dass eine vollständige Mitigation transienter Angriffsvektoren mittelfristig hardwareseitig erfolgen kann. Beim Design sicherer Systeme sollte daher vermehrt auf eine wirkungsvolle, möglichst weitgehend physische Separation zwischen Anwendungen und schützenswerten Geheimnissen gesetzt werden, etwa durch den verstärkten Einsatz von dedizierten Sicherheitselementen.

Cyber-Sicherheitslage 2019

Aktion und Reaktion



EMOTET

Hocheffizientes Social-Engineering



RANSOMWARE

Fortschrittliche Angriffstechniken führen zu massiven Konsequenzen

114 Mio.

neue Schadprogramm-Varianten

bis zu
110.000

Botinfektionen täglich
in deutschen Systemen

300 Gbit/s

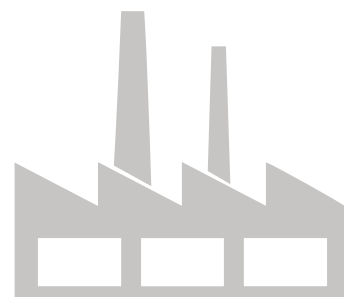
erreichten die Peaks in der Angriffsbandbreite
über die Cloud

2019: 300 Gbit/s

2018: >100 Gbit/s

40 Mio.
Euro

Schaden erlitt ein einzelnes
Unternehmen durch einen
Ransomware-Angriff





Ca. **770.000**

Mails mit Schadprogrammen in
deutschen Regierungsnetzen abgefangen



11,5 Mio.

Meldungen zu Schadprogramm-
Infektionen übermittelte das BSI
an deutsche Netzbetreiber



1.500

registrierte KRITIS-Anlagen

2019:

252

Meldungen von
KRITIS-Betreibern

2018:

145

Meldungen

3.700

Mitglieder der Allianz für Cyber-Sicherheit
(2018 = 2.700 Mitglieder)

105.000

Abonnenten Bürger-CERT
(2018 = 100.000 Abonnenten)



2 Zielgruppenspezifische Lösungen und Angebote

2 Zielgruppenspezifische Lösungen und Angebote

Im folgenden Kapitel werden unter Bezug auf die aktuelle Gefährdungslage der IT-Sicherheit anhand ausgewählter Themen Lösungsansätze und Angebote des BSI dargestellt - gegliedert nach den Aufgabenbereichen Staat/Verwaltung, Wirtschaft/Kritische Infrastrukturen, Gesellschaft/Bürger und Internationales/Wissenschaft. Um diese Angebote praktisch nutzbar zu machen, wird über Links auf zahlreiche Publikationen und Internetangebote des BSI verwiesen.

2.1 Staat/Verwaltung

Eine der Kernzielgruppen des BSI sind staatliche Stellen, insbesondere die Behörden des Bundes. Hier bietet das BSI zahlreiche Dienste wie im Folgenden auszugsweise beschrieben. Der Bedarf bei Behörden nach hochsicherer Verschlüsselung für die Erzeugung, Übermittlung und Speicherung vertraulicher Informationen wächst. Im Zeitalter der Digitalisierung erwartet der Nutzer, sich hochsicher, unkompliziert und schnell austauschen zu können. Die klassische Bearbeitung von staatlich geheimzuhaltenden Informationen und die Informationstechnik müssen einander in zunehmendem Maße wechselseitig unterstützen. Aus den sich entwickelnden Technologieansätzen entstehen Möglichkeiten zur Nutzung von für den staatlichen Geheimschutz konzipierten IT-Produkten in ganz neuen Einsatzfeldern. Das BSI unterstützt bei der Planung und Umsetzung hochsicherer Informationssicherheit.

2.1.1 Gefährdungslage der Bundesverwaltung

Die Abwehr von Gefahren für die Sicherheit der Informationstechnik des Bundes ist eine der gesetzlichen Kernaufgaben des BSI. Insbesondere erfüllt das BSI bereits seit seiner Gründung die Aufgabe, die zentralen Netze der Bundesverwaltung zu schützen. So trägt das BSI unter Mitwirkung von BMI und der Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS) Mitverantwortung für das IT-Sicherheitskonzept des Regierungsnetzes.

Die Informationssicherheitsleitlinie des Bundes (UP Bund) definiert die verbindlichen Rahmenbedingungen für den Schutz der in der Bundesverwaltung verarbeiteten Infor-

mationen und der dabei genutzten IT-Systeme, Dienste und Kommunikationsnetzinfrastrukturen. Diese sind als verbindliche und einheitliche Mindestanforderungen zu verstehen. Sie werden auf Basis der Standards für IT-Grundschutz des BSI in der jeweils gültigen Fassung festgelegt. Die Regelungen sind von den Ressorts im jeweiligen Zuständigkeitsbereich eigenverantwortlich umzusetzen sowie um die im jeweiligen Bereich notwendigen weiteren Anforderungen zu erweitern. Das BSI unterstützt hierbei im Rahmen seiner Aufgaben aus dem BSIG. Einen Lageüberblick erhält es insbesondere als zentrale Meldestelle und aus der IT-Sicherheitsberatung.

Die wichtigsten Sicherheitsmaßnahmen für das zentrale Regierungsnetz sind eine durchgängig verschlüsselte Kommunikation und eine robuste, redundante Architektur. Darüber hinaus wird ein geregelter, vertrauensvoller Betrieb gewährleistet. Zudem wird die sicherheitstechnische Aufstellung der Netze permanent verbessert sowie auch eine enge Anbindung der Netze der Länder und Kommunen realisiert.

Für den bestmöglichen Schutz der Netze und IT-Systeme hat das BSI ein mehrstufiges Sicherheitssystem etabliert. Es besteht neben kommerziellen Schutzprodukten auch aus individuell angepassten und entwickelten Maßnahmen. Sie werden kontinuierlich überprüft, weiterentwickelt und an die dynamische Bedrohungslage angepasst. Durch die Kombination verschiedener Abwehrmaßnahmen hat das BSI ein gutes Bild über die IT-Sicherheitslage der Regierungsnetze und steht diesbezüglich im täglichen Austausch mit dem Betreiber der Regierungsnetze, der BDBOS.

2.1.1.1 Erkenntnisse aus dem Schutz der Regierungsnetze

Cyber-Angriffe auf die Regierungsnetze finden täglich statt. Als Regierungsnetze werden die Netze des Bundes (NdB) und das gemeinsame Bund-Länder-Netz bezeichnet. Neben ungezielten Massenangriffen sind die Regierungsnetze auch gezielten Angriffskampagnen ausgesetzt.

Dabei zählen E-Mails mit Schadprogrammen zu den am häufigsten detektierten Angriffen auf die Bundesverwaltung. Mittels automatisierter Antivirus-Schutzmaßnahmen wurden pro Monat durchschnittlich 64.000 solcher E-Mails in Echtzeit abgefangen, bevor sie die Postfächer der Empfänger erreichten. Davon wurden monatlich im

Durchschnitt rund 39.000 schädliche E-Mails nur aufgrund vom BSI selbst erstellter Antivirus-Signaturen erfasst. Der signifikante Anstieg dieser Zahlen im Vergleich zum Vorjahresbericht ist insbesondere auf die hohe Anzahl von Emotet-Wellen zurückzuführen, die auch außerhalb der Regierungsnetze zu beobachten waren. Wie in den beiden Vorjahren hat sich der Trend fortgesetzt, dass Schadprogramme häufig nicht als Dateianhang in E-Mails versendet, sondern über Links in E-Mails verteilt werden.

Im HTTP-Verkehr wurden im Berichtszeitraum durchschnittlich rund 750 Schadprogramme und in der Spitze fast 2000 Schadprogramme pro Monat erkannt und abgewehrt.

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 6.100 Angriffe pro Monat identifizieren, die von den eingesetzten kommerziellen Schutzprodukten nicht detektiert oder blockiert werden konnten.

Zusätzlich zu diesen detektierten Angriffen wurden im Berichtszeitraum über zwei Millionen Zugriffe aus dem Regierungsnetz auf Server unterbunden, die mit Schadcode, Betrug oder Datendiebstahl in Verbindung standen.

2.1.1.2 Erkenntnisse aus Meldungen aus der Bundesverwaltung

Nach § 4 Abs. 3 BSIG sind die Bundesbehörden verpflichtet, das BSI unverzüglich zu unterrichten, wenn bei ihnen Informationen vorliegen, die für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik von Bedeutung sind. Hierbei handelt es sich um die so genannten SOFORT-Meldungen. Ziel ist es, jederzeit über ein verlässliches Bild der aktuellen IT-Sicherheitslage in der Bundesverwaltung zu verfügen. Handlungsbedarf und Handlungsoptionen bei IT-Sicherheitsvorfällen auf staatlicher Ebene als auch in der Wirtschaft sollen so schnell und kompetent eingeschätzt werden können.

SOFORT-Meldungen sind vorfallsbezogen und daher in ihrer Häufigkeit unregelmäßig. Grundsätzlich ist jedoch

auch das zahlenmäßige Aufkommen der Meldungen ein Indikator, um die Bedrohungslage zu bewerten.

Im Jahr 2018 wurden insgesamt 140 SOFORT-Meldungen an die „Zentrale Meldestelle und Nationales IT-Lagezentrum“ gemeldet.

2.1.1.3 Erkenntnisse aus der Informationssicherheitsberatung

Die medienwirksame Veröffentlichung umfassender persönlicher Informationen und Dokumente von politischen Mandatsträgern, Amtsträgern und Personen des öffentlichen Lebens Ende 2018/Anfang 2019 (siehe Vorfall Doxing auf Seite 9) zeigte einmal mehr auf, was im Hinblick auf unerlaubte Preisgabe von Daten möglich ist und auch jede andere Person betreffen kann oder schon getroffen hat. Die besondere Bedeutung liegt nicht nur in der Veröffentlichung von unerlaubt erlangten Informationen, sondern in der Aggregation dieser mit öffentlich zugänglichen Informationen. Diese Art der Informationssammlung kann ein recht umfassendes digitales Persönlichkeits- und Aktivitätsprofil einer Person ergeben und somit digitale oder analoge Angriffsformen auf eine Person ermöglichen bzw. erleichtern. Zielgerichtete und mit persönlichen Informationen versehene schadhafte E-Mails oder Identitätsdiebstahl sind nur einige Angriffsarten, die das Sammeln und Auswerten umfassender Informationen über eine Person erlauben. Der Vorfall zeigt auf, dass digitale (private) Identitäten und persönliche Daten noch intensiver vor unbefugtem Zugriff geschützt werden müssen sowie die eigenständige Veröffentlichung von potenziell sensiblen Informationen dem Gebot der Datensparsamkeit folgen sollte. Er belegt auch, dass unabhängig agierende Personen nicht notwendigerweise durch ein umgebendes, schützendes Informationssicherheitsmanagementsystem (ISMS) einer Institution (mit-) geschützt sind, sondern selbst zu ihrem eigenen Schutz beitragen müssen.

Ausgehend von durchgeführten Bedarfsabfragen und Erkenntnissen aus der Informationssicherheitsberatung ist ein erhöhter Bedarf nach Beratung zur Informationssicherheit auch auf Landesebene und kommunaler Ebene festzustellen. Einige Beratungsleistungen des BSI umfassen dabei Aktivitäten zur Umsetzung des Onlinezugangsgesetzes (OZG) wie etwa Beiträge zur Informationssicherheit für das Onlinegateway des Portalverbundes und zu weiteren Grundlagen für einige Digitalisierungsvorhaben bei übergreifenden Verwaltungsprozessen zwischen Bund, Ländern

2010	2011	2012	2013	2014	2015	2016	2017	2018	Bis 30.05.2019
136	138	216	79	149	150	182	157	140	48

Tabelle 01 abgegebene SOFORT-Meldung nach § 4 Abs. 3 BSIG

und Kommunen. Die zu digitalisierenden Verfahren, welche u. a. „digitale Behördengänge“ erfordern, stehen dabei im besonderen Fokus. Denn Angriffe auf diese Verfahren könnten in ihren Auswirkungen prinzipbedingt nicht nur die öffentliche Verwaltung als Verfahrensinhaber betreffen, sondern auch die Bürger und Unternehmen als Nutzer dieser Verfahren. Aufgrund dieser großen Reichweite bestehen hier besondere Anforderungen an die Informationssicherheit, zu denen sich ein wachsender Beratungsbedarf ergibt. Dies gilt ebenso für zu digitalisierende Leistungen der Justizverwaltung. Auch in Bezug auf die Justiz ist die Sicherheitsberatung des BSI unterstützend tätig und trägt so dazu bei, ein angemessenes Sicherheitsniveau zu schaffen und zu gewährleisten.

2.1.2 Lösungen und Angebote des BSI für Bund, Länder und Kommunen

Wie begegnet das BSI den aktuellen Gefährdungen, welche Maßnahmen können den Risiken entgegengesetzt werden? Im Folgenden werden anhand ausgewählter Themen der IT-Sicherheit Lösungsansätze und Angebote des BSI dargestellt.

2.1.2.1 Cyber-Abwehrzentrum

Das Nationale Cyber-Abwehrzentrum (Cyber-AZ) dient dem behördenübergreifenden Austausch zu Cyber-Sicherheitsvorfällen in Deutschland. Im Rahmen dieser Kooperations- und Informationsplattform arbeiten das Bundesamt für den Militärischen Abschirmdienst (BAMAD), das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), das Bundesamt für Verfassungsschutz (BfV), das Bundeskriminalamt (BKA), der Bundesnachrichtendienst (BND), die Bundespolizei (BPOL), das BSI, das Kommando Cyber- und Informationsraum (KdoCIR) und das Zollkriminalamt (ZKA) zusammen. Anlassbezogen werden weitere Bundes- sowie Landesbehörden und Wirtschaftsunternehmen einbezogen.

Als federführende Behörde stellte das BSI im Berichtszeitraum den Leiter, die Geschäftsstelle samt Personal sowie die Räumlichkeiten. Durch kurze Wege zwischen dem Cyber-AZ und dem Nationalen IT-Lagezentrum/IT-Krisenreaktionszentrum, dem CERT-Bund und den mobilen Einsatzteams des BSI (Mobile Incident Response Team, MIRT) sowie der engen Kooperation mit den beteiligten Behörden ist eine effiziente Zusammenarbeit auch in Krisensituationen sichergestellt.

Die Arbeit des Cyber-AZ erstreckt sich neben dem Austausch cyber-sicherheits-relevanter Informationen insbesondere darauf, die Bearbeitung von Cyber-Vorfällen

einschließlich der Erarbeitung von Handlungsempfehlungen zum Schutz und zur Abwehr solcher Vorfälle in Deutschland zu koordinieren und die operativen Maßnahmen der zuständigen Behörden abzustimmen. Die konkrete Fallbearbeitung wird von den beteiligten Behörden dabei im Rahmen ihrer jeweiligen Aufgaben und Befugnisse durch deren zuständige Fachreferate übernommen. Die Ergebnisse der Fallbearbeitung werden kontinuierlich im Cyber-AZ zusammengeführt, bewertet und an die jeweiligen Stellen berichtet.

Einer der im Berichtszeitraum bekannt gewordenen herausragenden Fälle, der im Cyber-AZ bearbeitet wurde, war die Veröffentlichung hunderter Datensätze von politischen Mandatsträgern, Amtsträgern und Personen des öffentlichen Lebens (siehe Vorfall Doxing auf Seite 9). Im Nationalen Cyber-Abwehrzentrum erfolgte die Abstimmung der Fallbearbeitung durch die zuständigen Behörden.

Im Berichtszeitraum wurde eine Weiterentwicklung der Zusammenarbeit im Cyber-AZ durchgeführt, welche im Laufe des Jahres 2019 wirksam wird.

2.1.2.2 Bundes Security Operations Center (BSOC)

Das BSI beobachtet eine konstant steigende Professionalisierung von Angreifern bei sinkenden Aufwänden für die Durchführung der Angriffe. Dieser bedrohlichen Lage begegnet das BSI schon seit Jahren durch die kontinuierliche Weiterentwicklung der Schutzmaßnahmen in den Regierungsnetzen. Die aktuellen Angriffsformen (z. B. APT-Angriffe) zeigen aber, dass die bislang übliche, ergänzende und eigenständige Erkennung und Abwehr von Cyber-Angriffen durch jede Bundesbehörde ausschließlich für deren eigene IT nicht mehr ausreicht. Das BSI hat daher im Rahmen seiner Aufgabe als BSOC durch eine größtmögliche Automatisierung unter Nutzung aktueller Standardprodukte, Eigenentwicklungen und KI-unterstützter Verfahren ausreichend Freiräume für die unverzichtbaren manuellen Analysen zu schaffen, die auch bislang schon Voraussetzung für die sehr erfolgreiche Erkennung von Angriffen waren. Ziel des BSOC ist zudem die zentrale Koordinierung der dezentralen Erkennungs- und Abwehrmaßnahmen in der Bundesverwaltung, die durch zentrale Dienste u. a. im Rahmen der IT-Konsolidierung des Bundes ergänzt werden.

Die bisher schon durch das BSI wahrgenommenen Aufgaben als Bundes-CERT und zentrales Lagezentrum des Bundes für Cyber-Sicherheitsvorfälle gewährleisten, dass auf erkannte Angriffe schnell und im Bedarfsfall auch vor Ort (Mobile Incident Response Team) reagiert werden kann.

2.1.2.3 Nationales Verbindungswesen und Ausbau der Bund-Länder-Zusammenarbeit

Die Gestaltung von Cyber-Sicherheit in der Digitalisierung kann nur gemeinsam von Bund und Ländern zum Erfolg geführt werden. Daher bietet das BSI den Ländern Unterstützung an und ergreift die erforderlichen Maßnahmen, um die Zusammenarbeit auf verschiedenen Ebenen auszubauen und Synergieeffekte zu erzielen.

Übergeordnetes Ziel der Zusammenarbeit ist es, ein angemessenes Niveau der Informationssicherheit in der Bundesrepublik Deutschland zu schaffen. Dieses Ziel wird insbesondere angesichts der fortschreitenden Digitalisierung der Verwaltung und einer zunehmenden Vernetzung von IT-Strukturen immer wichtiger.

Durch den Aufbau des Nationalen Verbindungswesens im BSI wird die Zusammenarbeit mit den Ländern vertieft. Feste Ansprechpartner in den Ländern ermöglichen es, sich eng und regelmäßig mit Ländern und Kommunen auszutauschen. Das BSI entsendet hierfür seit 2017 Verbindungspersonen nach Wiesbaden und Berlin. Seit 2018 wird auch die Region West aus dem BSI in Bonn heraus vom Nationalen Verbindungswesen betreut. Anfang 2019 sind Ansprechpartner für die Regionen Süd und Nord in Stuttgart und Hamburg hinzugekommen. Aufgrund der erfolgreichen Pilotierung des Nationalen Verbindungswesens wurden im Mai 2019 Ansprechpartner des BSI nach Dresden entsandt.

Das BSI als nationale Kompetenzstelle für Cyber-Sicherheit unterstützt die Länder bei der Erhöhung der Cyber-Sicherheit. Ziel ist es, das Know-how des BSI über verschiedene Schnittstellen auch den Ländern zur Verfügung zu stellen. Die Form der Zusammenarbeit wird dabei jeweils in Absichtserklärungen festgelegt. Die ersten Absichtserklärungen wurden Ende 2017 unterzeichnet. Bis zum Ende des Berichtszeitraums hat das BSI Absichtserklärungen mit neun Bundesländern unterzeichnet. Für das zweite Halbjahr 2019 befinden sich weitere Erklärungen in Vorbereitung.

2.1.2.4 Evaluierung zur Umsetzung des Umsetzungsplans Bund

Die im September 2017 in Kraft getretene Neufassung des Umsetzungsplans Bund (UP Bund) als Leitlinie für Informationssicherheit in der Bundesverwaltung bot die Chance, die geplante jährliche Evaluierung zu dessen Umsetzung ebenfalls an die veränderten Rahmenbedingungen anzupassen und zu modernisieren. Übergeordnetes Ziel des UP Bund und der zugehörigen jährlichen Erhebung zum Umsetzungsstand ist die kontinuierliche Verbesserung der Informationssicherheit in der Bundesverwaltung

durch ein Monitoring und eine gezielte ressortübergreifende Steuerung. Bei der Neukonzeption der Evaluierung wurde daher ein prozessgesteuerter Ansatz gewählt, um geeignetere Auswertungs- und Steuerungsmethodiken für die Ressorts und Einrichtungen der Bundesverwaltung zu ermöglichen. Insbesondere wird die Evaluierung auf Basis eines für diese Zwecke angepassten Reifegradmodells stattfinden, das den Entwicklungsstand der Informationssicherheit in einem Ressort bzw. einer Einrichtung anhand der Vorgaben des UP Bund stufenweise beschreibt. Hierfür wurden die Anforderungen aus den einzelnen Kapiteln des UP Bund 2017 gemäß der Reifegradmethodik in Kriterien und Indikatoren übersetzt. Die Ergebnisse von mehreren Evaluationen des UP Bund über die verschiedenen und abgestimmten Berichtszeiträume hinweg lassen sich durch den gleichbleibenden Fragenkatalog auf Basis des Reifegradmodells vergleichen. Aufgrund der Entwicklung der Reifegrade können Kurz-, Mittel- und Langzeitrückschlüsse getroffen werden. Individuell vorhandene Verbesserungspotenziale und dazu notwendige Maßnahmen können durch das Reifegradmodell leichter identifiziert und geeignet priorisiert werden. Ergänzend werden einzelne Sachverhalte pro Berichtszeitraum flexibel außerhalb der angepassten Reifegradmethodik erhoben. Dadurch können auch aktuelle Themen wie z. B. der modernisierte IT-Grundschutz bzw. Gefährdungslagen der Bundesverwaltung in den jährlichen Bericht einfließen, ohne dass die Vergleichbarkeit über die verschiedenen Berichtszeiträume hinweg tangiert wird. Im Rahmen der Aktualisierung wurde das vom BSI entwickelte Konzeptions- und Auswertungs-Tool für Erhebungen (KATE) anteilig überarbeitet und an die technischen Bedürfnisse der Erhebung angepasst, um eine standardisierte und automatisierte Auswertung und Steuerung zu ermöglichen.

2.1.2.5 Informationssicherheitsberatung

Die unbefugte Veröffentlichung von persönlichen Daten und Dokumenten im Internet stellte die Informationssicherheitsberatung Anfang 2019 vor die Aufgabe, den betroffenen Politikern, Amtsträgern und sonstigen Personen des öffentlichen Lebens ein Beratungs- und Unterstützungsangebot zu unterbreiten, das über die bisherigen, etablierten Angebote der Sicherheitsberatung für die Bundesverwaltung hinausgehen musste.

Neben ausführlichen persönlichen und individuellen Beratungen vor Ort entwickelte die Sicherheitsberatung in Zusammenarbeit mit weiteren Stellen im BSI konkrete und individuelle Maßnahmenpakete sowie Empfehlungen und Tipps zur Verbesserung der Informationssicherheit bei den Betroffenen. Hierzu gehörten Informationen, wie E-Mail-Postfächer und Benutzerprofile, z. B. in sozialen Netzwerken, sinnvoll abgesichert werden können. Empfehlungen zur sicheren Verwendung von Messengern, Cloud-Diensten,

zur Basis-Absicherung von IT-Geräten wie Smartphones sowie Kontaktmöglichkeiten zur Meldung von Vorfällen ergänzen die Handreichungen.

Die Informationssicherheitsberatung unterstützte im Berichtszeitraum darüber hinaus bei großen Digitalisierungsvorhaben der öffentlichen Verwaltung und Justiz, u. a. im Rahmen der Umsetzung des Onlinezugangsgesetzes (OZG) sowie bei der Absicherung des elektronischen Rechtsverkehrs. Zudem wurden Beratungen zu Themen wie Zensus 2021 durchgeführt und die Bundeswahlleitung zur Absicherung der Europawahl intensiv unterstützt. In Zusammenarbeit mit der Bundesakademie für öffentliche Verwaltung (BAköV) konnte die Fortbildung für IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung erfolgreich fortgeführt werden.

Mit der Umorganisation des BSI zum 15. April 2019 wurde ein neues Referat Informationssicherheitsberatung für Länder und Kommunen gegründet, u. a. um dem erhöhten Beratungsbedarf an Informationssicherheit auf Landes- und kommunaler Ebene zielgruppenspezifisch gerecht zu werden.

Die Informationssicherheitsberatung des BSI für Länder und Kommunen berät und unterstützt Landesverwaltungen sowie die drei kommunalen Spitzenverbände bei allen Fragen der Informationssicherheit mit den thematischen Schwerpunkten Informationssicherheitsmanagement, Sicherheitskonzeption, IT-Grundschutz. Dabei sind die Vorgaben aus der Informationssicherheitsleitlinie für die öffentliche Verwaltung (ISLL) sowie die jeweiligen landeseigenen Vorgaben und Anforderungen zu berücksichtigen. Grundlage für die Beratungstätigkeiten sind insbesondere die mit den Ländern jeweils abgeschlossenen Absichtserklärungen.

Die Informationssicherheitsberatung arbeitet auch eng mit den kommunalen Spitzenverbänden zusammen. Aufgrund der großen Anzahl an Kommunen wird eine Unterstützung der kommunalen Ebene weitgehend nur durch vielfach noch einzurichtende Multiplikatoren- und Bündelungsrollen erfolgen.

Durch die Leitung der Geschäftsstelle der Arbeitsgruppe Informationssicherheit (AG InfoSic) des IT-Planungsrats (IT-PLR) seit 2018 sowie die regelmäßige Mitwirkung in den einschlägigen Gremien erhält die Informationssicherheitsberatung für Länder und Kommunen einen kontinuierlichen Einblick in die Lage der Informationssicherheit in den Landesverwaltungen und ist somit in der Lage, die Cyber-Sicherheit nicht nur im Bund, sondern auch in den Ländern (und den Kommunen) angemessen mitgestalten zu können.

