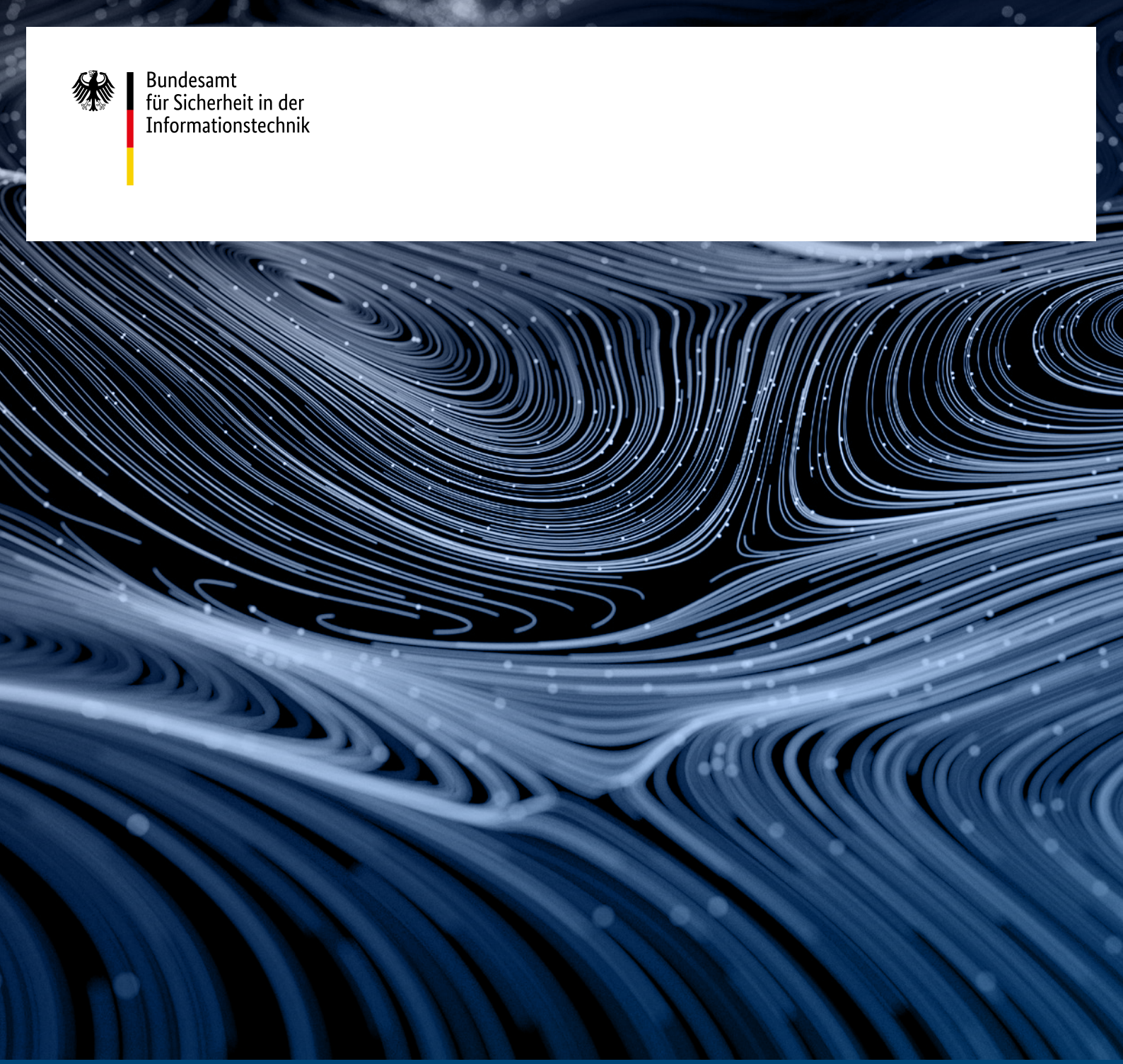
Bundesamt
für Sicherheit in der
Informationstechnik



Die Lage der IT-Sicherheit in Deutschland 2018

Vorwort

Unsere moderne, hochtechnisierte Gesellschaft ist vom Funktionieren empfindlicher Informationstechnologien und Kommunikationssysteme, von einer leistungsfähigen Infrastruktur sowie von einer sicheren Energieversorgung abhängig. Diese Systeme sind die Basis für technischen Fortschritt und wirtschaftliche Entwicklung in unserem Land.