2.1.2.6 Informationssicherheit bei Europawahl und Landtagswahlen

Die Informationssicherheitsberatung des BSI hat im Rahmen ihrer Strategie zur Absicherung von Wahlen auch die Europawahl 2019 betreut. In enger Zusammenarbeit und Mitarbeit in einer Arbeitsgruppe des Bundes- und der Landeswahlleiter (Bund-Länder-AG) wurden Informationssicherheitsziele entwickelt, die erfolgreich zum Schutz der Ergebnisübermittlung am Wahltag etabliert wurden. Ziel war die Stärkung der Integrität und Verfügbarkeit des Kern-Wahlprozesses. In dieser Sache hat das BSI die Bundeswahlleitung zur Informationssicherheit des Kern-Wahlprozesses bei der Ermittlung des vorläufigen Ergebnisses beraten. Betrachtet wurden die kommunale Ebene, die der Länder und die des Bundes. Das Vorgehen erfolgte angelehnt an den IT-Grundschutz des BSI. Dabei wurden die Erfahrungen aus der Bundestagswahl 2017 berücksichtigt. Ein weiteres Ziel war die Erhöhung der Resilienz gegen technische Manipulationsversuche im Umfeld der Wahlen. Hier hat das BSI Parteien und Kandidaten Beratungsangebote unterbreitet, das nationale Wahl-Kooperationsnetzwerk unterstützt, die Lage vor und während der Europawahl im Lagezentrum des BSI beobachtet und analysiert, Gespräche mit Plattformbetreibern Sozialer Medien geführt und an der europäischen Wahlübung am 5. April 2019 teilgenommen. Das BSI arbeitet zudem an der Erstellung des europäischen Kompendiums zur Cyber-Sicherheit von Wahltechnologie mit.

Neben der Europawahl ergab sich im laufenden Jahr ein Beratungsschwerpunkt bei den Landtagswahlen in Hessen und Bayern. Hier hat das BSI seine Erfahrungen bei der Absicherung der Ermittlung des vorläufigen Wahlergebnisses eingebracht. Das BSI hat damit dazu beigetragen, ein angemessenes Informationssicherheitsniveau zu gewährleisten. Die dabei gewonnenen Erkenntnisse zur Absicherung von parlamentarischen Wahlen werden in das Beratungsangebot des BSI zukünftig einfließen. Langfristiges Ziel der BSI-Aktivitäten ist, bei allen parlamentarischen Wahlen in Deutschland ein durchgängiges und an allen Stellen des Wahlprozesses einheitliches Sicherheitsniveau zu schaffen. Dies schließt eine Definition von Anforderungen an Wahlsoftware ein.

2.1.2.7 IT-Konsolidierung des Bundes

Die IT-Konsolidierung des Bundes wurde 2015 per Kabinettsbeschluss gestartet. Sie zielt auf

1. eine Konsolidierung des IT-Betriebs der Dienststellen der Bundesverwaltung bei wenigen Dienstleistern (Betriebskonsolidierung),

2. eine Konsolidierung der gemeinsamen IT-Dienste des Bundes (Dienstekonsolidierung), sowie
3. die Bündelung der IT-Beschaffung bei einer zentralen IT-Beschaffungsstelle (Beschaffungsbündelung).

Im Jahr 2018 zeichnete sich deutlicher als bisher ab, dass die IT-Konsolidierung Bund erhebliche Auswirkungen auf die IT-Governance der Bundesverwaltung hat. Denn die Abhängigkeit der Dienststellen von wenigen zentralen IT-Dienstleistern steigt und Entscheidungen über die konsolidierte IT betreffen grundsätzlich mehrere Ressorts.

Im Zuge der IT-Konsolidierung Bund entstehen daher einerseits neue Gremien, die Entscheidungen in der IT-Steuerung vorbereiten, z. B. der Anbieterbeirat. Das BSI vertritt in solchen Gremien die Anliegen der Informationssicherheit.

Andererseits arbeitet das BSI vor allem gestützt auf seinen Beratungsauftrag daran, das bisher erreichte Informationssicherheitsniveau der Bundesverwaltung auch in der zukünftig konsolidierten IT zu halten.

2.1.2.8 Digitalfunk BOS

Seit 2010 nutzen Behörden und Organisationen mit Sicherheitsaufgaben (BOS) in der Bundesrepublik Deutschland ein Digitalfunknetz für ihre taktische Kommunikation. Durch die Verwendung des vom BSI entwickelten Ende-zu-Ende-Verschlüsselungssystems für Sprache und Kurznachrichten wird im Digitalfunknetz BOS eine sehr hohe Vertraulichkeit der Kommunikation erreicht. Eines der Kernelemente des Verschlüsselungssystems ist die vom BSI entwickelte Sicherheitskarte, die gleichzeitig auch den Zugang zum Digitalfunknetz ermöglicht. Mittlerweile befinden sich über 800.000 dieser Sicherheitskarten im Einsatz.

Für die Sicherheitskarten- und Schlüsselverwaltung entwickelt das BSI auch passende Managementsysteme. Diese werden zum Teil vom BSI selbst, zum Teil von den einzelnen Bedarfsträgern betrieben. Diese dynamische Sicherheitsarchitektur bietet jedem Nutzer die Möglichkeit, eigene Anforderungen hinsichtlich des Betriebs und des Sicherheitsniveaus umzusetzen.

Die fortschreitende technologische Entwicklung erfordert, auch diese Systeme permanent weiterzuentwickeln. Ein zusätzlicher Technologiewechsel von ISDN zu TCP/IP wurde aufgrund der Abkündigung von ISDN-Anschlüssen durch Kommunikationsunternehmen notwendig.

Die Hauptaufgaben des BSI im Bereich Digitalfunk BOS im vergangenen Jahr waren:

- die Weiterentwicklung der Managementsysteme, insbesondere deren Erweiterung um TCP/IP-Funktionalität,
- die Entwicklung eines Migrationstools, mit dem vorhandene Nutzerdaten aus bestehenden Systemen in neue überführt und hierbei konsolidiert und bereinigt werden können.
- Beratungen und Schulungen von Bedarfsträgern aus Bund und Ländern, welche in enger Abstimmung mit der Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS) durchgeführt wurden,
- die Vorbereitung für die Weiterentwicklung der Sicherheitskarten, welche neben einem technologischen Hardwarewechsel auch neue Funktionen bieten werden.
- Die Infrastruktur des Kryptosystems wurde erfolgreich um IP-Funktionalität erweitert.

2.1.2.9 Technologieverifikation in sogenannten Security Labs

Das BSI steht im Kontakt mit zahlreichen Herstellern von Informations- und Kommunikationstechnik und intensiviert den technischen Dialog über sogenannte Security Labs. Diese Labs dienen zum einen als Austauschplattform, um Meetings und Videokonferenzen zu den Entwicklungsabteilungen rund um den Globus durchzuführen, zum anderen können dort tiefere technische Diskussionen und Einblicke bis hin zur Einsichtnahme auf Quellcodeebene realisiert werden. Hierbei werden die BSI-Mitarbeiter u. a. von auf Codeaudits spezialisierten Experten akkreditierter Prüflabore unterstützt. Durch diesen engen Austausch mit den Entwicklungsabteilungen der Hersteller lassen sich frühzeitig Trends und Risiken erkennen. Ob beim frühen Prototyp oder beim bereits breit im Einsatz befindlichen Produkt, der Schwerpunkt der Betrachtungen liegt stets bei der Informationssicherheit. Das BSI kommt damit seiner Verantwortung für die Gestaltung der Informationssicherheit in Deutschland nach. In dieser Zusammenarbeit achtet das BSI strikt auf eine Gleichbehandlung aller Hersteller und legt vergleichbare Standards zugrunde.

2.1.2.10 App-Testing für mobile Lösungen

Mobile Lösungen gewinnen zunehmend an Bedeutung sowohl beim Staat als auch in Wirtschaft und Gesellschaft. Applikationen auf mobilen Geräten erweitern die Funktionalität des Grundsystems und spielen eine wesentliche Rol-

le für den Erfolg mobiler Lösungen. Der Einsatz von Apps birgt jedoch Sicherheitsrisiken sowohl für die Daten, die eine App verarbeitet, als auch für die Gesamtlösung. Diese Risiken müssen bewertet werden, um eine Gesamtaussage zur Sicherheit einer mobilen Lösung treffen zu können.

Der vom BSI zur Verfügung gestellte App-Testing-Dienst 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 Hinweise und Empfehlungen an die Nutzer, welche Einstellungen oder Randbedingungen für eine möglichst sichere Nutzung der betreffenden App beachtet werden sollten.

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

Im Juni 2019 wurde der App-Testing-Dienst von registrierten Nutzern aus 40 Behörden und Organisationen verwendet; für 71 bereits geprüfte Apps standen die Prüfergebnisse zum Abruf bereit.

2.1.2.11 Abstrahlsicherheit

Staatliche Stellen müssen gemäß § 57 VSA (Allgemeine Verwaltungsvorschrift des Bundesministeriums des Innern, für Bau und Heimat zum materiellen Geheimschutz) Maßnahmen zur Abstrahlsicherheit ergreifen, wenn Verschlusssachen (VS) des Geheimhaltungsgrades VS-VERTRAULICH oder höher elektronisch verarbeitet werden. Das BSI hat ein engmaschiges Prüfsystem etabliert, um Bedarfsträgern abstrahlgeprüfte IT-Hardware auf Basis handelsüblicher Plattformen zur Verfügung zu stellen. Neben einer Reihe von Standardlösungen für typische Büroanforderungen können sich Bedarfsträger bei vom BSI anerkannten Anbietern auch individualisierte Lösungen für spezifische Anforderungen zusammenstellen lassen und werden durch den Zulassungsprozess begleitet. Auf diese Weise hat das BSI im Berichtszeitraum 524 Gerätesätzen nach dem Nationalen Zonenmodell und 11 Gerätesätzen für die höchste Sicherheitsstufe „Level A“ eine TEMPEST-Zulassung erteilt.

Das BSI trägt durch intensive Beteiligung an internationalen TEMPEST-Fachgremien dazu bei, dass internationale Geheimschutzanforderungen zu nationalen Verfahrensweisen kompatibel bleiben. Hierzu setzt das BSI mit fachlichen Beiträgen und Analysen zum Stand der Technik aktiv Akzente. So werden internationale Vorgaben durch das BSI zur Wahrung deutscher Interessen mitgestaltet.

2.1.2.12 Lauschabwehr

Die BSI-Lauschabwehr hat zahlreiche Überprüfungen in abhörgefährdeten Bereichen von Behörden des Bundes und der Länder sowie bei der geheimschutzbetreuten Wirtschaft durchgeführt.

Darüber hinaus wurden Konferenzen, bei denen VS-eingestufte Inhalte zu erörtern waren, mit Beratungs- und Prüfmaßnahmen begleitet.

2.1.2.13 VS-Zulassungen

Das BSI ist laut BSI-Gesetz (§ 3 Abs.1 S.2 Nr.7) befugt, im Rahmen einer Evaluierung IT-Sicherheitsprodukte zu prüfen und mit der Zulassung verbindliche Aussagen zum Sicherheitswert zu treffen. Dies gilt für IT-Sicherheitsprodukte, die für die Verarbeitung, Übertragung und Speicherung von amtlich geheimgehaltenen Informationen im Anwendungsbereich der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern, für Bau und Heimat zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA) oder bei Unternehmen im Rahmen von Aufträgen der öffentlichen Verwaltung mit VS-Bezug eingesetzt werden. Nach § 51 VSA müssen Produkte, die innerhalb von Informationstechnik zur Handhabung von Verschlusssachen (VS-IT) IT-Sicherheitsfunktionen übernehmen, vom BSI zugelassen werden; welche Funktionen die Zulassung eines Produktes erfordern, wird in § 52 VSA aufgeführt. Der Antrag auf Zulassung eines IT-Sicherheitsproduktes kann grundsätzlich nur von einem behördlichen Anwender (Bedarfsträger) gestellt werden.

Wie in den Vorjahren hat das BSI im Berichtszeitraum erneut über 50 Zulassungen ausgesprochen bzw. verlängert. Damit erhöht sich die Anzahl der VSA-konform verwendbaren Produkte bzw. Produktversionen auf 240. Eine tagesaktuelle Auflistung der allgemein zugelassenen IT-Sicherheitsprodukte ist der BSI-Schrift 7164 zu entnehmen, die auf der Webseite des BSI (https://www.bsi.bund.de/DE/Themen/Sicherheitsberatung/ZugelasseneProdukte/zugelasseneProdukte_node.html) zur Verfügung steht.

Um auch weiterhin den Bedarf der öffentlichen Verwaltung an zugelassenen Produkten decken zu können, betreut das BSI aktuell mehr als 60 Verfahren mit dem Ziel einer Zulassung.

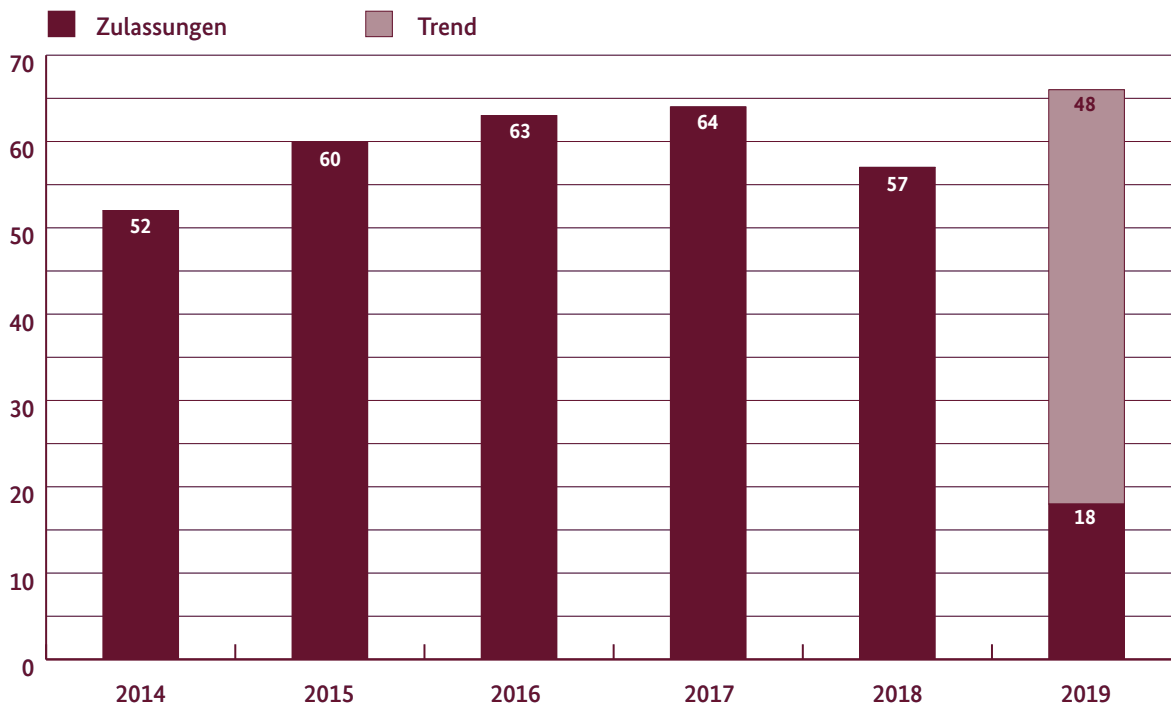


Abbildung 11 VS-Zulassungen der vergangenen fünf Jahre

Qualifiziertes Zulassungsverfahren

Das Qualifizierte Zulassungsverfahren für die Handhabung von Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) ist eine Vorgehensweise, die es unter Aufrechterhaltung der Vertrauenswürdigkeitsaussage des BSI ermöglicht, Zulassungsverfahren signifikant effizienter zu durchlaufen. Statt einer vollständigen rein technisch orientierten Produktevaluierung stützt es sich dabei auf die drei Säulen:

- Qualifizierung des Herstellers
- Konzeptionelle Evaluierung
- Herstellererklärung.

Durch diesen Ansatz durchlaufen Produkte des Geheimhaltungsgrades VS-NfD qualifizierter Hersteller effizient und dennoch effektiv einen wohldefinierten Prüfprozess. Dabei ist unter „effizient“ und „effektiv“ die Realisierung zeitnaher Prüfergebnisse bei optimiertem und ressourcensparendem Vorgehen bzw. die Wahrung der prinzipiellen Anforderungen an die Vertrauenswürdigkeit von IT-Sicherheitsprodukten zu verstehen.

Seit der Genehmigung des Verfahrens durch das BMI Mitte 2018 kann das Qualifizierte Zulassungsverfahren in vollem Umfang im Zulassungsschema des BSI genutzt werden. Nun steht der Abschluss der Verankerung in die Zulassungsprozesse sowie die Erhöhung der Anzahl „Qualifizierter Hersteller“ im Fokus. Das Qualifizierte Zulassungsverfahren wurde wie folgt in die Zulassungsprozesse integriert:

- Das Standard-Zulassungsverfahren behält weiterhin seine Gültigkeit und kommt für Zulassungen auf dem Niveau oberhalb VS-NfD, sowie für Hersteller, die sich noch nicht qualifiziert haben, zur Anwendung.
- Das BSI behält sich im Rahmen des Qualifizierten Zulassungsverfahrens vor, Produkte im Standard-Verfahren zu behandeln, auch wenn die entsprechenden Herstellervoraussetzungen erfüllt sind. Gründe dafür können insbesondere die Komplexität oder die spezielle Ausprägung eines zuzulassenden Produktes sein.
- Durch den Aufbau des Verfahrens ist gewährleistet, dass ein reibungsloser Übergang zwischen Standard- und Qualifiziertem Zulassungsverfahren möglich ist. Dies ist insbesondere in der Verwendung der Common

Criteria begründet, wodurch Herstellernachweise in einer zum Standardverfahren identischen Art und Weise vorliegen.

Eine signifikante Reduzierung der Aufwände im Qualifizierten Zulassungsverfahren steht einem minimalen Mehraufwand beim Erstdurchlauf einer Hersteller-Qualifizierung durch die zusätzlich zu erbringende Prozessevaluierung gegenüber. Wurde diese erfolgreich durchlaufen, können alle folgenden Zulassungsverfahren für Verschlusssachen des Geheimhaltungsgrades VS-NfD im Qualifizierten Zulassungsverfahren durchgeführt werden.

Neben dem Aufwand ist auch die Verfahrensdauer eines Qualifizierten Zulassungsverfahrens signifikant reduziert. Grund dafür ist, dass bei vorliegender Hersteller-Qualifizierung lediglich eine konzeptionelle Produktprüfung durchgeführt wird. Die im Standardverfahren angewandte detaillierte, tiefer greifende und iterative Prüfung, die wesentlich zu einer Verlängerung des Verfahrens führt, ist im Qualifizierten Zulassungsverfahren nicht mehr erforderlich.

Insgesamt führt das Qualifizierte Zulassungsverfahren damit zu einer effizienteren Bedarfsdeckung für zugelassene Produkte. Für die beteiligten Unternehmen stehen unter dem Aspekt „Time to Market“ neben einem finanziellen Gewinn durch das Verfahren die bessere Steuerbarkeit und zeitnahe Marktzuführung verbesserter und sicherer IT-Sicherheitsprodukte im Vordergrund.

Gemeinsam mit den bereits qualifizierten Herstellern sollen so bereits 2019 eine Reihe weiterer VS-NfD-Zulassungen ausgesprochen werden können, um den auch durch die VSA-Novellierung erhöhten Bedarf an zugelassenen IT-Sicherheitsprodukten besser decken zu können.

VS-Anforderungsprofile

Das BSI möchte dem stark wachsenden Bedarf der Bundesverwaltung an sicheren IT-Lösungen durch eine Optimierung des Zulassungsprozesses adäquat begegnen. Im Bereich der Verarbeitung, Übertragung und Speicherung von VS wird mit der Erstellung von VS-Anforderungsprofilen (VS-AP) für informationssichernde Systeme die Evaluierung und Zulassung deutlich beschleunigt. Dies spiegelt sich nicht zuletzt in der steigenden Anzahl zugelassener VS-IT-Systeme wider.

VS-Anforderungsprofile beschreiben IT-Sicherheitsanforderungen für bestimmte Produktklassen und -typen. Sie richten sich zum einen an Bedarfsträger und Betreiber wie beispielsweise Behörden und beschreiben die grundsätzlichen Anforderungen, denen Produkte genügen müssen, wenn diese beim Umgang mit eingestufteten Dokumenten

verwendet werden sollen. Zum anderen richten sich VS-AP an die Hersteller solcher Produkte, um diesen eine generelle technische Leitlinie zur Umsetzung geltender relevanter IT-Sicherheitsanforderungen zu geben.

Die einheitliche Formulierung technischer Sicherheitsgrundfunktionen ist eine wichtige Voraussetzung für die Zulassung von VS-Systemen. Bereits jetzt sind zahlreiche Bedarfsträger, Produkthersteller und Betreiber an einem Runden Tisch zusammengekommen, um die vorausschauende Gestaltung informationssichernder Systeme im VS-Bereich mitzugestalten.

Die Definition von VS-Anforderungsprofilen dient folgenden Zielen:

1. Gestaltung informationssichernder Systeme und Komponenten für den VS-Bereich durch das BSI,
2. Harmonisierung von IT-Sicherheitsanforderungen bestimmter Produktklassen und -typen,
3. Bedarfsgerechte Festlegung zeitgemäßer Anforderungen durch unmittelbare Beteiligung von Bedarfsträgern, Betreibern und Produktherstellern an der Entwicklung entsprechender VS-APs,
4. Effizienzsteigerung der Zulassungsverfahren im BSI durch frühzeitige Bereitstellung einschlägiger VS-APs.

Im Berichtszeitraum wurden vier VS-Anforderungsprofile publiziert, zwei überarbeitet und weitere zwei neu gestartet. Mit ihnen deckt das BSI unterschiedliche Produktklassen für den Schutz und die Verarbeitung von eingestuften Informationen ab. Parallel dazu befindet sich eine Vielzahl an VS-APs bzw. nPPs (national Protection Profile) für den Einsatz im VS-Bereich in der Vorbereitung für die Standardisierung weiterer IT-Sicherheitsprodukte. Der aktuelle Stand zur Entwicklung von Anforderungen an IT-Sicherheitssysteme zum Schutz von VS ist auf den Internetseiten des BSI zu finden (<https://www.bsi.bund.de/VS-Anforderungsprofile>).

Die Entscheidung des BSI, Bedarfsträger, Produkthersteller und Betreiber schon frühzeitig in die aktive Gestaltung derartiger IT-Sicherheitsanforderungen einzubinden, führt zu einer durchweg positiven Resonanz sowie regen Beteiligung am beschriebenen Vorgehen. Mit einem weiteren Ausbau des Themas VS-Anforderungsprofile trägt das BSI der gewonnenen Akzeptanz und Relevanz in 2019 Rechnung und begegnet den sich immer weiter verkürzenden Entwicklungszyklen des VS-Marktes adäquat.

2.2 Wirtschaft/Kritische Infrastrukturen

Vernetzung und Austausch sind ein wichtiger Faktor für die Produktivität und das wirtschaftliche Wachstum in Deutschland und damit wichtige Elemente des digitalen Wandels in der Industrie. Intelligente und miteinander vernetzte Maschinen tauschen Informationen direkt miteinander aus, Produktionsanlagen koordinieren Abläufe und Termine untereinander. Das macht die Produktion flexibler, dynamischer und effizienter. Mit den Vorteilen der Digitalisierung geht jedoch auch eine Erhöhung des Risikos einher, dessen sich die Beteiligten bewusst und auf das sie vorbereitet sein müssen. So ist die Mehrheit der Maschinen direkt mit allen IT-Systemen eines Unternehmens verbunden und kommuniziert so unmittelbar mit den Mitarbeitern. Dies erhöht die Anfälligkeit der Produkte und Unternehmen für Hackerattacken und Cyber-Angriffe. Im Folgenden findet sich eine Zusammenfassung der Erkenntnisse des BSI über die IT-Sicherheitslage in der Wirtschaft; darüber hinaus zielgruppenspezifische Angebote und Maßnahmen des BSI.

2.2.1 Gefährdungslage Wirtschaft/Kritische Infrastrukturen

Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das Gemeinwesen. Ihre Systeme und Dienstleistungen, wie die Versorgung mit Wasser oder Wärme, ihre Infrastruktur und Logistik sind immer stärker von einer reibungslos funktionierenden Informationstechnik abhängig. Eine Störung, Beeinträchtigung oder gar ein Ausfall durch einen Cyber-Angriff oder IT-Sicherheitsvorfall kann zu nachhaltig wirkenden Versorgungsengpässen, erheblichen Störungen der öffentlichen Sicherheit oder anderen dramatischen Folgen führen.

Auch sonstige Wirtschaftsunternehmen sind aufgrund ihres technologischen Know-hows, durch ihre Auslandsaktivität oder im Rahmen von breit gestreuten Angriffen Ziele für Cyber-Angriffe. Hier sind es vor allem die finanziellen Folgen durch Produktionsausfälle, Beschädigungen des Maschinenparks, Patentdiebstahl oder Cyber-Erpressung, die erhöhte IT-Sicherheitsvorkehrungen notwendig machen.

2.2.1.1 Erkenntnisse aus KRITIS-Meldungen und -Nachweisen

Die Gefährdungslage im Bereich Kritischer Infrastrukturen liegt weiterhin auf hohem Niveau. Es lassen sich für den Berichtszeitraum jedoch keine Gefährdungen erkennen, die sich ausschließlich gegen Kritische Infrastrukturen richten würden.