Mit der wachsenden Komplexität der Systeme und der fortschreitenden Vernetzung aller Bereiche der Informationsgesellschaft nehmen allerdings auch die Risiken von Störungen sowie Angriffen von innen oder außen zu. Bedrohungen im Cyber-Raum haben eine hohe Dynamik, Cyber-Angriffe werden flexibler und professioneller. Mit der rasanten Entwicklung der IT-Systeme verändern sich auch die Angriffsmethoden ständig.

Der Bund nimmt seine Verantwortung für Sicherheit auch im Cyber-Raum wahr: Durch gesetzliche Rahmenbedingungen für IT-Sicherheit, mit einer Cyber-Sicherheitsstrategie und mit der Stärkung seiner Behörden für Cyber-Sicherheit.

Bei dem Erreichten können und dürfen wir aber nicht stehen bleiben: Wir werden das IT-Sicherheitsgesetz mit einem IT-Sicherheitsgesetz 2.0 fortschreiben und damit den staatlichen Schutzauftrag stärken. Wir wollen die Beratungs- und Unterstützungsangebote des BSI für Bund und Länder, für die Bürgerinnen und Bürger sowie für Unternehmen weiter ausbauen.

Hier ist allerdings nicht nur der Staat alleine gefragt: Wenn es um den Schutz in der Wirtschaft geht, bleiben die Unternehmen selbst aufgerufen, ihre IT-Sicherheitsmaßnahmen zu intensivieren und an neue Herausforderungen anzupassen.

Informationsaustausch und Kooperation aller Akteure sind zentral, um Cyber-Gefahren effektiv zu begegnen. Sicherheitsstandards müssen etabliert und durchgesetzt werden. Dafür wird ein starker Moderator benötigt: Das BSI bietet - neben seiner Aufgabe als Sicherheitsdienstleister für die Bundesverwaltung - bereits heute ein breites Sicherheitsportfolio für Wirtschaft und Gesellschaft. Ich werde mich dafür einsetzen, die Fähigkeiten des BSI weiter auszubauen und das BSI als nationale Cybersicherheitsbehörde fortzuentwickeln.

Mit dem Lagebericht zur IT-Sicherheit 2018 legt das BSI einen umfassenden und fundierten Überblick über die Bedrohungen Deutschlands, seiner Bürgerinnen und Bürger und seiner Wirtschaft im Cyber-Raum vor. Der Bericht zeigt aber vor allem, welch erfolgreiche und unverzichtbare Arbeit das BSI leistet. Deutschland, seine Bürgerinnen und Bürger, seine Wirtschaft und seine Behörden stehen weiterhin im Fadenkreuz von Cyber-Angriffen. Sich diesen Herausforderungen zu stellen und auf neue Bedrohungen im Cyber-Raum schnell und effizient zu antworten: Das bleibt die Kernaufgabe des BSI und seiner Mitarbeiterinnen und Mitarbeiter.

Horst Seehofer
Bundesminister des Innern, für Bau und Heimat

Vorwort

Als mit Beginn des Industriezeitalters auch der motorisierte Verkehr zunahm, mussten neue Regelwerke geschaffen, neue technische Einrichtungen implementiert und neue Verhaltensweisen erlernt werden, um die Verkehrssicherheit zu gewährleisten. Ampeln regeln seit über 100 Jahren den Verkehr, in den Straßenverkehrs-Ordnungen sind seit 1934 Verhaltensregeln für alle Verkehrsteilnehmer verankert. Für einige Verkehrsteilnehmer wurde es sogar verpflichtend, eine Prüfung zu absolvieren, um ihr Fahrzeug benutzen zu dürfen. Neue Berufe wurden geschaffen, neue Regeln festgelegt, neue Institutionen mussten das Verkehrsgeschehen kontrollieren.

Heute stehen wir wieder am Beginn eines neuen Zeitalters. Die Digitalisierung bestimmt immer mehr staatliches und wirtschaftliches Handeln sowie den Alltag der Bürgerinnen und Bürger. Und wie zu Beginn des Industriezeitalters müssen neue Regelwerke geschaffen, neue technische Einrichtungen implementiert und neue Verhaltensweisen gelernt werden, um die Cyber-Sicherheit zu erhöhen: Das IT-Sicherheitsgesetz, IT-Grundschutz und Verhaltensregeln für den sicheren Umgang mit Smartphone und Tablet sind nur einige Beispiele dafür.

Doch anders als zu Beginn des Industriezeitalters haben wir als Gesellschaft weniger Zeit, um uns auf die neue technologische Basis ein- und umzustellen. Das Innovationstempo der Digitalisierung ist atemberaubend. Neue Anwendungen, neue Produkte kommen in immer kürzeren Zyklen auf den Markt, neue Unternehmungen, die auf innovativen digitalen Technologien gründen, verdrängen etablierte. Und die Globalisierung und technische Vernetzung bringt es mit sich, dass Fehler in der Entwicklung, Lücken in Regelwerken, Fahrlässigkeit im Verhalten oftmals immense Auswirkungen haben.

Je wichtiger Digitalisierung für staatliches Handeln, unsere Geschäfte und unseren Alltag wird, desto mehr müssen die damit verbundenen Herausforderungen der Cyber-Sicherheit von allen Akteuren auf nationaler und internationaler Ebene gemeinsam angegangen werden.

Auf diesem Weg ist Deutschland ein gutes Stück vorangekommen. Wichtige Maßnahmen auf legislativer und operativer Ebene wurden in allen Bereichen umgesetzt. Die Vernetzung der Akteure in Bund, Ländern und Kommunen wurde vorangetrieben, die Kooperation mit der Wirtschaft wurde ausgebaut, das BSI wurde nennenswert personell aufgestockt. Wir sind gut gerüstet.

Das sind wir aber nur so lange, wie wir als Gesellschaft nicht nachlassen, unsere Bemühungen um eine stabile und erfolgreiche Cyber-Abwehr zumindest parallel, noch besser aber proaktiv zur Gefährdungslage zu steigern. Der gesetzliche Rahmen muss weiterentwickelt, vorhandene Kooperationen müssen national und international intensiviert und betroffene Schutzmaßnahmen immer wieder auf den Prüfstand gestellt werden. Wir müssen offen bleiben für Neues, aktuelle Gefährdungen und das Bewusstsein für die Bedeutung der IT-Sicherheit weiter schärfen.

Uns muss eines immer klar sein: Eine erfolgreiche Fortsetzung des Digitalisierungsprozesses wird es ohne Cyber-Sicherheit nicht geben. Diesen Prozess gestaltet das BSI gemäß des eigenen Leitsatzes mit: Das BSI als die nationale Cyber-Sicherheitsbehörde gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft.

Ich wünsche Ihnen eine interessante und informative Lektüre des Lageberichts 2018.