Cyber-Sicherheit stellt sich asymmetrisch dar: Um eine Kritische Infrastruktur erheblich beeinträchtigen zu können, muss ein Angreifer lediglich eine einzige Schwachstelle erfolgreich ausnutzen. Betreiber Kritischer Infrastrukturen müssen hingegen einen ganzheitlichen Schutz gewährleisten, um sich umfassend abzusichern.

Die IT-Sicherheit Kritischer Infrastrukturen lässt sich durch technische Maßnahmen alleine nicht im Sinne eines umfassenden Schutzes sicherstellen. Vielmehr bedarf es einer Betrachtung der Faktoren Technik – Organisation – Mensch.

Im Bereich der Technik verdeutlichten Meldungen der KRITIS-Betreiber, dass Ausfälle im Bereich der Hard- und Software, insbesondere nach Updates und Patches von relevanter IT-Infrastruktur, Beeinträchtigungen und Ausfälle der kritischen Dienstleistungen verursachten. Die am intensivsten betroffenen Branchen waren hierbei diejenigen, deren Kritische Infrastrukturen eher im Bereich der IT zu finden sind als im Bereich der Operational Technology. Beispielhaft sind hier Gesundheits-, Finanz- und Versicherungswesen zu nennen.

KRITIS-Betreiber erbringen Nachweise darüber, angemessene Vorkehrungen zur Vermeidung von Störungen getroffen zu haben. Die Sichtung der beim BSI eingegangenen Nachweise hat gezeigt, dass die Umsetzung des IT-Sicherheitsgesetzes und die damit einhergehende Verpflichtung, IT-Sicherheit nach Stand der Technik nicht nur umzusetzen, sondern die Umsetzung auch gegenüber Dritten nachzuweisen, zu einer Verbesserung der IT-Sicherheit bei den KRITIS-Betreibern geführt hat. So lässt sich beispielsweise erkennen, dass im Rahmen der Nachweis-Erstellung die IT-Sicherheit organisatorisch verbessert wurde, indem das Informationssicherheitsmanagementsystem (ISMS) und die darin hinterlegten Prozesse und Verantwortlichkeiten implementiert bzw. angepasst wurden. In vielen der betrachteten ISMS bei KRITIS-Betreibern wurde als ein Baustein beispielsweise ein internes wie externes Meldewesen für Sicherheitsvorfälle eingeführt. Damit sind KRITIS-Betreiber nicht nur in der Lage, den gesetzlichen Auftrag der Meldepflicht erheblicher IT-Störungen zu erfüllen. Meldestrukturen leisten darüber hinaus einen wesentlichen Beitrag zum Gesamtbild der Cyber-Gefährdungen.

Der Faktor Mensch leistet nach wie vor einen entscheidenden Beitrag zur Erhöhung der Cyber-Sicherheit. Betreiber Kritischer Infrastrukturen berichten von anhaltenden Social-Engineering- und Spear-Phishing-Kampagnen im Verlauf des Berichtszeitraums. Die Spear-Phishing-Mails waren häufig aufwändig erstellt, so dass eine regelmäßige Sensibilisierung von Mitarbeitern in KRITIS-Organisationen erforderlich war und ist. Im Rahmen der Umsetzung



Betrügerische Support-Anrufe

Sachverhalt

Seit mehreren Jahren – wie auch im aktuellen Berichtszeitraum – gibt es Wellen von Angriffen durch Social-Engineering, bei denen sich Kriminelle telefonisch als Support-Mitarbeiter von Microsoft ausgeben. Durch die Mitteilung von vorgetäuschten Fakten (Lizenzprobleme, Schadsoftware-Infektionen etc.) wird versucht, die Angerufenen zu überreden, persönliche Daten preiszugeben oder dem anrufenden Kriminellen einen Zugang zu ihrem Computer zu gewähren. Im typischen Angriffsszenario bieten vermeintliche Support-Mitarbeiter Hilfe an, erhalten zur Problemlösung nicht vorhandener Probleme die Zugangsdaten und installieren dann z. B. eine Fernwartungssoftware oder ein Remote Access Tool. Microsoft meldete für das erste Quartal 2019 einen starken Anstieg von gefälschten Support-Anrufen. Für Kriminelle, die die Kontrolle über den Computer des Angerufenen erlangen, ist der Zugriff auf das Online-Banking des Opfers ein Hauptmotiv. Der erfolgreiche Missbrauch des Online-Bankings durch die Kriminellen wird von Banken und Strafverfolgungsbehörden als weit verbreitetes Massenphänomen von Cyber-Kriminalität mit hohen Opferzahlen bestätigt.

Ursache/Schadenswirkung

Für Angriffe durch Social-Engineering, auch bei gefälschten Support-Anrufen, sind keine besonderen technischen Fähigkeiten der Angreifer erforderlich. Ausgenutzt wird die Schwachstelle Mensch: so zum Beispiel Kooperationsbereitschaft und Unwissen über Sachverhalte und Zusammenhänge in der fortschreitenden Digitalisierung. Aufgrund der hohen Zahl an Vorfällen muss angenommen werden, dass die Kriminellen planvoll und organisiert vorgehen und kriminelle „Call Center“ betreiben. Durch den missbräuchlichen Zugriff auf Online-Banking oder Kreditkartendaten können den Betroffenen erhebliche finanzielle Schäden entstehen. Die Kreditinstitute haben erhöhten Aufwand durch die Aufklärung der Missbrauchsfälle und die Überweisungsrückrufe. Insgesamt wird das Vertrauen in die Digitalisierung beeinträchtigt.

Reaktion

Die betroffenen Bürger sollten im Verdachtsfall die Zugangsdaten zu ihrem Computer ändern und ihr Online-Banking und andere Dienste überprüfen. Bei ungewöhnlichen Zahlungsvorgängen muss das Bankinstitut unmittelbar benachrichtigt und gegebenenfalls Strafanzeige erstattet werden.

Empfehlung

Es wird empfohlen, nicht auf die Anrufe zu reagieren und einfach wieder aufzulegen. Weitere Empfehlungen zum Schutz vor Social Engineering gibt BSI für Bürger: https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/IT_Sicherheit_am_Arbeitsplatz/SoEng/Social_Engineering.html

des IT-Sicherheitsgesetzes berichten KRITIS-Betreiber von etablierten Übungen, um auch im Krisenfall handlungsfähig zu bleiben. Abläufe zur Vorfallsbearbeitung im Krisenfall können so getestet werden, die Meldestelle des BSI wird hierbei regelmäßig einbezogen, Kommunikationswege werden verstetigt.

Versäumnisse des IT-Betriebs und auch der Nutzer haben durch die ausgefeilten Methoden der Angreifer massive Konsequenzen für die Unternehmen. Selbst wenn Backups erstellt wurden, entstehen den Unternehmen Schäden durch den Ausfall der verschiedenen Netze und Systeme, durch die Zeit der Wiederherstellung aus den Backups sowie durch die Datenverluste aufgrund der Zeit zwischen der letzten Sicherung und dem Schadenseintritt. Sollten trotz der regelmäßigen Berichterstattung und Sensibilisierung zum Thema keine Backups verfügbar sein oder diese nicht hinreichend geschützt sein, sodass sie ebenfalls verschlüsselt werden, entstehen hohe bis sehr hohe Schäden.

2.2.1.2 Erkenntnisse aus Meldungen aus der Wirtschaft

Bei den Meldungen aus der Wirtschaft ist das Thema Ransomware weiterhin zentral. Schwachstellen, Fehler und

Energie	Ernährung	Finanzen	Gesundheit	IT+TK	Kerntechnische Anlagen	Transport und Verkehr	Wasser	SUMME
29	5	60	47	59	2	41	9	252

Tabelle 02 Meldungszahlen im Berichtszeitraum 01.06.18 – 31.05.2019

i WIRKUNG DES IT-SIG AUF DIE IT-SICHERHEIT IN DEN KRITISCHEN INFRASTRUKTUREN

Mit dem 2015 verabschiedeten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz, IT-SiG) wurde das BSI-Gesetz (BSiG) dahingehend geändert, dass Betreiber Kritischer Infrastrukturen „angemessene Vorkehrungen zur Vermeidung von Störungen ihrer informationstechnischen Systeme, Komponenten und Prozesse“ nach dem „Stand der Technik“ treffen müssen (§ 8a Abs. 1 BSiG). Die Einhaltung dieser Vorgabe haben die Betreiber gegenüber dem BSI nachzuweisen, sofern sie nicht einer Nachweispflicht einer anderen Behörde gegenüber unterliegen, wie es z. B. für Betreiber von Energieversorgungs- oder Telekommunikationsnetzen der Fall ist (§ 8a Abs. 3 und § 8d Abs. 2 BSiG).

Dem BSI liegen mittlerweile Nachweise zu über 280 Kritischen Infrastrukturen vor. Dabei entfallen

- etwa 150 auf den Sektor Wasser,
- etwa 60 auf den Sektor Energie,
- etwa 35 auf den Sektor Ernährung und
- etwa 30 auf den Sektor IT & Telekommunikation (TK).

Die Sektoren Gesundheit, Transport & Verkehr sowie Finanzen & Versicherungen gehören zum sogenannten „Zweiten Korb“ der BSI-KRITIS-Verordnung. Die Betreiber aus diesen Sektoren müssen Nachweise daher erst später im Jahr 2019 einreichen.

Aus den vorliegenden Nachweisdokumenten und Gesprächen mit Betreibern ist ersichtlich, dass die Betreiber der Kritischen Infrastrukturen sich zwischenzeitlich intensiv mit dem Thema IT-Sicherheit auseinandergesetzt haben. Es bestehen durchaus Unterschiede in der Reife der IT-Sicherheit im Vergleich der Branchen untereinander.

In Branchen mit bisher geringerer IT-Sicherheitsdurchdringung konnte durch die Umsetzung des IT-Sicherheitsgesetzes eine umfassende Anhebung des Sicherheitsniveaus erzielt werden:

- Eine beträchtliche Anzahl an Betreibern führte erstmalig ein ISMS ein, um die Vorgaben von § 8a Abs. 1 BSiG zu erfüllen.
- Teilweise wurden IT-Sicherheitsteams verstärkt und IT-Sicherheitsbeauftragte neu im Unternehmen eingestellt, oder es wurden Mitarbeiter dediziert für diese Aufgabe abgestellt.
- Zusätzlich wurden häufig externe Beratungsdienstleistungen eingekauft, um Prozesse aufzubauen oder zu optimieren, bereits vorhandenes Wissen zu ergänzen und Mitarbeiter entsprechend zu sensibilisieren.
- Teilweise wurde in den KRITIS-Anlagen auch Technik angepasst. So wurden beispielsweise alte Leitsysteme durch neue ersetzt, um die Anlagen tatsächlich nach dem „Stand der Technik“ absichern zu können.
- Generell wird mehr Geld in die IT-Sicherheit investiert, als es noch vor wenigen Jahren der Fall war.

Sowohl Betreiber und ihre IT-Dienstleister als auch die in den Branchen tätigen IT-Sicherheitsberater bauten ihr Wissen und ihre Fähigkeiten aus, um Kritische Infrastrukturen insbesondere im Hinblick auf die Verfügbarkeit der kritischen Dienstleistungen abzusichern.

In den regulierten Branchen konnte das im IT-Sicherheitsgesetz formulierte Ziel einer Erhöhung des IT-Sicherheitsniveaus somit erreicht werden. Gleichzeitig ergab sich innerhalb der Branchen eine Angleichung der IT-Sicherheit auf einem hohen Niveau.

Allein durch die Zeit, die eine (Teil-)Wiederherstellung benötigt, entstehen in Verbindung mit Produktionsausfällen große Verluste. In Einzelfällen können diese für kleinere Unternehmen existenzbedrohend sein.

Das BSI warnte in den vergangenen Monaten vor verschiedenen weiteren Fortentwicklungen der Angriffsmethoden, was vor allem auf Meldungen und Fällen aus der Wirtschaft beruhte.

Durch das gezielte Sammeln von Adress- und E-Mail-Informationen – das sogenannte „Outlook-Harvesting“ – können authentisch aussehende Angriffs-(Spam-) Mails erstellt werden. Dazu liest die Schadsoftware Kontaktbeziehungen und seit Ende 2018 auch E-Mail-Inhalte aus den Postfächern bereits infizierter Systeme aus (siehe Vorfall: Warnung vor Schadsoftware Emotet auf Seite 13). Diese Informationen nutzen die Täter zur weiteren Verbreitung des Schadprogramms in nachfolgenden Spam-Kampagnen, sodass die Empfänger fingierte E-Mails von Absendern erhalten, mit denen sie erst kürzlich in Kontakt standen. Jeder Infizierte wird so zu einer Gefahr für seine Kontakte. Hier sind zukünftig technische Maßnahmen gefragt, um so weit und so aktuell wie möglich Infektionen zu verhindern und, falls diese doch im Einzelfall erfolgreich sind, sicherzustellen, dass die

Kompromittierung eines einzelnen Systems nicht zur Gefährdung des gesamten Netzes führt.

Durch den Einsatz von Techniken, die bislang nur im Umfeld fortschrittlicher APT-Angriffe gesehen wurden, gelingt es aktueller Schadsoftware, sich innerhalb von Unternehmensnetzen auszubreiten (engl. Lateral Movement) und sie vollständig zu infiltrieren. Diese Schadprogramme ermöglichen den Angreifern etwa über das Auslesen von Zugangsdaten und Schwachstellen in verbreiteten Netzwerkprotokollen, sich selbstständig in einem IT-Netz auszubreiten und Remote-Zugriff auf die Systeme zu erlangen. Bei ungünstiger Netzwerkconfiguration ist es dabei zu Ausfällen kompletter Unternehmensnetzwerke gekommen. Die Schadprogramme werden aufgrund ständiger Modifikationen zunächst meist nicht von gängigen Virenschutzprogrammen erkannt und nehmen tiefgreifende Änderungen an infizierten Systemen vor. Bereinigungsversuche bleiben in der Regel erfolglos und bergen die Gefahr, dass Teile der Schadsoftware auf dem System verbleiben. Einmal infizierte Systeme sind daher grundsätzlich als vollständig kompromittiert zu betrachten und müssen neu aufgesetzt werden. In mehreren dem BSI gemeldeten Fällen hatte dies massive Produktionsausfälle zur Folge, da ganze Unternehmensnetzwerke vollständig neu aufgebaut werden mussten.

Zusätzlich haben sich Angreifer z. B. über Fernwartungstools (z. B. RDP, RescueAssist, LogMeIn) auch manuell Zugriff auf vorher automatisiert infizierte Netze verschafft und auf verschiedenen Systemen im IT-Netz der Opfer eine Backdoor installiert. Dann untersuchen und bewerten sie diese Netze auf ihren Wert und spähen ggf. weitere Opfer aus. Die Angreifer versuchen, etwaige Backups zu manipulieren oder zu löschen. Anschließend bringen sie bei vielversprechenden Zielen selektiv und koordiniert Ransomware auf den Computersystemen aus. Durch dieses aufwendige Vorgehen können Angreifer deutlich höhere Lösegeldforderungen an die Unternehmen stellen, als es bei bisherigen rein ungezielten Ransomware-Kampagnen der Fall war. Es sind teilweise sehr hohe Bitcoin-Forderungen gestellt worden. Dabei wurden wiederholt keine pauschalen Forderungen aufgestellt, sondern individuelle Zahlungen ausgehandelt.

Neben einzelnen Unternehmen sind zunehmend auch IT-Dienstleister betroffen, über deren IT-Netz sich die Angreifer Zugang zu deren Kunden verschaffen. In einem Fall wurde bekannt, dass der Angreifer, nachdem seine Ransomware-Erpressung gescheitert war, mit der Androhung der Veröffentlichung zuvor während des Angriffs gestohlener,

vertraulicher Daten einen weiteren Erpressungsversuch startete. Nachdem auch hier keine Lösegeldzahlung zustande kam, wurden die Daten tatsächlich veröffentlicht (siehe Vorfall unten: Erpressung von IT-Dienstleistern und Veröffentlichung abgeflossener Daten).

2.2.1.3 Ergebnisse und Erkenntnisse aus der Cyber-Sicherheitsumfrage der Allianz für Cyber-Sicherheit (ACS)

Schadsoftware war 2018 mit 53 % die häufigste Form von Cyber-Angriffen auf deutsche Unternehmen und Institutionen. In 90 % der Fälle dienten dabei schädliche Anhänge oder Links in E-Mails als Einfallstor. Bei der Hälfte der unterbundenen E-Mail-basierten Angriffe verhinderten technische Maßnahmen eine Infektion, in den übrigen Fällen war die vorausgegangene Sensibilisierung und Schulung der Beschäftigten der Erfolgsfaktor.

Das geht aus der jüngsten Cyber-Sicherheitsumfrage hervor, die das BSI im Rahmen der Allianz für Cyber-Sicherheit durchgeführt hat. An der Umfrage nahmen 1.039 Unternehmen und andere Institutionen teil.



Erpressung von IT-Dienstleistern und Veröffentlichung abgeflossener Daten

Sachverhalt

Ein deutscher IT-Dienstleister wurde im zweiten Quartal 2019 Opfer eines Cyber-Angriffs. Den Tätern gelang es zunächst, Firmeninterna sowie Kundendaten zu exfiltrieren und im Anschluss Daten zentraler IT-Systeme zu verschlüsseln. Der IT-Dienstleister kam der sechsstelligen Lösegeldforderung nicht nach, um die kriminellen Machenschaften nicht zu fördern. Daraufhin haben die Täter die Drohung wahr gemacht und die Daten über einen Webserver veröffentlicht.

Ursache/Schadenswirkung

IT-Sicherheitsvorfälle können einen hohen Reputationsschaden auslösen, der rasch, z. B. durch Auftragsrückgänge oder Schadensersatzforderungen von Kunden, zu einem immensen finanziellen Schaden führen kann. Bemerkenswert ist das als neu zu bewertende Vorgehen der Täter. Bisher wurden Opfer im Rahmen von Ransomware-Angriffen mit Lösegeldforderungen erpresst, um die Daten wieder entschlüsselt zu bekommen. Falls nicht gezahlt wird, kommt es zu einem Datenverlust, der durch Backups rückgängig gemacht werden kann. Durch die Veröffentlichung von zuvor ausgespähten Daten können die Täter weiteren Druck auf die Opfer ausüben, selbst wenn diese über Backups verfügen.

Reaktion

Der IT-Dienstleister hat unmittelbar die Strafverfolgung über das zuständige Landeskriminalamt in diesem schwerwiegenden Fall eingeschaltet. Des Weiteren erfolgte aufgrund der Betroffenheit von personenbezogenen Daten wie Namen, Telefonnummern und E-Mail-Adressen beim zuständigen Landesdatenschutzbeauftragten eine Vorfallsmeldung gemäß Datenschutzgrundverordnung (DSGVO) sowie eine Information der Kunden. Die polizeilichen Ermittlungen werden vom zuständigen Landeskriminalamt durchgeführt. Der Vorfall wurde im Nationalen Cyber-Abwehrzentrum eingebracht. Die betroffenen Betreiber Kritischer Infrastrukturen wurden über die Information des IT-Dienstleisters hinaus durch das BSI informiert und um Risikobewertung bezüglich der abgeflossenen Daten gebeten. Es gingen diesbezüglich keine Störungsmeldungen im BSI ein.

Empfehlung

Im konkreten Fall ließ sich das Einfallstor nicht mehr eindeutig ermitteln. Um solche IT-Sicherheitsvorfälle zu verhindern, sollte das Leitmotiv der Schutzmaßnahmen sein, dass eine nicht immer zu verhindernde Kompromittierung eines einzelnen Systems nicht zur Übernahme des gesamten Netzes führen darf. Um dies zu gewährleisten, muss eine Kombination aus Detektions- und Präventionsmaßnahmen umgesetzt werden. Dazu gehört zum Beispiel auf der Detektionsseite die Nutzung eines Antivirenprogramms mit signatur- und verhaltensbasierten Detektionsmechanismen, die Schadcode-Prüfung eingehender E-Mails sowie zentrale netz-/host-basierte Intrusion-Detection-Systeme mit aktuellen Signaturen und ausreichend Personalressourcen zur Auswertung. Aufseiten der Präventionsmaßnahmen ist die Absicherung von Fernwartungszugängen und über das Internet zugänglichen Diensten (bei letzteren z. B. mithilfe einer Zwei-Faktor-Authentifizierung für Webanwendungen), die Netzsegmentierung zumindest für Büro-Systeme, Server und zentrale Verzeichnisdienste wie das Active Directory auch auf administrativer Ebene, die Verwendung minimaler Benutzerrechte und die Umsetzung eines Whitelisting-Ansatzes für Anwendungen (auf Windows-Systemen etwa mithilfe von Microsoft AppLocker) und die Browser-Nutzung in einer isolierten Umgebung zu nennen. Auf den Webseiten des BSI finden Sie bei der Allianz für Cyber-Sicherheit (<https://www.allianz-fuer-cybersicherheit.de/>) sowie im IT-Grundschutz-Kompendium (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html) entsprechende Hinweise.

Die Cyber-Sicherheits-Umfrage für den Betrachtungszeitraum 2018 wurde als Online-Erhebung vom 21.02.2019 bis 07.03.2019 realisiert. Die Einladung zur Teilnahme erfolgte über die Kommunikationskanäle des BSI. In der Stichprobe ist die IT-Branche der am stärksten vertretene Wirtschaftszweig. Gut drei Viertel der Befragten waren IT-Sicherheitsverantwortliche in ihren Institutionen.

Insgesamt war im Jahr 2018 jeder dritte an der Umfrage teilnehmende Betrieb (33 %) von Cyber-Sicherheitsvorfällen betroffen, Großunternehmen hat es häufiger getroffen als kleine und mittelständische Unternehmen (43 bzw. 26 %). Rund 87 % der von Cyber-Sicherheitsvorfällen Betroffenen gaben an, dass es in der Folge zu Betriebsstörungen oder -ausfällen kam. Hinzu kamen häufig Kosten für die Aufklärung der Vorfälle und die Wiederherstellung der IT-Systeme (bei 65 % der Betroffenen) sowie Reputationsschäden (22 %).

Viele Unternehmen haben bereits geeignete Schutzmaßnahmen umgesetzt. Beispielsweise gaben insgesamt 71 % der befragten Institutionen an, 2018 über ein strukturiertes Patch-Management zu verfügen, um auf bekannt gewordene Sicherheitslücken schnell reagieren zu können. Rund 53 % der befragten Unternehmen setzten 2018 ein zentrales Management für die Sicherheit mobiler Endgeräte ein. Während rund 72 % der großen Unternehmen über ein solches System verfügten, waren es bei den kleinen und mittelständischen Unternehmen nur 39 %.

Oftmals fehlt es jedoch an einem Managementsystem für Informationssicherheit (ISMS): Nur 47 % der Befragten gaben an, einen ganzheitlichen Ansatz der Cyber-Sicherheit zu verfolgen. Von den großen Unternehmen betrieben 61 % ein solches System, bei den kleinen und mittelständischen Unternehmen waren es nur 37 %.

Ein gutes Drittel der Befragten gab an, Log-Daten und Protokolle grundsätzlich und systematisch auf Indizien für Cyber-Sicherheits-Vorfälle zu untersuchen. Auch Notfallmanagement und regelmäßige Übungen sind nicht überall Standard: Im Jahr 2018 lag der Anteil der Befragten, die ein Notfallmanagement betreiben, um bei einem Cyber-Vorfall schnell handlungsfähig zu sein, bei 43 %. Mit 49 % war der Anteil der Betreiber eines solchen Systems unter den großen Unternehmen deutlich höher als unter den kleinen und mittelständischen Unternehmen mit 38 %.

Die Ergebnisse der Cyber-Sicherheitsumfrage belegen, dass Cyber-Angriffe eine ernst zu nehmende Bedrohung für den Erfolg von Unternehmen darstellen und beträchtliche wirtschaftliche Schäden verursachen können. Nach Angaben der an der Umfrage teilnehmenden Unternehmen und Institutionen wurden 2018 bereits vielfältige Schutzmaßnahmen umgesetzt. Dabei muss die Mitarbeiter-Awareness genauso wichtig genommen werden wie die Umsetzung technischer Maßnahmen. Durch die Bereitstellung geeigneter Informationen und praktischer Empfehlungen arbeitet das BSI, beispielsweise im Rahmen der Allianz für Cyber-Sicherheit, weiterhin daran, Unternehmen beim Ausbau ihrer Schutzmaßnahmen gegen Cyber-Gefährdungen zu unterstützen.

2.2.2 Lösungen und Angebote des BSI für die Wirtschaft und Kritische Infrastrukturen (KRITIS)

Im folgenden Kapitel sind die Lösungen und Angebote des BSI für die Zielgruppe Wirtschaft zusammengefasst. Hier finden sich neben Informationen zu den renommierten

und bekannten BSI-Angeboten Zertifizierung, IT-Grundschutz, Allianz für Cybersicherheit (ACS) und UP KRITIS auch eine Zusammenfassung der Digitalisierungsprojekte in Deutschland sowie die Entwicklungen im Bereich Moderne Telekommunikationsinfrastrukturen (5G). Es wird deutlich, dass das BSI bereits in vielfältiger Weise Impulse gesetzt hat, um seinen Auftrag gegenüber der Wirtschaft zu erfüllen.

2.2.2.1 Zertifizierung

Das BSI bietet im Rahmen seiner Dienstleistungen verschiedene Zertifizierungsverfahren an. Zu den etablierten Verfahren im Bereich der Produktzertifizierung zählt die Zertifizierung nach Common Criteria (ISO/IEC 15408). Ferner können Produkte auch nach Technischen Richtlinien des BSI zertifiziert werden. Im Bereich der Managementsysteme erlaubt der ebenfalls seit Jahren praktizierte Grundschutz-Standard die Zertifizierung eines Informationssicherheitsmanagementsystems (ISMS). Diese Verfahren werden in den folgenden Abschnitten detaillierter betrachtet.