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 7

1.1 Gefährdungslage des Bundes 7

1.2 Gefährdungslage KRITIS und Wirtschaft 10

1.3 Gefährdungslage Gesellschaft 17

1.4 Angriffsmethoden und -mittel 23

2 Lösungen und Angebote des BSI 53

2.1 Zielgruppe Staat und Verwaltung 53

2.2 Zielgruppe Wirtschaft 64

2.3 Zielgruppe Gesellschaft 72

2.4 Internationale Zusammenarbeit 84

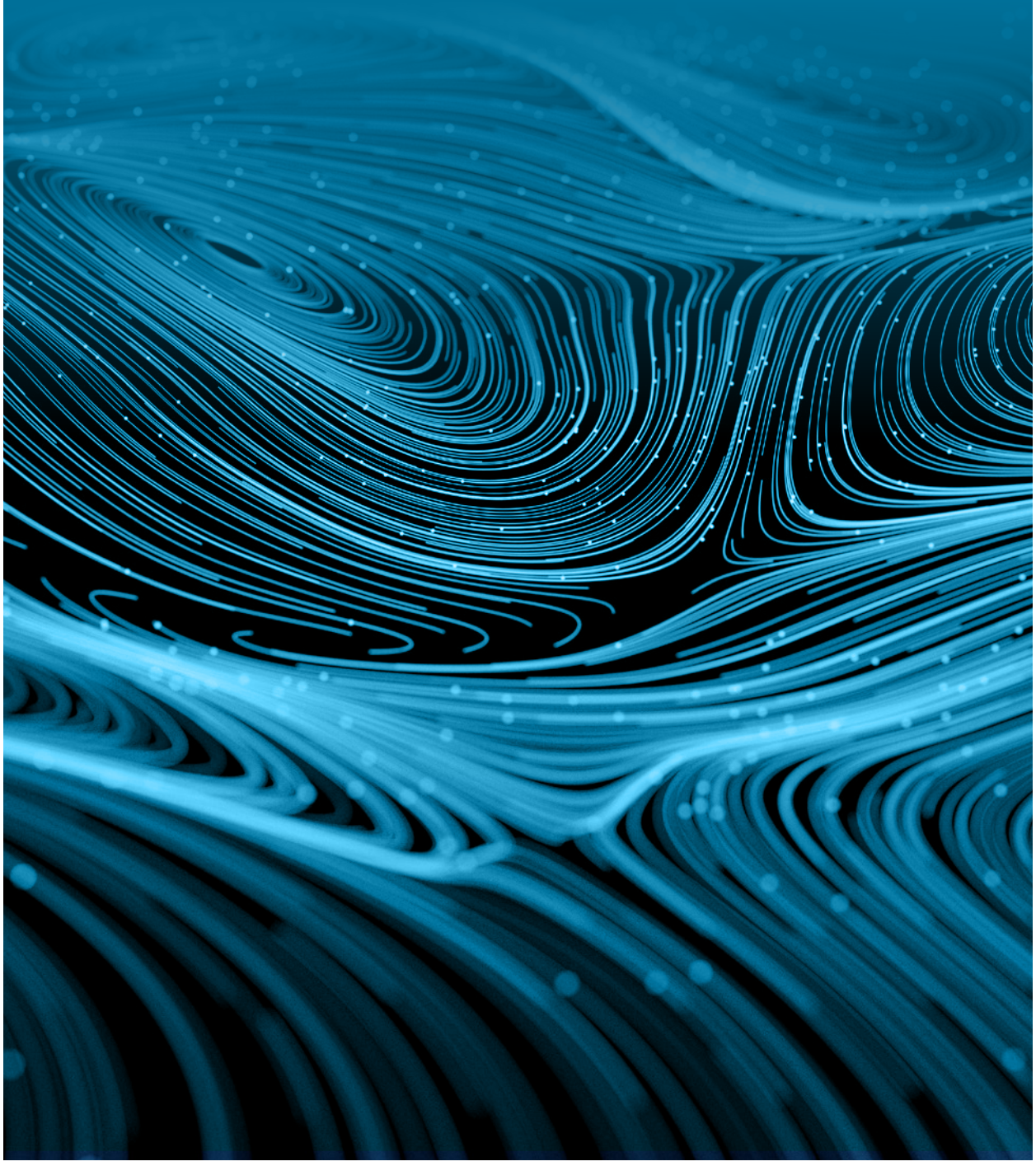
2.5 Cyber-Sicherheit IT-Fachkräfte 88

3 Gesamtbewertung und Fazit 91

4 Glossar 96

Impressum 99

1 Die Gefährdungslage



1 Die Gefährdungslage

In diesem Bericht wird die Gefährdungslage der IT-Sicherheit in Deutschland im Zeitraum 1. Juli 2017 bis 31.Mai 2018 beschrieben. Dieses Kapitel ist gegliedert in die Bereiche Bundesverwaltung, Kritische Infrastrukturen/Wirtschaft und Gesellschaft. Zudem wird auf Angriffsmethoden und Angriffsmittel der Angreifer sowie auf Rahmenbedingungen und Ursachen eingegangen. Anhand zahlreicher Beispiele wird erläutert, wie durch Angriffe auf die IT-Sicherheit das Leben in einer digitalisierten Gesellschaft beeinträchtigt werden kann.

1.1 Gefährdungslage des Bundes

Damit die Einrichtungen des Staates ihre verfassungsrechtlichen Aufgaben sicher und nachhaltig ausüben können, müssen die Informationssysteme des Staates zuverlässig und störungsfrei betrieben werden können. Nur auf diese Weise ist zuverlässiges, fälschungssicher dokumentiertes Verwaltungshandeln garantiert, nur so kann der Staat mit seinen Bürgerinnen und Bürgern lückenlos und gegen Manipulationen jeglicher Art geschützt kommunizieren. Ist dies wegen beeinträchtigter oder funktionsunfähiger Informationssysteme nicht möglich, wird das Vertrauen in die Integrität des Staates erschüttert. In der digitalen Gesellschaft sind die Informationssysteme der Staatsgewalten dadurch zu kritischen Größen für das Funktionieren des Gemeinwesens geworden.