Zertifizierung nach Common Criteria (ISO/IEC 15408)

Die Zertifizierung der IT-Sicherheit eines Produktes durch das BSI heißt: Es wurde auf Basis öffentlicher Prüfkriterien und in einem transparenten Prozess von einer unabhängigen Partei geprüft (<https://www.bsi.bund.de/zertifizierung>).

Beschaffer entnehmen einem Zertifikat des BSI:

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

Die Prüfkriterien Common Criteria (CC), die seinerzeit von den am internationalen Abkommen Common Criteria Recognition Agreement (CCRA, <https://www.commoncriteriaportal.org>) beteiligten Nationen erstellt und gepflegt wurden, wurden nunmehr von der Internationalen Standardisierungsorganisation ISO übernommen. Derzeit wird der Standard aktualisiert und erweitert. Das BSI beteiligt sich zusammen mit Experten aus Prüfstellen und der Industrie aktiv über das Deutsche Institut für Normung (DIN) an diesem Programm. 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 Forderung nach zertifizierten Produkten wurde in den letzten Jahren auch in zahlreichen Gesetzen und Verordnungen verankert. Vielfach betrifft dies die Digitalisierungsprojekte der Bundesregierung z. B. in den Bereichen eHealth, Hoheitliche Dokumente und Smart Metering und seit vielen Jahren auch die Digitale Signatur. Seit Mitte 2016 gilt in der EU die gegenüber der früheren EU-Richtlinie erweiterte Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen (eIDAS-Verordnung (EU) Nr. 910/2014). Darin wird u. a. die notwendige Zertifizierung für IT-Produkte zur Erzeugung von Digitalen Signaturen geregelt. Gemäß dem nationalen Vertrauensdienste-Gesetz ist das BSI die öffentliche Stelle, die die Konformität von Signaturerstellungseinheiten mit den Anforderungen der Verordnung bestätigt. Diesbezüglich erteilte Zertifikate werden bei der EU-Kommission notifiziert.

Das Abkommen zur Anerkennung von IT-Sicherheitszertifikaten in Europa (Mutual Recognition Agreement - MRA) wird nunmehr von 17 Nationen aktiv unterstützt: die Slowakei und Belgien sind dazugekommen (<https://www.sogis.org>). Die in der Senior Official Group Information Systems Security (SOGIS) organisierten Mitgliedsnationen bilden einen starken Verbund, um einen von öffentlichen Stellen unterstützten Vertrauenswürdigkeitsnachweis für IT-Sicherheitsprodukte zu fördern.

Die EU-Kommission hat sich im Rahmen der Förderung der Cyber-Sicherheit in Europa des Themas Zertifizierung angenommen. Das Gesetzespaket zur Cyber-Sicherheit (Cybersecurity Act), in dem auch ein EU-weites Zertifizierungsmodell verankert werden soll, wurde auf EU-Ebene abgestimmt. Die EU-Mitgliedstaaten haben mit SOGIS-MRA bereits ein starkes, eingespieltes Zertifizierungskonzept in Betrieb, das unter dem neuen EU-Dach verankert wird.

Die Durchführung der Produkt-Zertifizierung wird durch neue Schutzprofile (Protection Profiles, PP) unterstützt. Sie beschreiben einen Standard an Sicherheitsanforderungen für einen bestimmten Produkttyp. Beispiele für neue Schutzprofile, die in Produktzertifizierungen angewendet werden, sind:

- PP für eine „Security Module Application for Electronic Record-keeping Systems (SMAERS)“ z. B. für elektronische Kassensysteme,
- PP Cryptographic Service Provider (CSP), das Anforderungen an Kryptografie in einer technischen Plattform beschreibt.

Produktzertifizierungen unter Anwendung dieser neuen Schutzprofile sind bereits beantragt und in Bearbeitung.

Hersteller lagern die Prüfung der Sicherheit von Entwicklungs- und Produktionsstandorten verstärkt aus dem Produktzertifizierungsverfahren in eine separate Standortzertifizierung aus. Damit wird der Prozess der Produktzertifizierung verschlankt und effizienter gestaltet.

Zertifizierung nach Technischen Richtlinien

Funktionalität und Interoperabilität als Produkteigenschaft werden im Rahmen der Technischen Richtlinien (TR) des BSI durch funktionale Anforderungen als Standard beschrieben und können danach implementiert werden. Die Konformität eines IT-Produktes oder -Systems zu 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 TR durch die Deutsche Akkreditierungsstelle (DAkkS) akkreditiert.

Zertifizierung eines ISMS nach BSI-Grundschatz

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-Grundschatzes durchgeführt wird. Die IT-Grundschatz-Vorgehensweise und die im IT-Grundschatz enthaltenen Empfehlungen von Standard-Sicherheitsmaßnahmen stellen inzwischen einen De-Facto-Standard für IT-Sicherheit dar.

Sonstige Zertifizierungen

Das BSI ist Akkreditierungs- und Aufsichtsstelle für die De-Mail-Provider, die in Deutschland mit ihren De-Mail-Diensten eine Infrastruktur für eine rechtssichere elektronische Kommunikation anbieten. Seit 2012 sind folgende akkreditierte Provider im Markt tätig: Mentana-Claimssoft GmbH, Telekom Deutschland GmbH, T-Systems International GmbH und 1&1-Mail GmbH.

Europäische Bürgerinitiativen (EBI) müssen eine Million Unterstützungsbekundungen gesammelt und die Mindestwerte in mindestens sieben Mitgliedstaaten erreicht haben, damit die Europäische Kommission entscheidet, ob sie tätig wird. Um über das Internet Unterstützungsbekundungen zu sammeln, müssen Organisatoren auf ihrer Internetpräsenz ein Online-Sammelsystem zur Verfügung stellen, das die in der Durchführungsverordnung (EU) Nr. 1179/2011 genannten technischen Spezifikationen erfüllt.

Anschließend müssen sie ihr System von der jeweils zuständigen Behörde zertifizieren lassen. Das BSI ist die national zuständige Behörde für die Erteilung von Bescheinigungen über die Übereinstimmung von Online-Sammelsystemen mit der EBI-VO (VO (EU) Nr. 211/2011).

2.2.2.1.1 Fortentwicklung der Prüfstandards

Die vom BSI entwickelten Prüfstandards in Form von Technischen Richtlinien beschreiben üblicherweise technische Produkte – konkret IT-Produkte, die heutzutage kurzen Innovationszyklen unterliegen. Hersteller und Verkäufer solcher Produkte sind, den Gesetzen der Marktwirtschaft folgend, dauerhaft bestrebt, neue Produkte zu entwickeln bzw. bestehende Produkte weiterzuentwickeln, um den Verbrauchern neue Kaufanreize zu bieten.

Das bedeutet aber auch, dass bestehende Standards, die solche IT-Produkte beschreiben, ständig weiterentwickelt werden müssen, um die geänderten oder neuen Funktionalitäten der IT-Produkte zu berücksichtigen. Dabei ist neben dem eigentlichen Standard, der die Funktionalität des IT-Produkts in Form von Anforderungen definiert, auch der Prüfstandard weiterzuentwickeln. Schließlich sind bestehende Testfälle im Prüfstandard auf die geänderte Funktionalität anzupassen und zu ergänzen, oder es sind neue Testfälle zu beschreiben.

Erst wenn ein neuer Prüfstandard veröffentlicht wurde, kann dieser als Basis für neue Zertifizierungen herangezogen werden. Hierbei ist zu bedenken, dass ggf. auch die Prüfstellen, die im Rahmen der Zertifizierung nach Technischen Richtlinien die IT-Produkte prüfen, entsprechend weiter qualifiziert werden müssen, um die geänderten oder neuen Funktionalitäten in den IT-Produkten prüfen zu können.

2.2.2.1.2 Zertifizierung in Zahlen

Im Rahmen der CC-Zertifizierung beim BSI wurden im Berichtszeitraum insgesamt 119 Zertifikate in den neun Produktbereichen Betriebssysteme, Digitale Signatur, Digitaler Tachograph, Gesundheitswesen, Hoheitliche Dokumente, Intelligente Messsysteme, Netzwerk- und Kommunikationsprodukte, Serveranwendungen und Smartcards ausgestellt, wobei neben Erstzertifizierungen auch Folgezertifizierungen nach Produktanpassungen vorgenommen wurden.

Außerdem wurden 55 Zertifikate nach Technischen Richtlinien aus 15 Prüfbereichen erteilt, wobei 33 Erst- und Re-Zertifizierungen und 22 Maintenance-Verfahren durchgeführt wurden.

Im Bereich des IT-Grundschutz konnten im Berichtszeitraum insgesamt 37 „ISO 27001 Zertifikate auf Basis von IT-Grundschutz“ ausgestellt werden und es wurden darüber hinaus 74 Überwachungsaudits durchgeführt.

Ferner wurden drei Bescheinigungen für Online-Sammelsysteme erteilt.

2.2.2.1.3 Zertifizierung im europäischen und internationalen Umfeld

Das BSI genießt international im Bereich der Common Criteria eine hohe Reputation. Grundlage hierfür ist das fachliche Engagement des BSI in technischen Arbeitsgruppen der zwei Abkommen zur Anerkennung von IT-Sicherheitszertifikaten SOGIS-MRA und Common Criteria Recognition Arrangement (CCRA). In den Arbeitsgruppen bringt das BSI sein Fachwissen zu Themen wie Kryptografie, Sicherheit von Embedded Devices und Chip-Sicherheit ein. Darüber hinaus unterstützt das BSI das Common Criteria Users Forum (CCUF), ein Zusammenschluss von Common Criteria-Anwendern, mit seiner Expertise in den Bereichen Kryptografie, Betriebssysteme, Datenbanken und verschlüsselte USB-Sticks. Die Ergebnisse der Arbeit aus den internationalen Arbeitsgruppen lässt das BSI in die Standardisierung einfließen.

Neben der Arbeit in den multilateralen Abkommen CCRA und SOGIS-MRA bereitet das BSI zurzeit bilateral mit Frankreich die Anerkennung von Zertifikaten vor, die auf der Basis eines Penetrationstests ausgestellt werden. Ziel ist es, neben der gegenseitigen Anerkennung von CSPN-Zertifikaten (Certification de Sécurité de Premier Niveau) der französischen ANSSI und Zertifikaten der „Beschleunigten Sicherheitszertifizierung“ (BSZ) des BSI weitere europäische Zertifizierungsstellen zu gewinnen und als Zertifizierungsschema in den neuen europäischen Zertifizierungsrahmen zu überführen.

2.2.2.1.4 Internationale Gremienarbeit

Durch den Rechtsakt zur Cyber-Sicherheit (EU Cybersecurity Act) wird ein EU-weit geltender europäischer Zertifizierungsrahmen für die Cyber-Sicherheit von Produkten, Verfahren und Diensten geschaffen. Das BSI hat in enger Zusammenarbeit mit dem Bundesministerium des Innern, für Bau und Heimat (BMI) seine Expertise im Bereich der IT-Sicherheitszertifizierung in das Legislativvorhaben der Europäischen Kommission eingebracht. Diese Grundlagenarbeit ist Voraussetzung, um als BSI künftig weiterhin IT-Sicherheit durch Standardisierung und Zertifizierung aus Deutschland heraus zu gestalten. Aktuell trifft das BSI alle notwendigen Vorbereitungen, um das SOGIS-Abkommen (Senior Officials Group on Information Security) als

erstes Zertifizierungsschema in den neuen europäischen Zertifizierungsrahmen zu migrieren.

Neben den Aktivitäten rund um den Cybersecurity Act ist die Fortschreibung der Common Criteria in der International Organization for Standardization (ISO/IEC 15408) stark von der Beteiligung des BSI geprägt.

2.2.2.2 Digitalisierungsprojekte in Deutschland

Das BSI ist neutrales und unabhängiges Kompetenzzentrum für die IT-Sicherheit aller Ressorts und nimmt daher eine Querschnittsfunktion für die Digitalisierungsprojekte der Ressorts wahr. Beispiele für die Unterstützung der Ressorts sind: die IT-Sicherheitsberatung (alle Ressorts), die elektronische Gesundheitskarte (BMG), das Smart Meter (BMWi) sowie das Autonome Fahren (BMVI). Die Zusammenarbeit des BSI mit anderen Ressorts in Fragen der IT-Sicherheit ist für die Gestaltung der Informationssicherheit in der Digitalisierung elementar.

2.2.2.2.1 Zertifizierung Smart-Meter-Gateway

Am 20. Dezember 2018 hat das BSI das erste Zertifikat auf Basis des Schutzprofils für das Smart-Meter-Gateway im Bundesministerium für Wirtschaft und Energie übergeben. Das Produkt war von der Power Plus Communications gemeinsam mit der OpenLimit Sign-Cubes entwickelt worden. Neben dem Nachweis der Einhaltung der Sicherheitsvorgaben wurden im Zertifizierungsverfahren die Herstellungs- und Entwicklungsprozesse des Herstellers sowie die Auslieferungswege der Geräte betrachtet.

Das Smart-Meter-Gateway ist die Schlüsseltechnologie für die Digitalisierung der Energiewende und garantiert Datenschutz und Datensicherheit auf höchstem Niveau. Es versorgt die Akteure – vom Netzbetreiber über den Stromlieferanten bis zum Verbraucher – mit Informationen zu Erzeugung und Verbrauch.

Mit Hilfe des Smart Meterings können in Zukunft die Stromnetze, abhängig von Wind und Sonne, genauso intelligent gesteuert werden, wie Licht und Heizung in Gebäuden. Das Smart-Meter-Gateway legt somit den Grundstein für das intelligente und sichere Netz von morgen. Der sogenannte „verpflichtende Rollout“ beginnt, wenn mindestens drei voneinander unabhängige Unternehmen intelligente Messsysteme am Markt anbieten, die erfolgreich das Zertifizierungsverfahren durchlaufen haben und den gesetzlichen Anforderungen entsprechen.

2.2.2.2.2 Energiewende

Das BSI hat am 31. Januar 2019 die erste Marktanalyse nach dem Messstellenbetriebsgesetz (MsbG) veröffentlicht. In der Marktanalyse nach § 30 MsbG wird der Stand der Umsetzung der BSI-Standards sowie der eichrechtlichen Anforderungen über die Wertschöpfungskette Messeinrichtung, Smart-Meter-Gateway, Gateway-Administrator und Backendsysteme im Markt erfasst. Die für den sicheren Betrieb intelligenter Messsysteme notwendige Infrastruktur (Smart-Meter-Gateway-Administratoren und Smart-Metering-Public-Key-Infrastruktur) steht vollständig zur Verfügung. Da bislang nur ein Smart-Meter-Gateway zertifiziert wurde, kann das BSI die technische Möglichkeit für den Rollout mit Einbaupflicht noch nicht feststellen.

Zugleich müssen die technischen Mindeststandards für Smart-Meter-Gateways kontinuierlich fortentwickelt werden. Um den wachsenden Anforderungen von Energiewende und Cyber-Sicherheit gerecht zu werden, haben das Bundesministerium für Wirtschaft und Energie und das BSI gemeinsam am 29. Januar 2019 die „Standardisierungsstrategie zur sektorübergreifenden Digitalisierung nach dem Gesetz zur Digitalisierung der Energiewende“ veröffentlicht. Diese Roadmap ist der maßgebliche Arbeitsplan für die Fortentwicklung des Smart-Meter-Gateways hin zu der Kommunikationsplattform für die Energiewende. Gleichzeitig unterstützt die Roadmap die Stakeholder bei der Umsetzung der gesetzlichen Vorgaben und enthält Arbeits- und Zeitpläne, welche stetig im Dialog mit den betroffenen Branchen und Behörden weiterentwickelt werden.

2.2.2.2.3 IT-Sicherheit in kooperativen intelligenten Transportsystemen (C-ITS)

Die Europäische Kommission hat Anfang 2019 einen Entwurf für einen delegierten Rechtsakt zu kooperativen intelligenten Transportsystemen (C-ITS) vorgelegt. Damit soll die Grundlage für die Einführung von Diensten gelegt werden, die auf Fahrzeug-zu-Fahrzeug- und Fahrzeug-zu-Infrastruktur-Kommunikation basieren. Einen besonderen Schwerpunkt des vorgesehenen Regelwerks bildet die Sicherheit dieser Kommunikation. Der delegierte Rechtsakt beinhaltet ausführliche Regelungen zur Etablierung einer europäischen Public-Key-Infrastruktur (PKI) für intelligente Verkehrsdienste. Darüber hinaus ist eine Zertifizierung der dabei verwendeten Komponenten in den Fahrzeugen und in der Verkehrsinfrastruktur nach Common Criteria vorgesehen.

Das BSI hat im Vorfeld das BMVI in dieser Angelegenheit beraten und war in die Konsultationen zum delegierten Rechtsakt eingebunden.

2.2.2.2.4 Elektronische Identität (eID): Europaweite Anerkennung der Online-Ausweisfunktion

Für die Umsetzung der Digitalisierung ist die sichere Identifizierung von Personen und Dingen von entscheidender Bedeutung. Daher wurden bereits 2014 mit 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 intensiver 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 überhaupt erfolgreich abgeschlossen. Mit dem Ablauf einer Übergangsfrist von einem Jahr seit der Veröffentlichung der Notifizierung auf dem höchsten Vertrauensniveau gemäß eIDAS-Verordnung im Amtsblatt der EU trat im September 2019 die gegenseitige Anerkennungspflicht in Kraft. Seitdem sind alle EU/EWR-Mitgliedstaaten verpflichtet, die Online-Ausweisfunktion für Anwendungen des öffentlichen Sektors, d.h. insbesondere im E-Government, anzuerkennen.

Infolgedessen haben bis Mai 2019 mit technischer Unterstützung durch das BSI bereits 14 Staaten (Belgien, Dänemark, Estland, Finnland, Griechenland, Großbritannien, Luxemburg, Malta, Niederlande, Österreich, 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 etwa der Hälfte der EWR-Staaten zu verwenden. Weitere elf Staaten (Stand April 2019) befinden sich im Testbetrieb, sodass ein weiteres Wachstum der Abdeckung zu erwarten ist.

Aber auch andere Länder zeigen Bestrebungen, ihre eID-Schemata zu notifizieren. So haben 2018 nach Deutschland schon insgesamt acht weitere Mitgliedstaaten (Belgien, Estland, Großbritannien, Italien, Kroatien, Luxemburg, Portugal, Spanien) ein Notifizierungsverfahren abgeschlossen. Weitere Verfahren laufen derzeit oder sind fast abgeschlossen. Das BSI wirkt an diesen Notifizierungsverfahren aktiv mit seiner Fachkenntnis mit.

Die eID-Schemata der verschiedenen Länder unterscheiden sich teils sehr stark. Die meisten der begutachteten eID-Systeme nutzen tatsächlich die nationalen, auf Chipkarten basierten Ausweisdokumente. Es gibt darüber hinaus aber auch bereits ein eID-Schema, das auf der

Verwendung von zertifizierten SIM-Karten basiert. Ein weiterer Ansatz stützt sich sogar auf die Nutzung von mehreren sogenannten Identitäts Providern, die teilweise privatwirtschaftlich agieren und gleichzeitig mehrere Identifizierungsmittel (App-TAN, SMS-TAN etc.) anbieten können.

Diese unterschiedlichen Ansätze führen natürlich auch zu verschiedenen 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 Nutzung von VideoIdent oder SMS-TAN zurückgreifen, bisher nur einem mittleren Vertrauensniveau zugeordnet.

Auch bzgl. der Anerkennung der anderen notifizierten elektronischen Identitäten im deutschen E-Government sind die Vorbereitungen mit Unterstützung des BSI weit fortgeschritten. Deutschland ist daher auch für die Anerkennungsverpflichtung nach eIDAS zum September 2019 gut vorbereitet.

2.2.2.2.5 eHealth/elektronische Gesundheitskarte

Das Beispiel der elektronischen Gesundheitskarte (eGK) in Verbindung mit dem Ausbau der Telematikinfrastruktur (TI) zeigt, wie fortschreitende Digitalisierung und zunehmende Vernetzung von Leistungsträgern im Gesundheitswesen zielgerichtet zur Steigerung der Effizienz der Versorgung und Erhöhung der Sicherheit der Patienten beitragen kann. Ein Fokus liegt hier derzeit auf der Entwicklung und dem kommenden Einsatz von neuen Anwendungen wie zum Beispiel das Notfalldatenmanagement (NFDm), dem eMedikationsplan im Zusammenhang mit der Arzneimitteltherapiesicherheit (AMTS) und der elektronischen Patientenakte (ePA). Die Grundsteine hierfür wurden gelegt.

Auf Basis von Spezifikationen der Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH (gematik) hat das BSI entsprechende Technische Richtlinien verfasst (TR 03154, TR 03155, TR 03157). Sie sollen dabei helfen, die u. a. in Arztpraxen und Krankenhäusern im Einsatz befindlichen, mit den bisherigen Basisfunktionen ausgestatteten und vom BSI zertifizierten Konnektoren zur Anbindung an die TI sicher um die neuen Funktionen zu erweitern. So können zukünftig Daten für den medizinischen Notfall und eMedikationspläne in Verbindung mit der eGK sicher gespeichert und im Einsatzfall bereitgestellt werden. Im Fall des eMedikationsplans können so auf Wunsch des Patienten bei neu zu verschreibenden Medikamenten durch den behandelnden Arzt Wechselwirkungen mit bereits

bestehenden Medikationen abgeglichen und dadurch mögliche Risiken minimiert werden.

In einem weiteren Schritt steht Mitgliedern einer gesetzlichen Krankenkasse zusätzlich zu den bisherigen Funktionen in Verbindung mit Ihrer eGK auch eine elektronische Patientenakte zur Verfügung. Gemäß dem am 14. März 2019 vom Bundestag beschlossenen Terminservice- und Versorgungsgesetz (TSVG) sind die gesetzlichen Krankenkassen verpflichtet, bis spätestens 2021 ihren Versicherten solche elektronischen Patientenakten anzubieten. Behandelnde Ärzte oder Krankenhäuser können, nach Einverständnis und Freigabe des Versicherten, auf die jeweilige Akte sicher zugreifen, um entsprechende medizinische Daten des Patienten einzustellen oder einzusehen. Voraussetzung ist ein um ein entsprechendes Fachmodul erweiterter und vom BSI zertifizierter Konnektor.

So können auch praxisübergreifende medizinische Behandlungen aufeinander abgestimmt werden und für den Patienten u. U. belastende Mehrfachuntersuchungen vermieden werden. Der Zugriff durch die Versicherten auf ihre individuelle Akte soll hierbei mittels eigener Geräte (PC, auch mobil mittels Smartphone oder Tablet) und einer vom BSI zertifizierten und von der gematik zugelassenen Software ermöglicht werden.

2.2.2.2.6 Zwei-Faktor-Authentisierung

In vielen Bereichen elektronischer Geschäftsprozesse – vom Online-Shopping bis zum Homebanking – ist eine sichere Authentisierung nötig. Bisher wird dafür in vielen Bereichen eine Ein-Faktor-Authentisierung benutzt, die üblicherweise allein auf den Faktor Wissen in Form eines Passworts setzt. Dies hat mehrere Nachteile:

- Zum einen reicht der Besitz dieses einen Faktors, um den Authentisierungsmechanismus zu brechen.
- Zum anderen ist es für Nutzer äußerst aufwändig, für jeden Dienst ein sicheres und individuelles Passwort anzulegen und auswendig zu lernen.

Passwörter sind weiterhin das mit Abstand am meisten verwendete Authentisierungsmittel im Internet, obwohl sie in vielen Fällen kein ausreichendes Sicherheitsniveau bieten. Häufig wird das gleiche, leicht zu merkende Passwort bei vielen verschiedenen Diensteanbietern eingesetzt. Diese Vereinfachung erleichtert jedoch nicht nur dem berechtigten Nutzer den Zugriff auf den Dienst. Hat ein Angreifer Passwörter bei einem Diensteanbieter ausgespäht, kann er dann die erbeuteten Daten auch bei anderen Diensteanbietern zum unberechtigten Zugriff nutzen.

Eine sichere Zwei-Faktor-Authentisierung schafft hier Abhilfe. Dabei werden zwei Faktoren für die Authentisierung verwendet statt nur einem. Diese müssen unterschiedlichen Kategorien (Besitz, Wissen, Biometrie) angehören. Durch die Kombination der Stärken der einzelnen Faktoren wird der Angriff um ein Vielfaches erschwert. Dabei sollten biometrische Merkmale nicht beim Diensteanbieter gespeichert, sondern lokal zur Freischaltung z. B. des Mobiltelefons als Besitzfaktor verwendet werden, welches sich dann gegenüber dem Diensteanbieter durch kryptographische Methoden authentisiert.

Sichere Zwei-Faktor-Authentisierungslösungen sind weiterhin wenig verbreitet. Die Fast-Identity-Online-Allianz (FIDO) wurde 2013 mit vielen verschiedenen Stakeholdern offiziell 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 Authentikators 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 W3C und verschiedenen Client-to-Authenticator Protokollen (CTAP), über welche der Webbrowser mit den FIDO-Token kommuniziert.

Ein Nachweis über die Sicherheit des verwendeten FIDO-Authentikators ist notwendig, um eine sichere Umsetzung der Protokolle in Produkte zu gewährleisten. Als Mitglied der FIDO-Allianz ist das BSI an der Definition nachweisbar sicherer Authentikatoren beteiligt. Der Nachweis eines hohen Sicherheitsniveaus kann durch eine Zertifizierung nach Common Criteria erbracht werden. Das BSI hat hierzu ein Schutzprofil mit hoher Prüftiefe für sichere FIDO-U2F-Token veröffentlicht, nachdem ein durch das BSI entwickelter FIDO-U2F-Token erfolgreich evaluiert wurde. Derzeit erstellt das BSI ein modulares Schutzprofil, welches alle Varianten und Implementierungsoptionen von FIDO-Authentikatoren beinhaltet, so dass diese nach einem einheitlichen Schutzprofil zertifiziert werden können.

2.2.2.2.7 Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme

Im Zuge der Digitalisierung werden Geschäftsvorfälle heutzutage immer häufiger elektronisch erfasst, beispielsweise in Registrierkassen. Hierdurch haben sich die technischen Herausforderungen für die Steuerprüfung stark verändert, denn nachträgliche Manipulationen elektronischer Aufzeichnungen sind ohne geeignete Schutzmaßnahmen kaum feststellbar.

Um solchen Manipulationen entgegenzuwirken, müssen elektronische Aufzeichnungssysteme gemäß Abgabenordnung und Kassensicherungsverordnung ab dem 1. Januar 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. Hierzu enthält die Technische Sicherheitseinrichtung ein Sicherheitsmodul und gewährleistet, dass Aufzeichnungen nachträglich nicht unerkannt geändert, gelöscht oder erzeugt werden können.

Die gesetzliche Neuregelung fördert explizit eine technologieoffene Ausgestaltung der Technischen Sicherheitseinrichtung. Durch eine einheitliche digitale Schnittstelle wird die Integration in existierende und zukünftige Kassensysteme vereinfacht. Insbesondere sind für die digitale Schnittstelle keine besonderen Anforderungen an die physische Schnittstelle geplant, sodass übliche Standardschnittstellen wie z. B. USB, Ethernet, microSD-Karten etc. zum Einsatz kommen 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 werden vom BSI in Technischen Richtlinien und Schutzprofilen festgelegt. Diese wurden in Abstimmung mit einschlägigen Fachverbänden und Herstellern zeitgerecht 2018 fertiggestellt und veröffentlicht.

Zudem begleitet das BSI im Rahmen des Projekts ZERSIKA seit Herbst 2018 aktiv die Zertifizierung einer Technischen Sicherheitseinrichtung für den Einsatz in Registrierkassen.

Somit bleibt ausreichend Zeit, um Technische Sicherheitseinrichtungen zu entwickeln und in den Verkehr zu bringen.

2.2.2.2.8 Sichere elektronische Identitäten auf dem Smartphone

Verbraucher nehmen heute über ihr Smartphone zahlreiche Dienste in Anspruch, die ein hohes Sicherheitsniveau voraussetzen: Sie entriegeln etwa die Türen von Carsharing-Fahrzeugen, eröffnen Bankkonten oder melden ihre neue Adresse an die Stadtverwaltung. Dies stellt besondere Anforderungen an ein ausreichend hohes Schutzniveau. Neben Login und Registrierung bei Diensteanbietern kann die sichere elektronische Identität (eID) auch vor Ort mit Nahfeldkommunikationstechnologie (NFC) eingesetzt werden. Dazu hält der Nutzer das Mobilgerät nah an einen anderen Gegenstand mit NFC-Chip, etwa den Türgriff eines Hotelzimmers. Das macht die Nutzung der eID sehr einfach.

Im Projekt OPTIMOS 2.0, an dem sich das BSI seit August 2018 als assoziierter Partner beteiligt, werden die Voraussetzungen für die Bereitstellung neuer Technologien für sichere eID-Dienste geschaffen. Mithilfe dieser Technologien werden Anbieter in die Lage versetzt, mobile eID-Dienste mit dem Schutzniveau „substanziell“ und „hoch“ nach eIDAS-Verordnung anzubieten. Das im Projekt entwickelte Ökosystem soll auf dem Schutzniveau „substanziell“ bei der EU notifiziert und dadurch in ganz Europa anwendbar gemacht werden.

Anbieter von mobilen Services können von dem offenen Ökosystem profitieren, wenn sie neben der eID weitere sensible Daten auf dem Smartphone ablegen wollen: Fluggesellschaften beispielsweise die Bordkarte, Verkehrsbetriebe eine persönliche Jahreskarte oder Car-Sharing-Unternehmen und Hotels den digitalen Auto- bzw. Zimmerschlüssel. Diese anwendungsspezifischen Daten auf dem Smartphone der Kunden sicher abzulegen, ist bislang für jeden Service-Anbieter eine komplexe Herausforderung. Denn unterschiedlichste Smartphone-Modelle und Mobilfunkanbieter sorgen für große Heterogenität bei der Hardware.

Das Förderprojekt OPTIMOS 2.0 schafft eine Plattform, die den Service-Providern den aufwändigen Teil abnimmt und gleichzeitig eine hohe hardwaregestützte Sicherheit ermöglicht.

2.2.2.3 Moderne Telekommunikationsinfrastrukturen (5G)

Im Sommer 2018 entwickelte sich „5G“ vom Insiderthema für Mobilfunkspezialisten zum öffentlichen Diskussionsgegenstand. Im Fokus der Diskussion stand und steht der

Aspekt Sicherheit – die Sicherheit wichtiger Informationen vor unberechtigten Zugriffen ebenso wie die Versorgungssicherheit im Bereich der zentralen Telekommunikationsinfrastrukturen.

Die Sicherheit deutscher Mobilfunknetze hat mit dem Telekommunikationsgesetz (TKG) eine klar definierte gesetzliche Grundlage. § 109 Abs. 6 des TKG legt fest, dass die Bundesnetzagentur im Einvernehmen mit dem BSI und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit einen Katalog von Sicherheitsanforderungen erstellt, der auch für die Betreiber und Lieferanten der neuen 5G-Netze maßgeblich ist und laufend den neuen technischen Entwicklungen angepasst werden kann. Die aktuelle Überarbeitung des Sicherheitskatalogs wurde, etwa zeitgleich mit dem Start der Auktion für die ersten deutschen 5G-Frequenzen, im März 2019 durch die Veröffentlichung der thematischen Eckpunkte angekündigt. Demzufolge soll das BSI als Cyber-Sicherheitsbehörde des Bundes vor allem die Verantwortung für die Prüfung der Netzwerkkomponenten zum Nachweis ihrer objektiven Sicherheitseigenschaften übernehmen. Damit werden seit dem Start des modernen Mobilfunks in Deutschland im Jahr 1992 erstmalig anerkannte Sicherheitsnachweise für die sicherheitsrelevanten Komponenten der Mobilfunknetze zur Pflicht. Der Aufbau der deutschen 5G-Netze ab 2020 wird so nach deutlich strengeren Sicherheitskriterien erfolgen als dies bei älteren Mobilfunknetzen (3G, 4G) der Fall war.

Dass 5G in der öffentlichen Wahrnehmung als eine Herausforderung in Hinblick auf die Sicherheit wahrgenommen wird, ist aufgrund der Komplexität der Technologie, auch im Zusammenspiel mit den aktuellen Netzwerken der zweiten, dritten und vierten Generation, nachvollziehbar. Mit der Einführung von 5G werden in den kommenden Jahren auch zahlreiche seit langem bekannte Sicherheitslücken der Vorgängertechnologien geschlossen. Zu diesen Innovationen gehören eine verbesserte Kryptografie, ein verbessertes Roaming und umfassende Maßnahmen zur Absicherung der Signalisierung zwischen unterschiedlichen Mobilfunknetzen.

Auch wenn häufig von „dem 5G-Netz“ die Rede ist, so darf man sich den Mobilfunk der Zukunft doch eher als ein Baukastensystem vorstellen, in dem Dienste und Strukturen mit unterschiedlichsten Eigenschaften gleichzeitig realisierbar sein werden. Zu den offensichtlichen Neuerungen zählt die Möglichkeit, eine geografisch begrenzte Lizenz für die Nutzung von 5G-Frequenzen erwerben zu können. Zahlreiche deutsche Wirtschaftsunternehmen haben schon ihr entsprechendes Interesse bekundet. Eine Realisierung separater virtueller Netze innerhalb der öffentlichen Infrastrukturen wird aber ebenso möglich sein. Im Rahmen des

sogenannten „Network Slicing“ können virtuelle Netzwerke oder Dienste auch im Hinblick auf kurze Latenzzeiten oder hohe Sicherheit „designed“ werden. Sicherheit ist damit nicht ausschließlich eine globale Eigenschaft des gesamten Netzes, die sich für jede Art der Nutzung gleich darstellt. Das Sicherheitsniveau kann vielmehr individuell auch höheren Anforderungen angepasst werden.

Die Einführung des Mobilfunkstandards 5G hat das Potenzial, sich zum größten Infrastrukturvorhaben des kommenden Jahrzehnts zu entwickeln und die Digitalisierung von Staat, Wirtschaft und Gesellschaft auf eine vollkommen neue Basis zu stellen. Das BSI begleitet diesen Prozess von Anfang an. Das BSI ist als eine von wenigen staatlichen Organisationen weltweit Mitglied der maßgeblichen Dachorganisation der Mobilfunkbranche GSMA und wird seine enge Vernetzung in konstruktiver Weise nutzen.

2.2.2.4 IT-Grundschutz-Profil und Testate

Seit nunmehr 25 Jahren ist der IT-Grundschutz ein bewährtes Angebot des BSI zur Erhöhung der Informationssicherheit in Institutionen. Das umfangreiche Portfolio enthält Empfehlungen und Anforderungen zu allen Fragen der Informationssicherheit. Das Angebot richtet sich sowohl an Anwender, die sich erstmalig mit IT-Grundschutz beschäftigen, als auch an fortgeschrittene 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 in einer Institution zu verbessern.

IT-Grundschutz-Profile bieten als Muster-Sicherheitskonzepte einen erleichterten Einstieg in den IT-Grundschutz. Zugleich ermöglichen sie erste Schritte für den Aufbau eines Managementsystems für Informationssicherheit (ISMS) sowie eines Sicherheitskonzepts. Ein IT-Grundschutz-Profil bildet als Schablone eine Referenz-Architektur eines bestimmten Anwendungsfalls ab.

Seit der Vorstellung des Konzepts „IT-Grundschutz-Profil“ im vergangenen Jahr haben bereits mehrere Institutionen und Verbände in Zusammenarbeit mit dem BSI erste IT-Grundschutz-Profile erstellt. Zudem sind auf der BSI-Webseite erste IT-Grundschutz-Profile veröffentlicht und können für eigene Sicherheitsbetrachtungen herangezogen werden, z. B.:

- Handwerkskammern
- Handwerksbetriebe

- Reedereien (Landbetrieb)
- Kommunalverwaltungen.

Zurzeit werden IT-Grundschutz-Profile für weitere Branchen erstellt. Anwender, die beabsichtigen, ein IT-Grundschutz-Profil für ihre Branche zu erstellen, können sich an das BSI wenden. Ziel ist es, perspektivisch zu möglichst vielen Themen und für unterschiedliche Branchen IT-Grundschutz-Profile zu veröffentlichen, damit sich weitere Anwender dieser erprobten und praktikablen Arbeitshilfe bedienen können.

Die Vorgehensweise „Basis-Absicherung“ aus dem 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 hinweg bieten. Die Umsetzung lässt sich mit vergleichsweise geringem finanziellen, personellen und zeitlichen Aufwand realisieren. Dadurch eignet sich die Basis-Absicherung gerade für KMU oder kleinere Kommunen, die einen ganzheitlichen Ansatz zum Aufbau eines ISMS verfolgen wollen.

Unternehmen und Behörden können mit einem Testat nach der „Basis-Absicherung“ nachweisen, dass sie den IT-Grundschutz gemäß der gleichnamigen Absicherung umgesetzt haben. Mit einem Testat nach der „Basis-Absicherung“ 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 sind die Vorgehensweisen, die angestrebt werden sollten, um eine Institution angemessen und umfassend nach dem Stand der Technik zu schützen. Diese ermöglichen auch den Erwerb eines ISO-27001-Zertifikats auf der Basis von IT-Grundschutz.

2.2.2.5 Umsetzung IT-Sicherheitsgesetz (IT-SiG) und UP KRITIS

Das IT-Sicherheitsgesetz (IT-SiG) hat im BSI-Gesetz und in weiteren Gesetzen neue Pflichten für KRITIS-Betreiber eingeführt. So sieht das BSI-Gesetz nun für KRITIS-Betreiber Maßnahmen zur Vorbeugung (§ 8a) und zur Bewältigung (§ 8b) von IT-Sicherheitsvorfällen vor.

Status Umsetzung IT-SiG

KRITIS-Betreiber müssen zur Umsetzung des § 8a Abs. 1 BSIG „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen treffen“. Sie müssen den Stand der Technik einhalten und können dafür branchenspezifische Sicherheitsstandards (B3S) erarbeiten, die das BSI nach Antrag auf Eignung prüft. Über 20 KRITIS-Branchen haben bereits B3S erstellt oder erarbeiten solche. Zehn davon wurden bereits vom BSI mit positivem Ergebnis auf Eignung geprüft.

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

- Ernährungswirtschaft
- Fernwärme
- Versicherungen
- (medizinische) Labore
- Elektrizität.

Darüber hinaus müssen die Betreiber gemäß § 8a Abs. 3 BSIG die Umsetzung des Stands der Technik in ihren Anlagen überprüfen lassen, das BSI erhält die Nachweise der Prüfungen.

Seit 2015 haben die Betreiber Kritischer Infrastrukturen gemeinsam mit dem BSI das Meldewesen nach § 8b BSIG aufgebaut. Über 1.500 KRITIS-Anlagen haben sie beim BSI registriert, damit diese vom BSI mit Warnmeldungen versorgt werden. Gleichzeitig melden Betreiber größere Sicherheitsvorfälle an das BSI, damit das BSI aus diesen Informationen ein detailliertes Lagebild erstellen und andere Betreiber warnen kann.

Das BSI erhält viele Nachfragen zur Umsetzung der Vorgaben aus dem IT-Sicherheitsgesetz. Zur Erstellung von B3S und zum Thema Nachweise hat das BSI jeweils eine Orientierungshilfe herausgegeben. Die Orientierungshilfe für Nachweise sowie die Formulare zur Nachweiserbringung wurden überarbeitet. Die Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a Abs. 2 BSIG liegt weiterhin in Version 1.0 vor. Auch ergänzt das BSI regelmäßig die FAQs zu Themen des BSI-Gesetzes, die auf den BSI-Webseiten zur Verfügung stehen.

Kooperation im UP KRITIS

Für die kooperative Umsetzung der neuen Vorgaben aus dem BSIG nutzen Betreiber und Behörden den UP KRITIS (<http://www.upkritis.de>), die öffentlich-private Partner-

schaft von KRITIS-Betreibern, ihren Verbänden und dem Staat. Dort werden beispielsweise B3S in gemeinsamen Arbeitsgruppen entwickelt, aber auch Erfahrungen und Ideen zu Meldewesen, Nachweisen oder Cyber-Sicherheitsübungen ausgetauscht.

Der UP KRITIS hat als Plattform für die Belange der Betreiber Kritischer Infrastrukturen vom BMI ein Mandat erhalten. Er soll insbesondere bei Regulierungsvorhaben und anderen Sachverhalten, die Kritische Infrastrukturen sektorübergreifend betreffen, als Institution beteiligt und angehört werden. Gleichzeitig eröffnet das Mandat den Betreibern auch den Weg zur Formulierung ihrer Anliegen an öffentliche Stellen.

Leistungen aus dem IT-SiG: Warnungen, Lagebilder

Das BSI hat durch das IT-Sicherheitsgesetz im Jahr 2015 nicht nur neue Befugnisse, sondern auch neue Pflichten bekommen. Nach § 8b Abs. 2 BSIG hat das BSI die Aufgabe, alle ihm vorliegenden Informationen zur IT-Sicherheitslage zu analysieren, das Lagebild kontinuierlich zu aktualisieren und die Betreiber Kritischer Infrastrukturen über sie betreffende Informationen zu unterrichten.

Diese Unterrichtung geschieht durch verschiedene BSI-Produkte wie z. B. Cyber-Sicherheitswarnungen, BSI-Management-Informationen, Themenlagebilder oder Monatsberichte.

Im Berichtszeitraum wurden mehr als 60 anlassbezogene Warnungen und Informationen zu Sachverhalten mit besonderer Relevanz sowie 21 Lageprodukte und -berichte für unterschiedliche Zielgruppen zur allgemeinen Darstellung der IT-Sicherheitslage versendet oder zur Verfügung gestellt.

Eine wichtige Informationsquelle für die Erstellung von Warnungen sind die Meldungen der KRITIS-Betreiber über IT-Störungen. Wird das BSI frühzeitig über bestehende IT-Störungen informiert, kann das BSI andere Betreiber warnen und mit Empfehlungen versorgen. Diese Betreiber können somit zeitnah geeignete Abwehr- oder Schutzmaßnahmen ergreifen, um ihre Anlagen entsprechend abzusichern.

Darüber hinaus hat das BSI mit verschiedenen Betreibern Kritischer Infrastrukturen konkrete Austauschformate und Plattformen wie die Malware Information Sharing Platform (MISP) für technische Signaturen und Parameter diskutiert. Derzeit werden verschiedene Modelle für den zukünftigen operativen Austausch im größeren Kreis vorbereitet. Die ersten davon können voraussichtlich ab Mitte 2019 angeboten werden.

Vorfallsunterstützung und MIRT

Das BSI unterstützt Betroffene - vor allem aus seinen verschiedenen Zielgruppen in Verwaltung und Kritischen Infrastrukturen - bei schweren IT-Sicherheitsvorfällen. Diese Unterstützung reicht von telefonischen Erstberatungen mit Hinweisen auf Hilfen und Angebote des BSI über ausführliche und wiederholt durchgeführte Telefon- und Videokonferenzen mit verschiedenen Experten der Beteiligten bis hin zum Vor-Ort-Einsatz von Mobilien Vorfallaufklärungsteams, sogenannten MIRTs (Mobile Incident Response Teams). Dabei wird die Unterstützung jeweils an die Erfordernisse und Bedürfnisse der Betroffenen angepasst. Ziel ist dabei stets, Tiefe und Ausdehnung eines Angriffs festzustellen, diese einzudämmen und gemeinsam mit dem Betroffenen die IT-Infrastruktur zu bereinigen und gegen Neuinfektionen zu härten. Auch bei verschiedenen schweren Cybercrime-Angriffen oder -Vorfällen mit Schadsoftware konnte das BSI mit Erfahrungen und konkreten Empfehlungen helfen. Während im Cybercrime-Umfeld noch bis vor kurzem eher großflächige, opportunistische Angriffe das Bild prägten, verwenden die Täter dort mittlerweile ebenfalls Techniken, die bislang vorrangig im Umfeld gezielter Angriffe (APTs) zu beobachten waren. Hierzu zählen beispielsweise manuelles Verbinden mit infizierten Systemen sowie aktives Bedienen von Schadprogrammen oder Administrationswerkzeugen, um Betroffene auszuspähen und den „Wert“ einer möglichen Erpressung abschätzen zu können, Seitwärtsbewegung und Ausbreitung im internen Netz auszulösen oder zentrale IT-Systeme wie etwa das Active Directory zu übernehmen.

Bei der Analyse von Angriffen und der Vor-Ort-Unterstützung von Betroffenen arbeitet das BSI im Rahmen des Nationalen Cyber-Abwehrzentrums eng mit anderen Sicherheitsbehörden auf Bundes- und Landesebene zusammen. So können Betroffene gemeinsam angesprochen und beraten werden; ein kontinuierlicher Informationsaustausch zwischen den Beteiligten sorgt für einen gemeinsamen aktuellen Erkenntnisstand. Zum Schutz der Interessen der Betroffenen findet diese Beratung grundsätzlich unter einer besonderen Vertraulichkeit statt. Nur selten machen diese im Nachgang die Tatsache öffentlich, dass sie betroffen waren und wie mit dem Angriff umgegangen wurde. Bereinigt um konkrete Details zu individuellen Betroffenen, kann das BSI aus diesen Vorfällen jedoch abstrahierte Informationen und Empfehlungen ableiten, die es dann über die bestehenden Informationsaustauschplattformen anderen ins Visier Geratenen oder von möglichen ähnlichen Angriffen Betroffenen in Verwaltung, Kritischen Infrastrukturen und Wirtschaft zur Verfügung stellt.

2.2.2.6 Allianz für Cyber-Sicherheit

Im Jahr 2012 rief das BSI mit der Allianz für Cyber-Sicherheit ein kostenfreies Angebot für Unternehmen und Institutionen mit Sitz in Deutschland ins Leben. Von den Cyber-Sicherheitsempfehlungen, Veranstaltungen zum gegenseitigen Austausch und Fortbildungsangeboten konnten seitdem zahlreiche Organisationen – insbesondere (aber nicht ausschließlich) kleine und mittlere Unternehmen – profitieren.

Inzwischen verzeichnet die Allianz für Cyber-Sicherheit mehr als 3.700 Teilnehmer (Stand: Juni 2019), welche die Angebote nutzen, ca. 120 Partner, die eigenständig Inhalte erstellen, und über 90 Multiplikatoren, von denen die Informationen zu Cyber-Bedrohungen und Lösungsangeboten in ihre Netzwerke verteilt werden. Auf Basis der Rückmeldungen dieser Mitglieder konnte das Portfolio immer weiter optimiert werden: Stand in den Anfangstagen insbesondere der Aufbau eines tagesaktuellen Informationsportals im Vordergrund, so liegt ein weiterer Schwerpunkt der Arbeit nunmehr im Austausch von Expertenwissen, Erfahrungen und praktischen Empfehlungen sowie dem Networking.

Unter dem Motto „Netzwerke schützen Netzwerke“ werden seitens der Allianz für Cyber-Sicherheit insbesondere im Jahr 2019 Angebote entwickelt, die IT-Sicherheitsinteressierten praxisnahe Lösungen in die Hände geben und so unmittelbar zu mehr Cyber-Sicherheit in den Betrieben in Deutschland führen können.

2.2.2.7 Austausch der Cyber-Sicherheitsinitiativen in Deutschland

Der Mitte 2017 gestartete Dialogprozess des BSI mit deutschen Cyber-Sicherheitsinitiativen wird fortgesetzt und intensiviert. Ziel ist es, Synergien zu nutzen und das Bewusstsein für Cyber-Sicherheit in Deutschland sowie die Reichweite einzelner Sensibilisierungsaktionen zu erhöhen. Die Organisation des regelmäßigen Austauschs liegt bei der Allianz für Cyber-Sicherheit.

Im Oktober 2018 hat das BSI interessierten Initiativen für den European Cyber Security Month (ECSM) Kampagnen-Material zur Verbreitung in den sozialen Medien bereitgestellt. In den vier Aktionswochen konnten Awareness-Grafiken mit Tipps zum Umgang mit unbekannten USB-Sticks, Sicherheits-Updates sowie Phishing- oder Social Engineering-Angriffen über Twitter, Facebook und Co. geteilt werden. Ziel der ersten gemeinsamen Aktion war es, konzentriert für die Umsetzung von Cyber-Sicherheits-Maßnahmen in Unternehmen zu werben.

In diesem Jahr haben die Cyber-Sicherheitsinitiativen zusammen eine Kampagne für den ECSM im Oktober 2019 entwickelt, um Unternehmen für einen sicheren Umgang mit IT zu sensibilisieren und dem gemeinsamen Ziel näherzukommen, die Cyber-Sicherheit in Deutschland zu stärken. Die Arbeitsergebnisse werden der Öffentlichkeit am 26. September 2019 auf dem Cyber-Sicherheitstag in Berlin präsentiert und im Rahmen des diesjährigen ECSM gemeinsam verbreitet.

2.2.2.8 Sonstige Lösungen/Angebote für die Wirtschaft

Investitionsprüfung

Das BSI wird vom Bundesministerium des Innern, für Bau und Heimat (BMI) bei Verfahren zur Kontrolle 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 Sicherheit der Bundesrepublik Deutschland durch den beabsichtigten Erwerb gefährdet sind. Dies gilt beispielsweise in Fällen, in denen die Zielgesellschaft Produkte oder wesentliche Komponenten für VS-zugelassene 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 der Beteiligten analysiert und bewertet das BSI mögliche Auswirkungen auf die IT-Sicherheit. Die Gefährdungsbewertung fließt in das sicherheitspolitische Votum des BMI ein. Um die Unternehmen durch die Verfahren nicht unnötig zu belasten, führt das BSI die teilweise sehr komplexen Einzelprüfungen sehr zügig, d. h. im Regelfall innerhalb von nur ein oder zwei Arbeitswochen durch.

Unter anderem folgende Faktoren haben zu einem signifikanten Anstieg der Prüfungsverfahren geführt, bei denen das BSI aktiv eingebunden wurde:

Durch eine grundsätzliche Neufassung von AWG und AWV wurden Gesetz und Verordnung 2017 und 2018 verschärft, um Lücken in den Verfahrensregeln zu schließen und die Schutzmaßnahmen Kritischer Infrastrukturen zu konkretisieren. Zuletzt wurden die Kritischen Infrastrukturen zum Jahreswechsel 2018/2019 um den neuen Bereich Rundfunk, Telemedien und Druckerzeugnisse erweitert sowie für Hersteller branchenspezifischer Software der Schwellwert einer meldepflichtigen Beteiligungshöhe von 25 % auf 10 % abgesenkt.

Seit Jahren steigen Anzahl und Volumen der Investitionen von außerhalb der EU in deutsche Unternehmen und Konzerne.