1.1.1 Erkenntnisse aus dem Schutz der Regierungsnetze

Wichtigste 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.

Abwehr von Schadprogrammen

Cyber-Angriffe auf die Regierungsnetze finden täglich statt. 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 28.000 solcher E-Mails in Echtzeit abgefangen, bevor sie die Postfächer der Empfänger erreichen konnten. Davon wurden monatlich im Durchschnitt rund 6.000 schädliche E-Mails nur aufgrund eigens erstellter Antivirus-Signaturen erfasst. Der Rückgang dieser Zahlen im Vergleich zum Vorjahresbericht ist insbesondere auf den starken Rückgang von Ransomware im Jahr 2017 zurückzuführen, der auch außerhalb der Regierungsnetze zu beobachten war. Im Vergleich zu den Vorjahren wurden zudem deutlich mehr Schadprogramme nicht als Dateianhang in E-Mails versendet, sondern über Links in E-Mails verteilt.

Im HTTP-Verkehr wurden im Jahr 2017 durchschnittlich rund 500 Schadprogramme pro Monat erkannt und abgewehrt. Auch hier setzte sich 2018 der Trend fort, dass Schadsoftware immer öfters in E-Mails nur verlinkt und nicht als Anhang beigefügt ist.

Den automatisierten Antivirus-Schutzmaßnahmen nachgelagert betreibt das BSI ein weiteres System zur Detektion von Schadprogrammen im Datenverkehr der Regierungsnetze, welches auf Grundlage der erweiterten Befugnisse des BSIG betrieben wird (nach § 5 BSIG). Die Analysten des BSI konnten auf diese Weise im Berichtszeitraum über 40.000 Angriffe identifizieren, die von den eingesetzten kommerziellen Schutzprodukten nicht detektiert oder blockiert werden konnten. Zudem wurden über zwei Millionen Zugriffe aus dem Regierungsnetz auf Server unterbunden, die mit Schadcode, Betrug oder Datendiebstahl in Verbindung standen.