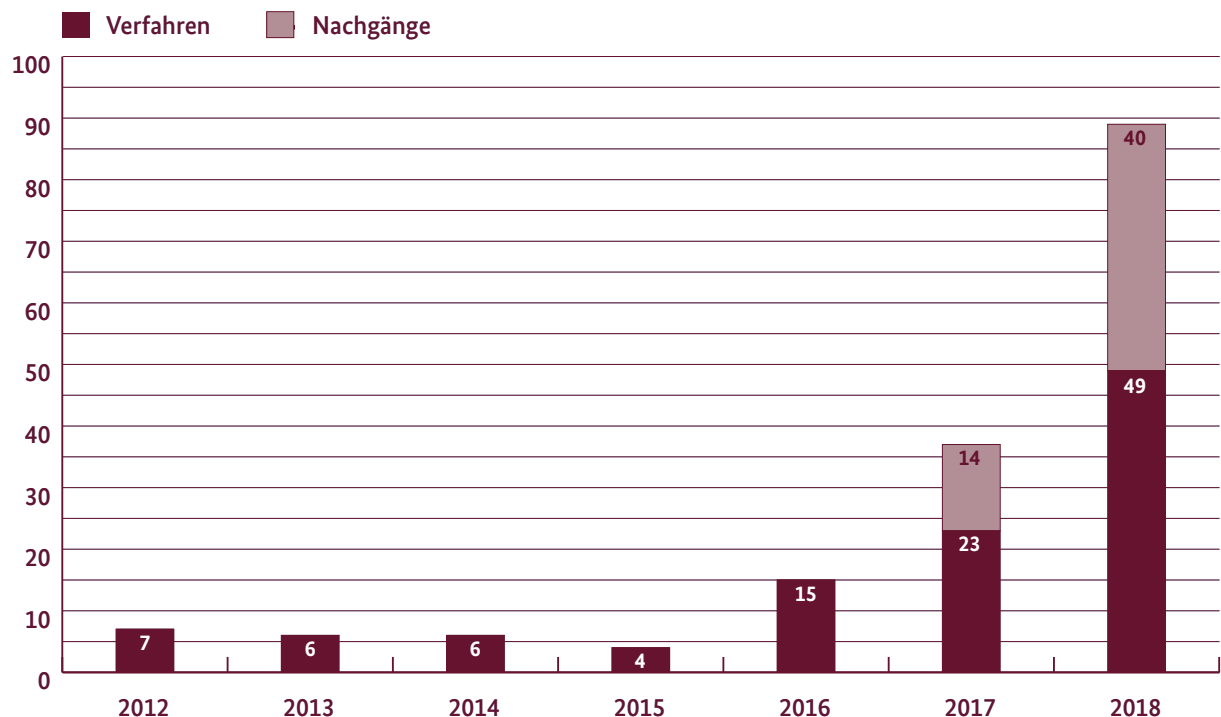


Abbildung 12 Anzahl der im BSI bearbeiteten AWG-Verfahren und zugehöriger Nachgänge, 2012-2018.

Die Anzahl der durch das BSI begleiteten Einzelprüfungen im Zusammenhang mit Investitionskontrollverfahren hat sich im letzten Jahr erneut verdoppelt. Sie stieg von 4 Verfahren 2015 auf 49 Verfahren 2018. Die seit Januar eingegangenen Verfahren haben den Trend zur jährlichen Verdopplung bestätigt, so dass das BSI von bis zu 100 Verfahren im Jahr 2019 ausgeht.

BAFA Ausfuhrkontrolle

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

1. die Unterstützung aber auch der (Selbst-)Schutz der deutschen Kryptoindustrie
2. Schutz zugelassener IT-Sicherheitsprodukte und Komponenten wie Smartcards etc. und Technologie (vor Re-Engineering Manipulation etc.)

Das BSI hat im Jahr 2018 112 Anträge bearbeitet, wodurch ein Gesamtumsatz von rund 134 Mio. € generiert wurde.

Zudem wurden im Berichtszeitraum folgende Themen bearbeitet:

- Seit Mai 2016 konzentriert sich die Bearbeitung der Anträge auf Ausfuhr-/Verbringungs-genehmigung auf zugelassene IT-Sicherheitsprodukte, um die Anzahl der im BSI bearbeiteten BAFA-Anträge zu reduzieren als Reaktion auf die steigende Anzahl der Anträge allgemein (s. Abb. 11). Dies geschah in bilateraler Abstimmung mit dem BAFA.
- Das Ergebnis ist eine umfassende, schnelle und qualitätsorientierte Bearbeitung der Anträge, entsprechend der Vorstellung von BAFA, BSI und den Antragstellern gegenüber den vergangenen Jahren.
- Mitarbeit bei der Überarbeitung von EU Allgemeingenehmigungen (AGG)
- Beteiligung bei Firmen-Verkäufen/-Übernahmen im Bereich der Informationssicherheit im Rahmen der Erlassbearbeitung/-Beteiligung
- Unterstützung des BAFA bei der Auskunft zur Güterliste (AzG) zur Feststellung der Exportpflicht eines Produktes im o. g. Kontext
- Unterstützung des BAFA bei Anfragen bzgl. verschiedener Technologien wie z. B. 5G und Quantenkryptografie.

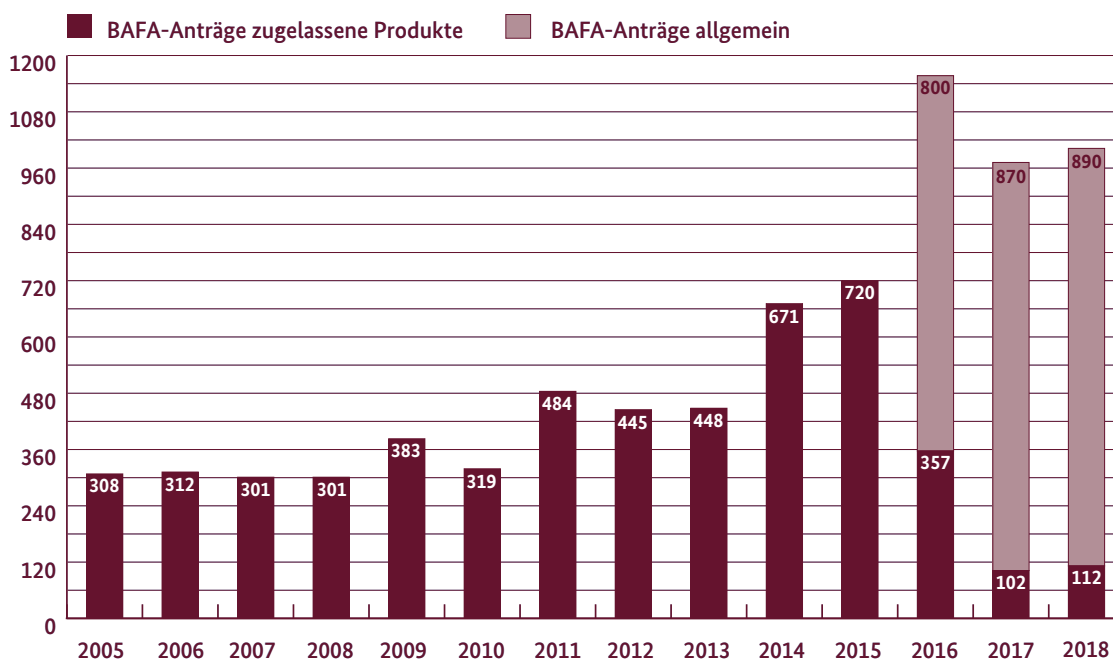


Abbildung 13 Darstellung der Anzahl der im BSI bearbeiteten BAFA-Anträge von 2005 bis 2018.

2.3 Gesellschaft/Bürger

Die Information und Sensibilisierung von Bürgerinnen und Bürgern für einen sicheren Umgang mit Informationstechnologie, mobilen Kommunikationsmitteln und dem Internet ist eine wichtige Aufgabe des BSI. Unter dem Namen „BSI für Bürger“ steht Interessierten ein umfangreiches Informationsangebot zur Verfügung. Auch der digitale Verbraucherschutz ist eine Aufgabe, die im Koalitionsvertrag der Bundesregierung 2018 etabliert wurde.

2.3.1 Gefährdungslage Gesellschaft/Bürger

Erkenntnisse aus Umfragen, die das BSI in Kooperation mit der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK) durchgeführt hat, werden im folgenden Kapitel zusammengefasst. Hierbei geht es um den Schutz der Internetnutzerinnen und -nutzer vor Gefahren der digitalen Welt. In diesem Zusammenhang gewinnt der Bereich Smart Home und das Internet der Dinge immer mehr an Bedeutung. Weitere Themen: die Sicherheit von Medizinprodukten und die Sicherheit von Bezahlverfahren.

2.3.1.1 Ergebnisse und Erkenntnisse aus der gemeinsamen Umfrage BSI und ProPK

Das BSI und die ProPK kooperieren, um Bürgerinnen und Bürger umfassend über Schutzmöglichkeiten und die Risiken im Internet aufzuklären. In einer repräsentativen Umfrage erhoben die beiden Partner, welche Bedeutung Sicherheit im Internet bei Privatanwendern hat, inwiefern sie sich vor den Gefahren der digitalen Welt schützen und wie sie sich über Schwachstellen und Risiken informieren.

Es stellte sich heraus, dass das Thema „Sicherheit im Internet“ generell einem Großteil wichtig ist: Über 80 % der Befragten machen sich Sorgen um die eigene Sicherheit im Internet. Die Intensität variiert jedoch: Die Hälfte (51 %) machen sich eher selten Sorgen, knapp jeder Dritte (31 %) häufig oder fast immer.

Fast jeder Vierte (24 %) war bereits Opfer von Kriminalität im Internet. Dabei sind der Betrug beim Online-Shopping (36 %), Phishing (28 %) und Schadsoftware (26 %) den Befragten am häufigsten widerfahren. 39 % der Befragten haben sich nach der Straftat selbst geholfen. Als Schutzmaßnahmen wurden am häufigsten Antivirenprogramme (61 %), sichere Passwörter (58 %) und eine aktuelle Firewall (52 %) von denjenigen genannt, die sich um ihre Sicherheit im Internet sorgen. Sofortige Installationen von verfügbaren Updates wenden nur 36 % an.

Nach ihrem Informationsverhalten befragt, gab nur ein Drittel (31 %) an, sich regelmäßig über Internetsicherheit zu informieren, die meisten nur, wenn sie selbst Opfer einer Cyber-Attacke geworden waren. Die Hälfte der Befragten kennt die aktuellen Sicherheitsempfehlungen zum Schutz vor Kriminalität im Internet. Etwa jeder Vierte erhält diese durch das BSI und kennt die Website von „BSI für Bürger“ (24 %).

Besonders wichtig sind den Befragten Aktivitäten im Internet, bei denen finanzielle Daten bearbeitet werden: Sicherheit beim Online-Banking (62 %) sowie Online-Shopping (44 %). Auch das allgemeine Surfen (33 %) und E-Mail-Kommunikation (30 %) wurde relativ häufig genannt. Weniger wichtig ist den Bürgern die Sicherheit bei der Nutzung sozialer Netze (14 %) und bei der Kommunikation per Messenger (11 %). Fast keine Bedeutung für die Befragten haben die Themen „Installieren von Apps“ und die „Nutzung von offenen WLAN“ (jeweils 6 %) sowie die sichere Nutzung vernetzter Heimgeräte und Online-Spiele (jeweils 3 %). Die Ergebnisse der Umfrage fließen in die weitere gemeinsame Aufklärungsarbeit von Polizei und BSI ein.

2.3.1.2 Smart Home und das Internet der Dinge

In vielen Haushalten werden Breitbandrouter (im Folgenden Router genannt) genutzt, um damit auf das Internet zuzugreifen. Sie ermöglichen nicht nur den Zugriff auf das Internet, man kann mit ihnen auch meist das Heimnetzwerk, teils sogar das Smart Home, verwalten. Durch ihre Funktion als Türöffner zur digitalen Welt können sie aber auch von zwei Seiten, lokal (z. B. über das WLAN) und über das Internet, angegriffen werden. Wie in Kapitel 1.2.5 Botnetze erläutert, ist ihnen daher ein besonderes Gefahrenpotenzial und eine besondere Schutzfunktion zuzuschreiben.

Router sind verhältnismäßig leistungsfähige integrierte Systeme. Dadurch können sie sich erfolgreich gegen Angriffe zur Wehr setzen, bieten aber auch einen hohen Anreiz für Angreifer, sich die Ressourcen der Router für rechtswidrige Aktionen zunutze zu machen. Mit einer Kontrollübernahme des Routers können diese selbst zum Risiko werden. So können z. B. Nutzer ausgespäht oder vom kompromittierten Gerät selbst Angriffe initiiert werden. So wurde im Jahr 2016 durch Angreifer versucht, knapp eine Millionen Router über einen Fernwartungsport mit Schadsoftware zu infizieren und in das Mirai-Botnetz zu integrieren. Dies schlug fehl, da die Router beim Versuch, die Schadsoftware zu installieren, abstürzten.

Es ist daher wichtig, für einen Basisschutz bei Routern zu sorgen. Im besten Falle können Angriffe auf den Router so schon im Vorfeld verhindert und damit der Schutz des Heimnetzes aufrechterhalten werden.

Aus Sicht des BSI sind auch im Bereich Smart Home Prävention und Detektion zwingend notwendig. Mit der Veröffentlichung der Technischen Richtlinie (TR) für Router (kurz: Router-TR) durch das BSI im November 2018 wurde eine Grundlage geschaffen, um Router gegen Angriffe zu schützen und widerstandsfähiger zu machen. Nach der Veröffentlichung erhielt die Router-TR viel Lob, aber auch Kritik und markiert daher den Einstieg in eine fortwährende Diskussion und Fortentwicklung der TR.

Parallel hat das BSI Anfang des Jahres 2019 mit der Entwicklung einer Prüfspezifikation für die Router-TR begonnen. Die TR kann mit Hilfe der Prüfspezifikation als Grundlage für eine Prüfung oder auch Zertifizierung verwendet werden. Dadurch kann eine Vergleichbarkeit hinsichtlich der Sicherheitsleistung verschiedener Router für den Verbraucher erreicht werden.

Neben dem Router als Zentrum des Smart Home, fallen unter diesen Begriff auch andere Geräte oder Dienste, beispielsweise im Kontext Heimautomation oder Unterhaltungselektronik. Die Nutzerinteraktion mit diesen Geräten erfolgt weniger mit klassischen Desktop-PCs oder Laptops, sondern mittels Sprachassistenzsystemen, Smartphone- und Tabletanwendungen oder Wearables. Bezeichnend für die Entwicklung in diesem Sektor ist der weiterhin wachsende Stellenwert der Kommunikationsfähigkeit der einzelnen Komponenten untereinander und mit durch den Router erreichbaren Diensten aus dem Internet.

Um ein geeignetes IT-Sicherheitsniveau in den Markt internetfähiger Produkte für den Endverbraucher zu bringen, arbeitet das BSI im Dialog mit vielen Stakeholdern an entsprechenden Anforderungen und Prüfkriterien. In diesem Kontext wurde die vor kurzem veröffentlichte DIN SPEC 27072 in einem Arbeitskreis unter dem Dach des Deutschen Instituts für Normung (DIN) entwickelt. Das Dokument enthält generische Mindestanforderungen zur IT-Sicherheit für den privaten Endkundenbereich und soll als Grundlage für verschiedene Evaluations- und Zertifizierungsverfahren dienen.

2.3.1.3 Sicherheit von Medizinprodukten

Die fortschreitende Digitalisierung im Gesundheitswesen, vernetzte Medizinprodukte und das Gefühl, dass es nahezu täglich neue, smarte Produkte rund um den Gesundheitssektor gibt, beschreiben die derzeitige Situation in

Deutschland recht gut. Gerade im Gesundheitswesen, wo es gesetzliche Vorgaben, wie die Einführung einer elektronischen Patientenakte für gesetzlich Versicherte gibt, ist der Trend und Druck in Richtung mobiler Lösungen spürbar präsent. Die alltägliche Routine bei der Nutzung mobiler Endgeräte (Tablet, Smartphone), die Steigerung der Funktionalität und der benutzerfreundliche orts- und zeitunabhängige Zugriff tragen dazu bei, dass mobile Anwendungen großen Zuspruch in der Gesellschaft finden.

Die Anwendungsbreite mobiler Lösungen nimmt im medizinischen Umfeld rasant zu. Die meisten dienen zur Speicherung und Übermittlung von Gesundheitsdaten (z. B. Fitness-Tracker), die dem Privatanwender zur Verfügung stehen (Gesundheits-Apps). Darüber hinaus werden vermehrt Apps für chronisch Kranke (z. B. Diabetiker) und für die Begleitung von klinischen Studien entwickelt. Bei einer Vielzahl dieser Anwendungen handelt es sich bereits um Medizinprodukte und viele weitere werden in naher Zukunft voraussichtlich als solche in den Verkehr gebracht. Die mobilen Technologien erlauben Ärzten und medizinischem Fachpersonal, schnell und einfach auf personenbezogene Daten zuzugreifen und dem Patienten Daten zu übermitteln. Es sind keine speziellen Geräte, außer einem Smartphone oder Tablet, vonnöten. Personenbezogene Daten sind z. B.: Name, Vorname, Alter, Geschlecht, Größe, bei med. Anwendungen: Blutzuckerwerte, Blutdruckwerte, Sauerstoffsättigung, Diabetes-Tagebuch, Blutdruck-Tagebuch, Schwangerschafts-Tagebuch etc. Die Nutzung mobiler Anwendungen spart Patienten und Ärzten langfristig Zeit und Papier. Mit mobilen Anwendungen sind Gesundheits-/Fitnessapps im weitläufigen Sinne gemeint und damit alle mobilen Anwendungen, die personenbezogene Gesundheitsdaten aufnehmen. Dabei kann es sich auch um eine App, in Kombination mit einem Medizinprodukt, handeln. Bei Insulinpumpen oder Schlafapnoe-Therapiegeräten gibt es beispielsweise solche Lösungen. Besonders im Bereich der telemedizinischen Betreuung und Nachsorge gewinnen mobile Anwendungsszenarien zunehmend an Bedeutung, mit dem Ziel, die Orts- und Zeitunabhängigkeit besser für Patienten, Ärzte und medizinisches Fachpersonal nutzbar zu machen.

Die Cyber-Sicherheit spielte bei den Herstellern mobiler Anwendungen oft nur eine untergeordnete Rolle. Dies zeigt sich in den beiden BSI-Projekten im Bereich der vernetzten Medizinprodukte/Altenpflegeprodukte. In dem Projekt eCare (vernetzte Altenpflegeprodukte) wurden bereits Schwachstellen in mobilen Anwendungen gefunden, die noch nicht öffentlich gemacht wurden. Die Ergebnisse des eCare-Projekts werden im Herbst 2019 erwartet und veröffentlicht. Die Ergebnisse des Projekts ManiMed (Manipulation von Medizinprodukten) werden im Herbst 2020 erwartet. Hier wird bald mit der

Testung der Produkte begonnen, so dass aktuell noch keine Schwachstellenfindings vorliegen. Der steigende Vernetzungs- und Verbreitungsgrad sowie die Akzeptanz für mobile Anwendungen in der Bevölkerung bringen die Gefahr mit sich, dass zeitgleich auch das Risiko für einen Cyber-Angriff steigt. Das BSI ist nach § 7a BSIG Abs.1 dazu befugt, Produkte und Systeme mit IT-Bezug, die auf dem deutschen Markt bereitgestellt werden, zu untersuchen und, unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen, zu warnen. Neben vernetzten Medizinprodukten wurden auch einige mobile Anwendungen aus dem Gesundheitsbereich geprüft. Bei vielen der überprüften mobilen Anwendungen ist aufgefallen, dass oftmals sensible, personenbezogene Daten unverschlüsselt im Arbeitsspeicher zwischengespeichert werden und dass Mechanismen zum Onboarding fehlen oder nicht sicher implementiert worden sind. Mit Onboarding ist das (erste) Anmelden in der mobilen Anwendung gemeint. Hier wird oftmals nicht geprüft, ob die Identität der Person stimmt. Es gibt bspw. mTan-Verfahren, Einmalpasswörter, Authentifizierung mit der Ausweis-App etc., oder kein besonderes Verfahren für die Erstanmeldung. Die Verfahren sind unterschiedlich sicher (kein Faktor, 1-Faktor-, 2-Faktor-Authentisierung). Unsichere Apps bieten potenziell die Möglichkeit, ohne Kenntnis des Patienten Daten auszulesen, zu speichern und gegebenenfalls zu manipulieren.

Die ab 2020 geltende EU-weite Medical Device Regulation (MDR) wird massive Änderungen für Hersteller, Betreiber, benannte Stellen und Anwender mit sich bringen. Erstmals werden Cyber-Sicherheitseigenschaften von Medizinprodukten gefordert und viele Produkte werden höheren Risikoklassen zugeteilt werden. Bisher wurde der Fokus beim Design solcher Produkte auf die Gefährdungsfreiheit des Patienten gelegt.

Die Gefährdungslage ist als kritisch zu betrachten, so dass auch in Zukunft verstärkt geeignete Sicherheitsmechanismen für vernetzte Medizinprodukte und mobile Anwendungen im Gesundheitswesen zu entwickeln sind. In Zusammenarbeit mit den zuständigen Aufsichtsbehörden und durch die Projekte „eCare – Digitalisierung in der Pflege“ und „ManiMed-Manipulation von Medizinprodukten“ reagiert das BSI auf diese Entwicklungen. In diesem Jahr sind bereits Veröffentlichungen in diesen Bereichen und der ersten Projektergebnisse geplant.

2.3.1.4 Sicherheit von Bezahlverfahren

Als PSD2 (Payment Service Directive 2) wird die erweiterte Zahlungsdienste-Richtlinie (Nr. 2015/2366) des Europäischen Parlaments und des Rates vom 25. November 2015 über die Zahlungsdienste im Binnenmarkt bezeichnet. Sie

ist seit dem 13. Januar 2018 gültig und wird in Deutschland – zumindest der aufsichtsrechtliche Teil – durch das neue Zahlungsdiensteaufsichtsgesetz (ZAG) umgesetzt.

Die European Banking Authority (EBA) ist in enger Zusammenarbeit mit der Europäischen Zentralbank (EZB) durch die PSD2 beauftragt, technische Regulierungsstandards (RTS) und Leitlinien für verschiedene Aspekte der PSD2 auszuarbeiten. Im Januar 2018 wurde der RTS zur sicheren Kommunikation und starken Kundenauthentifizierung veröffentlicht und muss ab dem 14. September 2019 umgesetzt werden.

Der RTS gibt keine konkreten Hinweise zur Umsetzung, obwohl er die PSD2 in technischer Sicht ausgestalten soll. Er lässt vielmehr Raum für Interpretationen. Festgelegt ist, dass ab Inkrafttreten immer zwei von drei Faktoren der Kategorien Besitz, Wissen und Inhärenz zur Authentifizierung angewendet werden müssen, sobald ein Online-Zugriff auf ein Bankkonto erfolgt. Ungeklärt ist, wie die Stärke des Authentifizierungsverfahrens ausgeprägt sein soll und auf welchem Level die Sicherheitsanforderungen zu erfüllen sind.

Aus Sicht des BSI besteht die Gefahr, dass Finanzinstitute zugunsten einer schnellen Abwicklung ohne Aufwand für den Nutzer auf die starke Kundenauthentifizierung verzichten. Dies ist möglich, wenn das Instrument der eigenen Risikoanalyse angewendet wird. Dabei obliegt es dem Risikomanagement des Zahlungsdienstes, das Authentifizierungsverfahren abhängig von der eigenen Risikobereitschaft zu wählen.

Primäres Ziel der PSD2 und der entsprechenden anhängenden Dokumente ist es, den Wettbewerb im Zahlungsverkehr zu stärken, die Sicherheit von Zahlungsdienstleistern zu erhöhen und die Verbraucher besser zu schützen, wenn sie online bezahlen, sowie die Entwicklung und Nutzung innovativer Online- und Mobilfunkzahlungen zu fördern. So soll beispielsweise der Einkauf im Internet durch die starke Kundenauthentifizierung sicherer werden, die Betrugsraten sollen sinken. Dies kann aus Sicht des BSI jedoch nur erreicht werden, wenn sichere Authentifizierungsverfahren angeboten und vom Nutzer auch eingesetzt werden. Das Mobile Banking, bei dem die bekannte Chipkarte (Kredit- oder Debitkarte) durch das Einbringen der Daten in eine Banking App auf dem Mobilgerät ersetzt wird, kommt zunehmend zum Einsatz. So können Nutzer damit nicht nur für Einkäufe im Online-Handel, sondern auch an den inzwischen gängigen NFC-Terminals (Near Field Communication) an den Points of Sales (POS) im Handel zahlen. Die im mobilen Gerät hinterlegte digitale Karte kommuniziert dabei wie die kontaktlose Chipkarte über die NFC-Schnittstelle mit dem POS-Terminal.

Beim Onlinebanking ist der Einsatz von Anmeldenamen und die Eingabe eines 4 bis 6 stelligen PINs zur Anmeldung und einer TAN-Eingabe zur Freigabe der Transaktion quasi etabliert. Die Freigabe der Zahlungen am POS erfolgte bisher durch die PIN-Eingabe oder eine Unterschrift. Wahlweise bei kontaktlosen Kreditkarten unter bestimmten Voraussetzungen nur durch das Auflegen der Karte. Mit dem Einsatz von mobilen Geräten sind weitere Authentisierungsverfahren denkbar. So könnte sich der Nutzer statt an dem POS-Terminal auch an seinem eigenen mobilen Gerät identifizieren und die Zahlung damit autorisieren. Dieses Verfahren nennt sich Consumer Device Cardholder Verification Method oder kurz CDCVM. Der Nutzer verwendet die Entsperrmechanismen seines mobilen Gerätes zur Autorisierung. Dazu zählen die Eingabe der Geräte-PIN oder eines Passworts am eigenen Gerät oder die Nutzung biometrischer Verfahren (Fingerabdruck-, Iris-, Sprach- oder Gesichtserkennung), bei deren Einsatz die von dem mobilen Endgerät bereitgestellte Hardware wie beispielsweise der Bildschirm, die Kameras, Sensoren, Mikrofone etc. genutzt werden. Da die Mechanismen in die zugrunde liegende Plattform (das Betriebssystem) des mobilen Gerätes integriert sind und von ihr verwaltet werden, hat der Zahlungsdienstleister nicht die Kontrolle über das im Endgerät eingesetzte Verfahren. Die Erstellung von Fingerprintvorlagen oder die einer sicheren PIN liegt ganz im Ermessen des Nutzers.

Zusätzlich werden die biometrischen Merkmale und die PIN nicht direkt vom Zahlungsdienstleister verarbeitet. Die biometrischen Vergleichswerte verbleiben sowohl aus datenschutzrechtlicher als auch sicherheitstechnischer Sicht im mobilen Endgerät, sodass der Abgleich nur mit den im Speicher des mobilen Endgerätes hinterlegten Vergleichswerten erfolgt.

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

Grundsätzlich ist es wichtig, dem Nutzer nicht zusätzliche Sicherungsmethoden aufzuzwingen, sondern benutzerfreundliche und sichere Verfahren zu forcieren.

2.3.2 Lösungen und Angebote des BSI für Gesellschaft und Bürger

Neben dem umfangreichen Angebot von „BSI für Bürger“ nimmt der digitale Verbraucherschutz einen hohen Stellenwert der Lösungen des BSI für Gesellschaft und Bürger ein. In diesen Bereich fällt auch das IT-Sicherheitskennzeichen. Hier arbeitet das BSI derzeit in enger Abstimmung

mit den zuständigen Ministerien daran, Grundlagen für die Einführung eines großflächig einsetzbaren Sicherheitskennzeichens für IT-Produkte zu schaffen, um den Verbrauchern eine klare Hilfestellung bei der Kaufentscheidung an die Hand zu geben.

2.3.2.1 Verbraucher digital schützen

Die Gefährdungslage für Verbraucherinnen und Verbraucher ist auch in diesem Berichtszeitraum von größeren Vorfällen gekennzeichnet, die auf Sicherheitsmängel bei IT-Systemen und Online-Diensten zurückgehen. Für sichere Systeme und Dienste zu sorgen, die Verbraucherinnen und Verbraucher für Risiken zu sensibilisieren und zu einem sicheren Handeln zu befähigen, stellt daher eine entscheidende Herausforderung für den Verbraucherschutz auf dem Weg der Digitalisierung dar.

Das BSI hat mit dem Koalitionsvertrag der Bundesregierung aus dem Februar 2018 die neue Aufgabe des „Digitalen Verbraucherschutzes“ zugeordnet bekommen. Zukünftig soll diese Aufgabe auch im BSI-Gesetz explizit berücksichtigt werden. Zur Umsetzung des Themas wurde im April 2019 eine Projektgruppe „Digitaler Verbraucherschutz“ eingerichtet. Deren Mitglieder werden aufbauend auf den bisherigen Arbeiten abteilungsübergreifend die Aktivitäten im Feld des Verbraucherschutzes vorantreiben.

Das BSI sieht sich mit seiner technischen Expertise als kooperativ agierendes Kompetenzzentrum für IT-Sicherheit im Bereich der Consumer-Produkte. Ein besonderer Mehrwert wird in der Verknüpfung von Kompetenzen und Befugnissen gesehen, um so einen größtmöglichen Gewinn an Sicherheit für Verbraucherinnen und Verbraucher bei der Nutzung von vernetzten Geräten zu erzielen. Beispielhaft zeigt dies die Zusammenarbeit mit der Verbraucherzentrale NRW: Die Untersuchung und das gemeinsame Vorgehen gegen unsichere Smartphones, die Zusammenarbeit bei vernetztem Spielzeug und bei Smart-Home-Geräten oder dem Phishing-Radar zeigen einen Ausschnitt der Themen der Kooperation. Das BSI wird die Zusammenarbeit mit etablierten Akteuren im Verbraucherschutz noch weiter ausbauen und so zu einem effektiven Schutz für Verbraucherinnen und Verbraucher in der digitalen Welt beitragen.

2.3.2.2 IT-Sicherheitskennzeichen

Bereits in der 2016 veröffentlichten Cyber-Sicherheitsstrategie für Deutschland hat das BMI die Einführung eines Gütesiegels für IT-Sicherheit angekündigt. Es soll dem Verbraucher ermöglichen, IT-Sicherheit zum Bestandteil seiner Kaufentscheidung zu machen. Das Vorhaben wurde im Koalitionsvertrag 2018 bestätigt.

Bereits heute gehört die Zertifizierung von IT-Sicherheitsprodukten zu den etablierten Verfahren des BSI. Hersteller können ihre Produkte beim BSI zertifizieren lassen und damit nachweisen, dass ihre Produkte in Bezug auf IT-Sicherheit dem Stand der Technik entsprechen. Durch das BSI zertifizierte Produkte finden meist im Rahmen von Digitalisierungsprojekten des Bundes ihre Anwendung. Bislang richten sich Zertifikate an professionelle Anwender. Hiervon muss sich eine Lösung für den Verbraucher unterscheiden, z. B. durch eine verbrauchergerechte Darstellung der Sicherheitseigenschaften und deren Geltungsbereich.

Mittlerweile hat das BMI unter dem Namen „IT-Sicherheitskennzeichen“ ein neues Verfahren für Produkte und Dienstleistungen aus dem Verbrauchermarkt konzipiert. Die Ausgestaltung des Verfahrens wird derzeit im BSI geplant.

Voraussetzung für ein IT-Sicherheitskennzeichen sind transparente Kriterien, auf deren Basis ein Zertifikat erteilt oder ein IT-Sicherheitskennzeichen geführt werden kann. Diese Kriterien werden u. a. in Form von Protection Profiles oder Technischen Richtlinien durch das BSI veröffentlicht und werden zukünftig durch Anforderungen für IT-Produkte des Verbrauchermarktes erweitert. Hierbei können auch branchenabgestimmte Standards zur Anwendung kommen, welche das BSI als geeignet ansieht.

Parallel dazu muss ein Rechtsrahmen etabliert werden, der es ermöglicht, IT-Sicherheitskennzeichen so zu überwachen, dass Verbraucher ihnen vertrauen können. Dieser Rechtsrahmen soll im IT-Sicherheitsgesetz 2.0 umgesetzt werden.

Insgesamt ergibt sich ein dreistufiger Lebenszyklus eines IT-Sicherheitskennzeichens:

1. Stand der Technik festlegen und fortschreiben,
2. Einhaltung des Stands der Technik bestätigen,
3. Rechtmäßigkeit des Umlaufs überwachen.

Die ersten Produkte, die mit einem IT-Sicherheitskennzeichen für den Verbraucher ausgestattet werden sollen, sind Breitband-Router.

2.3.2.3 Gesellschaftlicher Dialog für Cyber-Sicherheit

Die mit dem digitalen Wandel verbundenen gesellschaftlichen Herausforderungen im Themenfeld Cyber-Sicherheit können nur mit einem gesamtgesellschaftlichen Ansatz bewältigt werden. Ziel des BSI ist es daher, Cyber-Sicherheit für, mit und in der gesamten Gesellschaft zu gestalten.

Bereits seit dem Jahr 2016 intensiviert das BSI im Rahmen eines partizipativ ausgerichteten Multistakeholder-Ansatzes den gesellschaftlichen Dialog zum Thema Cyber-Sicherheit. Der Dialogprozess, der im Rahmen des Projekts „Institutionalisierung des gesellschaftlichen Dialogs“ geführt wird, umfasst eine jährlich stattfindende Denkwerkstatt und themenspezifische Workshops, Veranstaltungen und ergebnisorientierte Arbeitsgruppen.

Die Denkwerkstatt, die im Februar 2019 zum fünften Mal stattgefunden hat, bringt die unterschiedlichen Stakeholder aus den Bereichen Zivilgesellschaft, Kultur/Medien, Wissenschaft, Staat und Wirtschaft auf einer Veranstaltung zusammen und bildet eine Plattform für die Diskussion aktueller Themen der Cyber-Sicherheit.

Mit der zweiten Phase des Projekts wurde im Sommer 2018 ein wichtiger Schritt in Richtung der Vertiefung und Verstärkung des gesamtgesellschaftlichen Dialogs getan. Ausgehend von der Teilnehmerschaft der Denkwerkstätten wurde im Juni 2018 eine aus den verschiedenen gesellschaftlichen Gruppen paritätisch besetzte „Kerngruppe“ gebildet, die noch bis September 2019 drei selbst gewählte Themen erarbeitet:

Thema 1: Institutionalisierung des gesellschaftlichen Dialogs: Die Kerngruppe hat auf Grundlage eines partizipativen Vorgehens erarbeitet, welches Modell für die Institutionalisierung des Dialogs denkbar ist und das Modell dem BSI präsentiert.

Thema 2: Mapping zivilgesellschaftlicher Akteure: Aufbauend auf Rechercheergebnissen und qualitativen Interviews soll das Mapping eine übersichtliche Zusammenstellung zivilgesellschaftlicher Akteure im Feld Cyber-Sicherheit, ihrer wesentlichen Aktivitäten, Zielsetzungen und Vernetzungsstrukturen beinhalten.

Thema 3: Vernetzungstag zum Thema Wissensvermittlung: Es wird eine Veranstaltung konzipiert und durchgeführt, die zur Vernetzung der Akteure im Feld Wissensvermittlung und Cyber-Sicherheit beitragen, Synergien

schaffen und Bedarfe bei der Erstellung von Informationsmaterialien verdeutlichen soll.

Der gesamtgesellschaftliche Dialog bleibt für das BSI weiterhin ein zentrales Instrument, um den Austausch unterschiedlicher Sichtweisen auf das Thema Informationssicherheit zu fördern und zu einer Öffnung im Sinne der verschiedenen Zielgruppen beizutragen.

Aufbauend auf bestehenden und noch zu erwartenden Projektergebnissen und in dem Bewusstsein, dass Cyber-Sicherheit nur in einem gesamtgesellschaftlichen Dialog gestaltet werden kann, ist das BSI bestrebt, den Dialog mit den verschiedenen Zielgruppen über das Projekt hinaus weiter zu vertiefen und zu verstetigen.

2.3.2.4 Bürger-Services des BSI

Das BSI bietet ein breites Informations- und Beratungsangebot für Privatanwender und -anwenderinnen unter dem Namen „BSI für Bürger“ an. Herzstück ist die Website www.bsi-fuer-buerger.de, auf der Informationen zu Risiken und Schutzmechanismen im Cyber-Raum bereitgestellt werden. Im Fokus stehen Empfehlungen für ein sicheres und selbstbestimmtes Handeln im digitalen Raum. Auf aktuelle Cyber-Sicherheitsvorfälle wird direkt reagiert und Handlungsempfehlungen zu Sicherheitslücken oder Schadsoftware-Wellen werden gegeben. Die oftmals komplexen Themen sind einfach und verständlich aufgearbeitet als Checklisten, informative Grafiken und interaktive Quizze sowie in Experten-Interviews und animierten Videos.

Mit dem kostenlosen Warn- und Informationsdienst „Bürger-CERT“ informiert das BSI in Form von Technischen Warnungen oder mit dem vierzehntägig erscheinenden Newsletter „Sicher · Informiert“ über Schwachstellen und gibt entsprechende Hilfestellungen. Derzeit nutzen rund 105.000 Abonnenten und Abonnentinnen dieses Angebot.

Eine fünfteilige Broschüren-Reihe befasst sich mit dem digitalen Basisschutz und gibt praxistaugliche Tipps zu den Themen Surfen, Sicher mobil unterwegs, Soziale Medien, Internet der Dinge und Cloud. Die Broschüren stehen auf der Website zum Download zur Verfügung und können auch auf Nachfrage bestellt werden.

Flankierend zur Website präsentiert sich das BSI auf den bürgernahen Social-Media-Plattformen Facebook (rund 39.000 Abonnenten) und YouTube (seit März 2019, rund 450 Abonnenten im Juni 2019). 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.

Um Synergien zu nutzen, arbeitet „BSI für Bürger“ mit zahlreichen Organisationen und Initiativen zusammen, die sich ebenfalls mit der Cyber-Sicherheit für Bürgerinnen und Bürger befassen. So gibt es eine rege Zusammenarbeit mit den Verbraucherzentralen, z. B. eine gemeinsame Kommunikation von Themen bei anstehenden Warnungen. Mit der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK) wurde anlässlich des Doxing-Vorfalles Ende 2018/Anfang 2019 über Identitätsdiebstahl informiert. Neben einer gemeinsamen Pressemitteilung wurden in verschiedenen Fallbeispielen Wege aufgezeigt, wie Cyber-Kriminelle an sensible Daten kommen. Zusammen mit dem Verein Deutschland sicher im Netz (DsiN) wurde eine „Cyber-Fibel“ erarbeitet, die Orientierung für Multiplikatoren in der Aufklärungsarbeit geben soll. Andere Kooperationen – beispielsweise mit der Bundesarbeitsgemeinschaft der Senioren-Organisationen (BAGSO) – wurden initiiert und unterstützen zukünftig bei der zielgruppenspezifischen Erarbeitung von Aufklärungs- und Sensibilisierungsmaßnahmen.

Europäischer Aktionsmonat

Auch 2018 beteiligte sich das BSI als nationaler Koordinator am European Cyber Security Month (ECSM). Mit knapp 200 Aktionen und Veranstaltungen von über 100 Partnern konnte die Bedeutung der Cyber-Sicherheit in Deutschland weiter in die Öffentlichkeit getragen werden. Zu den teilnehmenden Partnern gehörten Unternehmen, Ministerien und Behörden, Industrie- und Handelskammern (IHK), Wirtschaftsverbände, Hochschulen und Universitäten sowie auch die unter dem Dach der ACS kooperierenden Cyber-Sicherheitsinitiativen.

Zudem hat sich „BSI für Bürger“ mit eigenen Aktionen beteiligt: Auf der Website, auf Facebook und Twitter rückten die Grundlagen der IT-Sicherheit für das eigene Zuhause in den Mittelpunkt.

2.4 Internationales und Wissenschaft sowie ausgewählte neue Technologien

Als die Cyber-Sicherheitsbehörde des Bundes ist das BSI in den Cyber-Sicherheitsgremien der EU und NATO vertreten und gestaltet so die Cyber-Sicherheit auch auf internationaler Ebene mit. Das BSI steht zudem im regen Austausch mit der deutschen Cyber- und IT-Sicherheitsforschung.

2.4.1 Internationales

Das internationale Engagement des BSI ist stark geprägt von seiner Rolle als verantwortliche Cyber-Sicherheitsbehörde des Bundes. Um dieser Aufgabe und Verantwortung auch international nachzukommen, wurde im vergangenen Jahr der Wirkungskreis des BSI in Richtung von Gesprächspartnern bzw. Institutionen im Ausland erweitert. Im Rahmen von Konferenzteilnahmen, bilateralen Gesprächen und der Einbringung in Gremien und relevanten Gesetzesvorhaben hat die Vernetzung und Zusammenarbeit mit Behörden, wirtschaftlichen Akteuren, der Wissenschaft und Zivilgesellschaft im Ausland zugenommen. Dabei standen die Sicherung der technologischen Beurteilungsfähigkeit und die internationale Ausrichtung des BSI im Vordergrund der internationalen Aktivitäten.

Die Tätigkeitsschwerpunkte und Prioritäten des internationalen BSI-Engagements lagen dabei in den Handlungsfeldern EU, NATO sowie bilaterale und multilaterale Beziehungen. Schwerpunkte der bilateralen Zusammenarbeit waren die Vertiefung der Partnerschaften im europäischen und NATO-Umfeld. Vertrauensvolle Kooperationen mit engen Partnern ermöglichen dem BSI unter anderem den schnellen und zielgerichteten Informationsaustausch bezüglich Detektion und Reaktion von Cyber-Angriffen. Auch mit diesem Ziel wurden im letzten Jahr einige neue Kooperationen etabliert oder vorhandene intensiviert, beispielsweise mit asiatischen Partnern.

Als zentrales Gesetzesvorhaben und zugleich Meilenstein auf EU-Ebene wurde der sog. Cybersecurity Act zur Schaffung eines neuen, permanenten Mandats für die Europäische Agentur für Netz- und Informationssicherheit (ENISA) sowie zur Einführung eines einheitlichen europäischen Cyber-Sicherheitszertifizierungsrahmens für IKT-Produkte, -Dienstleistungen und -Prozesse seitens BSI mitgestaltet.

Auch jenseits der direkten Beziehungen zu engen Partnern wird das BSI im Ausland zunehmend als Kompetensträger für Cyber-Sicherheit und als anerkanntes IT-Sicherheitskompetenzzentrum wahrgenommen.

2.4.1.1 Smart Borders (Biometrie)

Ein konkretes Beispiel für die internationale Zusammenarbeit ist die Smart-Borders-Initiative der EU-Kommission. Mit dieser wurde u. a. die Einführung eines europäischen Ein-/Ausreiseregisters (Entry-Exit-System, EES) für Reisende aus Drittstaaten angestoßen. Mit dem EES wird die Digitalisierung der ehemals in Reisedokumenten beim Grenzübergang aufgetragenen Ein- und Ausreisestempel

in einer zentralen EU-Datenbank geschaffen, um u. a. irregulärer Migration zu begegnen und Informationen über Aufenthaltsüberziehungen zu erhalten. Auch das Gesichtsbild und die Fingerabdrücke von Reisenden aus Drittstaaten werden zukünftig im EES als biometrische Merkmale zur zweifelsfreien Wiedererkennung der Reisenden beim Grenzübergang abgelegt.

2.4.1.1.1 Sachstand Smart Borders Projekt

Neben dem EES umfasst das Smart-Borders-Vorhaben auch die Einführung des Europäischen Reiseinformations- und -authorisierungssystems (European Travel Information and Authorisation System, ETIAS). Seit Verabschiedung der Verordnungen über die Einführung des EES und ETIAS begleitet das BSI gemeinsam mit den nationalen Behörden Bundespolizei, Bundesverwaltungsamt, Bundeskriminalamt und Informationstechnikzentrum Bund insbesondere die nationale, aber auch die internationale Ausgestaltung und Umsetzung des europäischen Smart-Borders-Vorhabens. Das BSI ist dabei Teil der nationalen behördenübergreifenden Projektgruppe Smart Borders unter Federführung des BMI.

Im letzten Jahr hat das BSI umfangreich an der europäischen Verordnungsgebung mitgewirkt und zahlreiche Umsetzungsrechtsakte mit ausgestaltet. Darüber hinaus wurden im Rahmen der nationalen Konzeption mehrere Technische Richtlinien sowohl für die hoheitliche Prüfung von elektronischen Reisedokumenten als auch für die biometrischen Verfahren der Grenzkontrolle erstellt und veröffentlicht. Diese dienen als technologische Basis für die Implementierung und Zertifizierung neuer Grenzkontrollsysteme im Rahmen der zukünftigen Grenzkontrollprozesse für EES und ETIAS. Hierbei wird insbesondere die Umsetzung und Spezifikation von Systemen zur Selbsterfassung von biometrischen Merkmalen durch Drittstaatsreisende im Vorfeld der eigentlichen Grenzkontrolle unterstützt. Ziel ist es, die Sicherheitsvorgaben an eine effektive Identitätsfeststellung von Reisenden für die operative Praxis effizient umzusetzen.

Um die Weiterentwicklung der neuen Grenzkontrollsysteme im operativen Betrieb auch in Zukunft eng zu begleiten, hat das BSI eigens ein Fachreferat für den Bereich Smart Borders eingerichtet.

2.4.1.1.2 Schulung für Frontex Schengen-Evaluatoren

Der Einsatz biometrischer Systeme gehört mittlerweile zum Standard-Repertoire der Informationssicherheit – mit einem stetig expandierenden Anwendungsbereich,

welcher von der Smartphone-Authentifizierung bis hin zu hoheitlichen Systemen in der Grenzkontrolle reicht. Aufgrund ihrer Komplexität lassen sich die tatsächliche Performanz und insbesondere die Überwindungssicherheit solcher Systeme allerdings nur durch umfangreiche Tests und viel Expertise ermitteln. Das BSI hat sich über mehr als 15 Jahre eine international anerkannte Kompetenz erarbeitet, insbesondere auf dem Gebiet der Schwachstellenanalyse in der Biometrie und der Entwicklung von Fälschungserkennungs-Technologien. Als querschnittlicher Dienstleister für die hoheitlichen und nicht-hoheitlichen Bedarfsträger ist das BSI bestrebt, diese Kompetenz in der ganzen Bandbreite von technologischen Grundlagen, Entwicklung neuer Technologien, Beratung von Herstellern bis hin zur Beratung und Schulung von zentralen Endanwendern anzubieten. Damit will das BSI einen nachhaltigen Beitrag zur Verfügbarkeit von sichereren und zuverlässigeren Systemen sowie zur fachgerechten Nutzung im Feld leisten. Im Rahmen der nationalen Umsetzung der Smart Borders/EES-Initiative der EU (vgl. Kapitel 2.4.1.1.1 Sachstand Smart Borders Projekt) ist die Durchführung von Beratungs- und Schulungsmaßnahmen für die Bundespolizei daher eine der Aufgaben des BSI.

Die Europäische Agentur für die Grenz- und Küstenwache (Frontex) hat das BSI zum zweiten Mal damit beauftragt, eine spezielle Schulung für Frontex Schengen-Evaluatoren durchzuführen. Dabei ging es um die Themenbereiche „biometrische und nicht-biometrische Angriffsvektoren auf Grenzkontrollsysteme“, „Dokumentenechtheitsprüfung“, „Übersicht über das Entry-Exit-System der EU“ sowie Selbsterfassungssysteme. Die Schulungsveranstaltung mit dem Titel „Vulnerability Assessment and Testing for Automated Border Control Systems“ fand im März 2019 zum ersten Mal in den Räumlichkeiten des

„Biometrie Evaluations Zentrums“ (BEZ) auf dem Campus der Hochschule Bonn-Rhein-Sieg (H-BRS) statt (siehe auch LinkedIn-Beitrag von Frontex unter <https://www.linkedin.com/company/frontex/>). Die Teilnehmer waren von ihren jeweiligen Staaten offiziell entsandte Schengen-Evaluatoren, die zumeist auch Verantwortung für Teile der jeweiligen nationalen Umsetzungen der Smart Borders/EES-Initiative übernommen hatten.

Ein besonderer Fokus einer zweitägigen BSI-Schulung lag auf der Gefahr, die von Fälschungsangriffen auf dem Gebiet der Gesichts- und Finger-Biometrie sowie der elektronischen Ausweisdokumente ausgehen kann, und auf den derzeit möglichen organisatorischen und technischen Erkennungs- und Gegenmaßnahmen. Nach dem positiven Feedback hat Frontex angekündigt, die Kooperation mit dem BSI zu vertiefen. Eine weitere Schulung ist für November 2019 geplant.

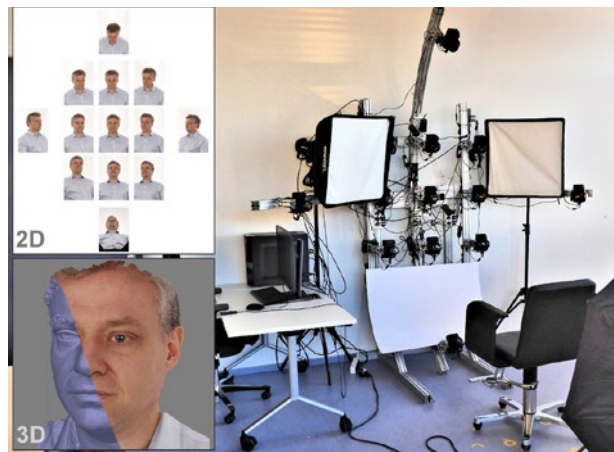


Abbildung 15 Portrait-Studio für Referenzaufnahmen von Testpersonen. Mit speziell angeordneten DSLR-Kameras werden zugleich 13 Multiposen-Fotos, d. h. Aufnahmen aus verschiedenen Blickwinkeln, und ein hochdetailliertes 3D-Modell erfasst. Im Rahmen der Frontex-Schulungen wurden die Teilnehmer hier abgelichtet, um für die Schwachstellenanalyse gemorphte Bilder zu erstellen.



Abbildung 14 (links) Testraum zur Evaluation hoheitlicher Grenzkontrollsysteme, in dem Teile der Frontex-Schulung stattfanden. An den EasyPass-Systemen konnten die Teilnehmer einerseits den Normalbetrieb der Schleusen beobachten (Betrieb wie an den deutschen Grenzen) und andererseits Überwindungsangriffe mit gefälschter Biometrie übernehmen. (rechts) Beispiele von Prüfmitteln zur Schwachstellenanalyse von Gesichts- und Finger-biometrischen Systemen, wie sie in der Frontex-Schulung zum Einsatz kamen.

2.4.2 Zusammenarbeit mit der Wissenschaft

Von der Zuverlässigkeit der Informations- und Kommunikationstechnik (IKT) sowie dem Vertrauen in die Sicherheit der IKT-Systeme hängen inzwischen weite Bereiche des gesellschaftlichen und wirtschaftlichen Lebens ab. Da sich das Innovationspotenzial im Umfeld der IKT zunehmend vergrößert, geht damit auch eine steigende Gefährdung durch IT-Sicherheitsrisiken einher, weshalb neben der eigentlichen Technologieforschung die IT-Sicherheitsforschung immer mehr an Bedeutung gewinnt.

IT-Sicherheitsforschung ist ein wichtiger Baustein, um auf neuen Entwicklungen basierende innovative IT-Sicherheitsverfahren auszuarbeiten. Durch eine frühzeitige Einbindung der IT-Sicherheit als integraler Bestandteil in Technologieentwicklungen trägt IT-Sicherheitsforschung dazu bei, das Sicherheitsniveau in Deutschland zu erhöhen, Bürgerinnen und Bürger sowie Unternehmen und den Staat vor Angriffen präventiv und nachhaltig zu schützen und die Wettbewerbsfähigkeit des Standortes Deutschland zu stärken.

Das BSI beteiligt sich an der Fortentwicklung der nationalen und europäischen IT-Sicherheitsforschung. Hierunter fallen neben der Mitgestaltung nationaler und EU-weiter Forschungsprogramme auch Beratungsaktivitäten auf politischer Ebene, um eine nachhaltige IT-Sicherheitsforschung zu etablieren und weiter auszubauen. Relevante Schwerpunkte und aktuelle Forschungsthemen werden aktiv durch eigene Projekte mit den großen Zentren der IT-Sicherheitsforschung in Deutschland sowie weiteren Hochschulen und verschiedenen Fraunhofer-Instituten vorangetrieben. Zudem berät das BSI das Bundesministerium für Bildung und Forschung (BMBF) bei der Auswahl von Forschungsvorhaben im Rahmen von Gutachtertätigkeiten, unterstützt als assoziierter Partner ausgewählte Forschungsprojekte mit IT-Sicherheitsbezug und begleitet fachlich die deutschen Kompetenzzentren für IT-Sicherheitsforschung sowie weitere IT-Sicherheitsforschungseinrichtungen mit herausgehobener Bedeutung. Vertreter des BSI und der Forschungsstandorte der Cyber- und IT-Sicherheit in Deutschland führen regelmäßig Fachgespräche, um sich zu neuesten Forschungsergebnissen auszutauschen. So wurden Expertenworkshops und Dialogveranstaltungen mit Vertretern der IT-Sicherheitsforschungslandschaft zu Themen mit herausgehobener Bedeutung für die IT-Sicherheit veranstaltet, wie maschinelles Lernen und Quantentechnologien.

Weiterhin unterstützt das BSI personell den Aufbau und die Ausgestaltung der in Planung befindlichen „Agentur für Innovation in der Cyber-Sicherheit“, die Forschungs-

und Entwicklungsvorhaben sowie Schlüsseltechnologien mit hohem Innovationspotenzial auf dem Gebiet der Cyber-Sicherheit fördern und finanzieren soll. So können zukünftig in Bezug auf risikobehaftete aber auch langfristig orientierte, grundlegende und damit potenziell bahnbrechende Forschungsvorhaben beauftragt und in Bereichen eigener Expertise Projekte der Agentur als Projektpartner begleitet werden.

2.4.3 Kryptografie

In der Kryptografie ist das beherrschende Thema in den letzten Jahren die Entwicklung und Standardisierung von Post-Quanten-Kryptografie, d. h. von kryptografischen Verfahren, die resistent gegen Angriffe mit Quantencomputern sind. Das US-amerikanische National Institute for Standards and Technology (NIST) hat im November 2016 einen Auswahlprozess zur Standardisierung von quantencomputer-resistenten kryptografischen Verfahren gestartet.

Bis Ende November 2017 konnten Verfahren vorgeschlagen werden, die anschließend im Rahmen eines Workshops im April 2018 vorgestellt wurden. Von den 82 eingereichten Verfahren sind nach einer ersten Analysephase als Kandidaten für die zweite Runde nur noch 17 Verschlüsselungs- oder Schlüsseltransportverfahren und neun Signaturverfahren übrig. Bei den Verschlüsselungs- oder Schlüsseltransportverfahren haben sich im Wesentlichen gitterbasierte und codebasierte Verfahren durchgesetzt, bei den Signaturverfahren vor allem multivariante und gitterbasierte Verfahren.

Mit Bekanntgabe der Kandidaten für die zweite Runde hat eine zweite Analysephase begonnen. Die Autoren der Verfahren hatten bis Mitte März 2019 Zeit, Anpassungen an ihren Einreichungen vorzunehmen. Die aktualisierten Dokumente sind seit Anfang April auf der Webseite von NIST abrufbar. Ende August fand in Santa Barbara (USA) ein zweiter Standardisierungsworkshop statt. Erste Draft-Standards werden frühestens in zwei Jahren veröffentlicht werden.

Neben der Entwicklung von quantencomputer-resistenten kryptografischen Verfahren ist auch die Anpassung von kryptografischen Protokollen an die neuen Verfahren eine große Herausforderung. Beispielsweise ist ein Hauptproblem bei der Verwendung von quantencomputer-resistenten Schlüsseleinigungsverfahren im Internet Key Exchange (IKE) Protokoll, dass bei vielen dieser Verfahren die öffentlichen Schlüssel deutlich größer sind als bei den heute eingesetzten Verfahren und nicht in die initiale IKE-Nachricht passen.

Auch Standardisierungsgremien wie das Europäische Institut für Telekommunikationsnormen (ETSI) beschäftigen sich intensiv mit Quantenthemen. Eine ETSI-Arbeitsgruppe zu Quantum-Safe Cryptography (ETSI TC Cyber QSC) untersucht neben quantencomputer-resistenten Verfahren auch praktische Aspekte der Migration auf Post-Quanten-Kryptografie wie beispielsweise Anforderungen an quantensichere Virtuelle Private Netzwerke.

2.4.4 Blockchain-Technologie

Im Bereich der Informationssicherheit gehört Blockchain gegenwärtig zu den am häufigsten diskutierten Themen. Wie bei allen neuen Technologien sollte auch bei der Blockchain-Technologie Sicherheit von Anfang an mit berücksichtigt 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 die Eckpunkte des BSI zur Blockchain-Technologie vertieft, die bisherigen Diskussionen aufgreift und Entwickler und potenzielle Nutzer von Blockchain-Lösungen dabei unterstützt, 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 erstellen und danach ausgewählte Produkte aus verschiedenen Produktklassen exemplarisch evaluieren lassen.

2.4.5 Künstliche Intelligenz

Das Gebiet „Künstliche Intelligenz“ (KI) entwickelt sich seit Jahren stetig fort. Insbesondere durch die Steigerung der Rechenleistung, Entwicklung neuer Algorithmen und Verfügbarkeit großer Mengen von Daten konnten sich KI-Systeme in den letzten Jahren in unterschiedlichen Be-

reichen erfolgreich durchsetzen. Bekannte Anwendungen reichen von Textanalyse und Übersetzung über Bild- und Spracherkennung bis hin zum autonomen Fahren. Auch im Bereich der Cyber-Sicherheit spielen KI-Algorithmen eine zunehmend wichtigere Rolle.

Die neuen Methoden werden im BSI permanent evaluiert, in einigen Anwendungsbereichen weiterentwickelt und bereits eingesetzt. Das BSI hat an einem Beispiel (<https://eprint.iacr.org/2019/037>) gezeigt, dass KI-Methoden die Kryptoanalyse von Verschlüsselungsverfahren beschleunigen können. Auch bzgl. der Detektion von Cyber-Angriffen auf IT-Systeme und IT-Infrastrukturen evaluiert das BSI die Verwendung von KI-Systemen. Weitere Anwendungsbereiche sind Authentisierungsverfahren im Kontext hoheitlicher Dokumente und automatische Textverarbeitung zur effizienten Lagebilderstellung.

Im Berichtszeitraum wurde ein neues Referat eingerichtet, das sich als technisches Kompetenzzentrum mit Fragen aus dem Bereich Künstliche Intelligenz insbesondere im Bereich IT-Sicherheit beschäftigt und als zentraler Ansprechpartner für das BSI und die Bundesverwaltung dient. Dies spiegelt die wachsende Bedeutung des Themas wider. Denn einerseits kann durch KI-Methoden die IT-Sicherheit erhöht werden, andererseits entstehen durch die Nutzung von KI-Systemen neuartige Angriffsvektoren. Diese müssen rechtzeitig erkannt und analysiert sowie Gegenmaßnahmen entwickelt werden, damit Systeme mit KI-Komponenten robust und sicher gestaltet werden können.

Im Fokus der Arbeit des BSI stand im Berichtszeitraum das Thema Maschinelles Lernen und Künstliche Intelligenz. So wird im BSI die Expertise bei KI-basierten Ansätzen in der Seitenkanalanalyse weiter ausgebaut und es wird untersucht, unter welchen Voraussetzungen diese den konventionellen Verfahren überlegen sind. Seitenkanalanalysen sind u. a. zentrale Bausteine von Com-mom-Criteria-Evaluierungen von Chipkarten.

BSI beim internationalen Seitenkanalwettbewerb

Die international renommierte CHES (Conference on Cryptographic Hardware and Embedded Systems) hat im Sommer 2018 einen Seitenkanalwettbewerb ausgerichtet. Ein Team des BSI hat an zwei Teildisziplinen teilgenommen und diese gewonnen. Aufgabe war es, aus den Stromprofilen, welche von einer geschützten AES-Implementierung auf einem Mikrocontroller aufgenommen wurden, die verwendeten AES-Schlüssel zu rekonstruieren. Das Team gewann durch die Kombination von maschinellem Lernen und einem klassischen Lösungsansatz (<https://eprint.iacr.org/2019/094>).

i DAS BSI ALS ARBEITGEBER: WIR WOLLEN DEINE DIGITALE SEITE

Nachdem das BSI bereits in den vergangenen Jahren vor der Herausforderung stand, einen Personalaufwuchs von mehr als 40 % zu bewältigen, fand diese Entwicklung ihre Fortsetzung in der Zuweisung von 100 zusätzlichen Stellen für das Jahr 2018 und weiteren 350 Stellen für das Jahr 2019. Erneut war und ist die größte Herausforderung, die stark umworbene Zielgruppe der Fachkräfte aus dem MINT-Bereich für die Arbeit im BSI zu begeistern. Zusätzlich erforderte die Einarbeitung und Integration der neu gewonnenen Kolleginnen und Kollegen besondere Aufmerksamkeit und Anstrengung der gesamten Organisation.

Die Botschaft: Der beliebteste IT-Arbeitgeber des öffentlichen Sektors

Im Berichtszeitraum konnte das BSI einen besonderen Erfolg verzeichnen: Studierende und Absolventen/-innen aus IT-Studiengängen wählten die Behörde auf den 14. Platz deutschlandweit und somit zum beliebtesten IT-Arbeitgeber des öffentlichen Sektors (Trendence Absolventen Barometer, IT-Ausgabe 2018). Diese Botschaft galt es nun zu nutzen, um so noch mehr Absolventen/-innen und (Young) Professionals zu erreichen. Dazu wurden neben der bereits etablierten Kampagne „Was wir wollen: Deine digitale Seite“ weitere Wege der Rekrutierung initiiert. Neben dem persönlichen Kontakt auf Hochschulveranstaltungen oder bei Exkursionen ins BSI wurde ein sogenanntes „Recruitment Format“ entwickelt, welches eine interessierte Person spielerisch zum Arbeitgeber BSI führt. Des Weiteren soll eine zusätzliche Form des Storytellings, in welcher die spannenden und sinnhaften Aufgaben in Ausschnitten dargestellt werden, interessierten Fachkräften Einblicke in das Amt gewähren. Zuletzt wurden auch die Kampagnenmotive erweitert: Neben den bisher verwendeten Gegenständen aus der Lebenswelt von IT-Fachkräften treten demnächst reale Beschäftigte des BSI mit ihrer persönlichen und digitalen Seite auf.

Viele neue Gesichter: Einarbeitung und Integration

Um die neuen Mitarbeiterinnen und Mitarbeiter in das BSI zu integrieren, wurden aus mehreren Modulen bestehende, verpflichtende Einführungsveranstaltungen initiiert, um sowohl die Fachaufgaben in den unterschiedlichen Bereichen allen Mitarbeitenden näher zu bringen und somit einen Blick für das große Ganze zu erzeugen, als auch Verwaltungsgrundlagen für die MINT-Fachkräfte zu vermitteln, die oftmals noch keine Berührungspunkte mit diesen Anforderungen hatten. Weiterhin wurden Inhouse-Schulungen zu grundsätzlichen methodischen sowie sozialkompetenzrelevanten Themen angeboten, wie Projektmanagement, Präsentation, Resilienz, Konfliktmanagement, Zeitmanagement, Kommunikation und Kooperation, Verhandlungsführung und Stressmanagement. Hierin spiegeln sich unterschiedliche überfachliche Anforderungen an neue und erfahrenere Mitarbeiterinnen und Mitarbeiter wider. Vor allem die bereichsübergreifende Kooperation und Zusammenarbeit wird forciert, aber auch BSI-spezifische Vorgehensweisen z. B. im Projektmanagement. Weiterhin wurden neben dem ohnehin etablierten Führungskräftenachwuchsprogramm speziell für Führungskräfte Schulungen in den Bereichen Konfliktmanagement, Führung auf Distanz, gemeinsame Ziele, Personalrecht, Feedbackgespräche und allgemeiner Verwaltung angeboten. Hierbei wurde auch stets der Aspekt der gesunden Führung mit einbezogen, um auch das Thema Gesundheitsmanagement als Führungsthema zu verankern.

Neben den Grundlagenschulungen für Mitarbeiter und Führungskräfte entsendet das BSI, den fachlichen Anforderungen entsprechend, die Mitarbeiter in großem Umfang zu externen fachspezifischen Schulungen.

3 Gesamtbewertung und Fazit

3 Gesamtbewertung und Fazit

Die technologischen Entwicklungen unserer Zeit sorgen für eine große Dynamik, die Staat, Wirtschaft, Gesellschaft und jeden Einzelnen gleichermaßen erfasst. Die Herausforderung ist, mit dieser Dynamik Schritt zu halten, damit sie in geordneten Bahnen sicher abläuft und allen Zielgruppen größtmöglichen Nutzen bringen kann. Die im vorliegenden Lagebericht beschriebenen Erkenntnisse und Entwicklungen bestätigen die Erwartung, die das BSI bereits im Lagebericht des Vorjahres formuliert hatte: Schon 2018 hatte das BSI vor einer neuen Qualität an Cyber-Angriffen gewarnt, und genau diese haben stattgefunden. Schon 2018 hatte das BSI die Schadsoftware Emotet als eine der größten Cyber-Bedrohungen der Welt bezeichnet und vor einer professionellen Weiterentwicklung gewarnt. Auch darin sieht sich das BSI nach den gezielten Ransomware-Angriffen auf Unternehmen im aktuellen Berichtszeitraum bestätigt.

Auch unabhängig von Emotet zählt Ransomware nach wie vor zu den größten Bedrohungen für Unternehmen, Behörden und andere Institutionen sowie für Privatanwender. Immer wieder kommt es zu Komplettausfällen von Rechnern und Netzwerken, aber auch von Produktionsanlagen. Auch Einrichtungen des Gemeinwesens sind zuletzt wiederholt Ziel von Ransomware-Angriffen geworden. Dazu zählen beispielsweise Krankenhäuser in Deutschland genauso wie Kommunalverwaltungen in den USA. Ein Trend dabei ist der gezielte Angriff auf zentrale Dienstleister, über die dann deren Kunden oder angeschlossene Netzwerke mit Ransomware infiziert werden können. Das Schadenspotenzial ist enorm: Die Kosten u.a. für Produktionsausfälle, Datenverlust, Bereinigung und Wiederherstellung der Systeme gehen zum Teil in die Millionen, Dienstleistungen von Einrichtungen des Gemeinwesens sind nicht oder nur eingeschränkt verfügbar.

Die vom BSI prognostizierte neue Qualität der Cyber-Angriffe drückt sich auch durch mehrere große Fälle von Identitätsdiebstahl aus, die 2018/2019 für Aufmerksamkeit sorgten. Unter anderem betroffen waren Anwender von Sozialen Netzwerken und Kunden einer großen Hotelkette, hunderte Prominente und Politiker aus Deutschland im Zuge des Doxing-Vorfalles, der im Januar 2019 bekannt wurde, sowie hunderte Millionen andere Internetnutzer, deren Daten im Zuge der als „Collection #1“ bis „Collection #6“ bezeichneten Vorfälle öffentlich im Internet verfügbar gemacht wurden. Bemerkenswert dabei ist nicht nur die Häufung der Vorfälle, sondern auch die riesige Menge der abgeflossenen und im Internet veröffentlichten persönlichen Daten.

Nach wie vor ist eine hohe Dynamik der Angreifer bei der (Weiter-)Entwicklung von Schadprogrammen und Angriffswegen festzustellen. Rund 114 Millionen neue Schadprogramm-Varianten wurden im Berichtszeitraum identifiziert, und auch das Bedrohungspotenzial von Schadprogramm-Spam steigt weiterhin an, trotz der in diesem Fall verminderten Menge. E-Mails mit Schadprogrammen zählen zu den am häufigsten detektierten Angriffen auf die Bundesverwaltung. Die Auswirkungen durch Schadprogramme nehmen neben der klassischen Bürokommunikation auch in Produktivbereichen der Wirtschaft weiter zu. Insbesondere im Maschinenbau vergrößern die laufende Digitalisierung und zunehmende Vernetzung durch IoT und Industrie 4.0 die Angriffsfläche und können bei unsachgemäßer Implementierung mögliche Schäden durch Schadprogramme potenzieren.

Die Bedrohungslage durch Botnetze bleibt unverändert hoch, wobei sich auch hier die Angreifer die Digitalisierung zunutze machen und den Fokus auf mobile Endgeräte und IoT-Systeme legen. Diese bieten durch die täglich zunehmende Verbreitung bei gleichzeitig oft nur mangelhafter Absicherung eine willkommene Möglichkeit der unbefugten Übernahme und missbräuchlichen Nutzung durch Kriminelle. Täglich bis zu 110.000 Botinfektionen deutscher Systeme wurden registriert und vom BSI mit dem Ziel der Bereinigung an die jeweiligen Netzbetreiber gemeldet. Noch mehr Angriffspotenzial ermöglichen serverbasierte Botnetze, insbesondere vor dem Hintergrund der zunehmend genutzten Cloud-Infrastrukturen. Mehr als jede zweite Attacke wird über kompromittierte oder missbräuchlich angemietete Cloud-Server ausgeführt. Fast jeder Cloud-Dienstleister wurde demnach bereits mindestens einmal von Kriminellen zur Durchführung von DDoS-Attacken missbraucht.

Unnötig verschärft wird die ohnehin angespannte Cyber-Sicherheitslage durch die in vielen Fällen festzustellende digitale Hilflosigkeit aufseiten der Anwender. Täter nutzen Schwächen individuellen Sicherheitsverhaltens in Verbindung mit strukturell unzureichend gesicherten Produkten und Systemen gezielt aus. Abhilfe kann die konsequente Nutzung von IT-Sicherheitsmaßnahmen nach Stand der Technik sowie eine Stärkung der digitalen Eigenverantwortung jedes einzelnen Nutzers schaffen.

Integrierte Wertschöpfungskette zum Schutz von Staat, Wirtschaft und Gesellschaft

Auch vor dem Hintergrund der in diesem Bericht beschriebenen angespannten Gefährdungslage kann die Digitalisierung in Deutschland sicher gestaltet werden. Das Eindringen

von Digitalisierung in alle Lebens- und Wirtschaftsbereiche bedeutet, dass sich Cyber-Sicherheit weiterentwickeln muss. Für einen starken und auch in Zukunft sicheren Standort Deutschland ist es notwendig, die Chancen der Digitalisierung aufzugreifen und zugleich den potenziellen Risiken von Beginn an angemessen zu begegnen. Deutschland als Wirtschafts- und Innovationsstandort muss Vorreiter einer Digitalisierung sein, die die Absicherung von IT-Produkten und auch von Unternehmensnetzwerken von vornherein mitdenkt und die Prinzipien Security-by-Default und Security-by-Design verinnerlicht hat.

Das BSI hat als Kompetenzzentrum des Bundes für IT- und Cyber-Sicherheit dazu erfolgreich die Weichen gestellt und übernimmt Verantwortung bei dieser gesamtgesellschaftlichen Aufgabe. Das BSI beschäftigt sich täglich damit, in welchen Anwendungsfeldern der Digitalisierung Risiken entstehen könnten und wie sie kalkulierbar und beherrschbar gemacht werden können. Der jahrzehntelange Aufbau und die Bündelung von Know-how im Bereich der Cyber-Sicherheit hat das BSI zu einer schlagkräftigen Behörde gemacht, in der die Fäden der Cyber-Sicherheit zusammenlaufen. Aus den gewonnenen Erkenntnissen leitet das BSI jeweils passende Empfehlungen, Produkte oder Dienstleistungen für die unterschiedlichen Anforderungen von Staat, Wirtschaft und Gesellschaft ab. Die integrierte Wertschöpfungskette der Cyber-Sicherheit aus Prävention, Detektion und Reaktion unter einem Dach ist ein weltweites Alleinstellungsmerkmal des BSI.

Das BSI nimmt aktiv an neuen Entwicklungen in der zunehmend digitalisierten Gesellschaft teil und bringt durch eine enge Zusammenarbeit mit nationalen und internationalen Playern seine Erkenntnisse und Forderungen zur Stärkung der Cyber-Sicherheit unmittelbar und von Beginn an in den jeweiligen Entwicklungsprozess ein. Als Thought Leader in den Bereichen Künstliche Intelligenz, Quantencomputing oder Blockchain und bis hin zur neuesten Mobilfunkgeneration 5G leistet das BSI einen entscheidenden Beitrag zur Beibehaltung der digitalen Souveränität Deutschlands und zur Gewährleistung der Sicherheitsaspekte.

Sei es von Bonn aus, aus dem Raum Dresden oder aus den Verbindungsstellen heraus: Das BSI befasst sich mit Themen, die für die wirtschaftliche und gesellschaftliche Entwicklung Deutschlands von immenser Bedeutung sind, und zeigt auf, wie Digitalisierung ‚Made in Germany‘ funktionieren kann: Cyber-Sicherheit ist die Antwort auf die neuen Herausforderungen, vor denen Behörden, Unternehmen, Kritische Infrastrukturen und Privatanwender jeden Tag aufs Neue stehen, um die Vorteile ihrer digitalisierten Geschäftsprozesse oder die Vorzüge ihres digitalen Lebens zu nutzen. Unterstützung erfahren Anwender aller

Zielgruppen nicht zuletzt durch konkrete Angebote des BSI wie den Digitalen Verbraucherschutz, das geplante IT-Sicherheitskennzeichen, den Ausbau der Beratungsangebote für Länder und Kommunen, den Leistungen der Allianz für Cyber-Sicherheit und des UP KRITIS sowie den Zertifizierungs- und Standardisierungsmöglichkeiten. Damit leistet das BSI einen entscheidenden Beitrag dazu, das Niveau der Informationssicherheit gesamtgesellschaftlich kontinuierlich zu erhöhen, potenziellen Gefahren präventiv zu begegnen und, wo notwendig, angemessen zu reagieren. Die Bedrohungslage nimmt weiter zu, wie auch die Digitalisierung weiter fortschreitet. Beides gehört zusammen, für beides hat das BSI Antworten parat. Mit neuen Aufgaben, einer stetig wachsenden Anzahl qualifizierter und motivierter Mitarbeiterinnen und Mitarbeiter und zusammen mit seinen nationalen und internationalen Partnern übernimmt das BSI Verantwortung und entwickelt auch weiterhin Strategien und Lösungen, mit denen sich die Digitalisierung für alle zum Erfolg führen lässt.

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.

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.

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.

CERT/Computer Emergency Response Team

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

CERT-Bund

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

Cloud/Cloud Computing

Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die im Rahmen von Cloud Computing angebotenen Dienstleistungen umfassen das komplette Spektrum der Informationstechnik und beinhalten u. a. Infrastrukturen (Rechenleistung, Speicherplatz), Plattformen und Software.

Digitaler Persönlichkeitsschutz

Digitaler Persönlichkeitsschutz ist die Absicherung der Aktivitäten von wichtigen Persönlichkeiten im digitalen Raum. Dazu gehören neben dem Schutz privater E-Mail-Postfächer auch Maßnahmen wie die Verifizierung von Twitter- und Facebook-Accounts.

DNS

Das Domain Name System (DNS) ordnet den im Internet genutzten Adressen und Namen, wie beispielsweise www.bsi.bund.de, die zugehörige IP-Adresse zu.

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-Angriff (DDoS = Distributed Denial of Service). DDoS-Angriffe erfolgen häufig durch eine sehr große Anzahl von Computern oder Servern.

Doxing

Doxing bezeichnet das vorsätzliche Bloßstellen und Schädigen von Individuen oder Organisationen durch die Verbreitung und Veröffentlichung von Dokumenten, die zusammengetragene personenbezogene Daten enthalten.

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-Kit

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

Firmware

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

Padding

Padding (englisch to pad „auffüllen“) wird in der Kryptografie bei Verschlüsselungsverfahren verwendet, um Datenbereiche aufzufüllen. Bei einer Block-Chiffre werden z. B. die zu verschlüsselnden Daten in Blöcken fester Größe gespeichert. Damit auch der letzte Block „voll“ wird, kann Padding zum Auffüllen der letzten Bytes benutzt werden.

Patch/Patch-Management

Ein Patch („Flicken“) ist ein Softwarepaket, mit dem Softwarehersteller 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.

Plug-in

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

Ransomware

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

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 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 Täter 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 enthält Spam jedoch auch Schadprogramme im Anhang, Links zu verseuchten Webseiten oder wird für Phishing-Angriffe genutzt, sog. Malware-Spam.

SSL/TLS

TLS steht für Transport Layer Security (Transportschichtsicherheit) und ist ein Verschlüsselungsprotokoll für die sichere Übertragung von Daten im Internet. Bekannt ist auch die Vorgängerversion SSL (Secure Sockets Layer).

UP KRITIS

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

Impressum

Herausgeber

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Bezugsquelle

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

E-Mail

bsi@bsi.bund.de

Telefon

+49 (0) 22899 9582-0

Telefax

+49 (0) 22899 9582-5400

Stand

Oktober 2019

Druck

Appel & Klinger Druck und Medien GmbH, Schneckenlohe

Gestaltung

Fink & Fuchs AG

Texte und Redaktion

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Bildnachweis

alle Bilder: GettyImages KTSDESIGN_SCIENCE PHOTO LIBRARY

Grafiken

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Artikelnummer

BSI-LB19/508

Diese Broschüre ist Teil der Öffentlichkeitsarbeit des BSI.

Sie wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt.