1.1.2 Erkenntnisse aus der IT-Sicherheitsberatung

Das Arbeitsumfeld in der Bundesverwaltung wird durch zahlreiche Veränderungen geprägt. Neben der Zentralisierung der benötigten IT-Dienstleistungen im Rahmen der IT-Konsolidierung des Bundes schreitet die Digitalisierung der Arbeitsabläufe und der verwaltungsinternen Prozesse weiter voran.

Die immer komplexer werdenden IT-Komponenten sind grundsätzlich angreifbar und können Schwachstellen enthalten. Dies hat zur Folge, dass in der Bundesverwaltung auf entdeckte Schwachstellen und Angriffe planvoll und systematisch reagiert werden muss. Nachdem die Erstmaßnahmen umgesetzt wurden, sollten anschließend sinnvollerweise auch das Informationssicherheitsmanagementsystem (ISMS) auf Aktualität sowie Konformität mit den Vorgaben überprüft und die Sicherheitsmaßnahmen angepasst werden. Die Absicherung gegen APT-Angriffe stellt hohe Anforderungen an das Sicherheitsmanagement und die Umsetzung von Maßnahmen. Die Prozessorschwachstellen *Spectre* und *Meltdown* haben gezeigt, das auch die Hardware eine bedeutende Rolle bei der Absicherung von IT-Infrastrukturen spielt. Entsprechende Gegenmaßnahmen sind zu entwickeln und umzusetzen.

Cyber-Angriff auf deutsche Behörden

Sachverhalt
Gegen Ende des Jahres 2017 hat das BSI über das Nationale Cyber-Abwehrzentrum Hinweise auf einen erfolgreichen Cyber-Angriff erhalten, von dem einzelne Bundesbehörden betroffen sein sollten. Das BSI startete den Prozess der Vorfallsbearbeitung in Abstimmung mit den im Nationalen Cyber-Abwehrzentrum beteiligten Behörden, informierte die potenziell betroffenen Behörden und begann mit der Analyse und Verifikation der initial vorliegenden Informationen.

Ursache/Schadenswirkung
Primäres Ziel des Angriffs war das Auswärtige Amt. Eine von der Hochschule des Bundes betriebene Lernplattform wurde angegriffen, um über diesen Zwischenschritt einen Zugang in das Netz des Auswärtigen Amtes aufzubauen, denn etablierte Schutzmaßnahmen haben verhindert, dass der Angreifer in der Lage war, einen direkten Zugang in das Netzwerk des Auswärtigen Amtes aufzubauen.

Der Angreifer war in der Lage, einige Client-Systeme im Auswärtigen Amt erfolgreich zu infizieren und interne Dokumente in geringer Stückzahl auszuleiten. Der Angriff richtete sich jedoch nicht gegen die Regierungsnetze insgesamt.

Reaktion (des BSI)
In enger Zusammenarbeit zwischen betroffenen Behörden, Nationalem Cyber-Abwehrzentrum und BSI wurden Reaktionsmaßnahmen wie

- Analyse der Betroffenheit,
- Identifikation und Sicherung von infizierten Systemen,
- forensische Analyse sowie
- Protokoll- und Logdaten-Auswertung bei den Betroffenen

an zentralen Stellen der Regierungsnetze ergriffen. Zusätzlich hat das BSI ein Mobile Incident Response Team (MIRT, im Sinne des § 5a BSIG) entsandt, um die Vorfallsbearbeitung bei den Betroffenen vor Ort auch an Wochenenden zu unterstützen.

In Abstimmung mit den Betroffenen wurde der Angriff verdeckt beobachtet, um das Vorgehen der Angreifer zunächst zu analysieren und sodann die Effektivität der zu ergreifenden Maßnahmen zu maximieren. Gewonnene Erkenntnisse sind bereits während der Analyse in die Schutzmaßnahme der Bundesverwaltung eingeflossen.

Nachdem Presseberichte GEHEIM eingestufte Informationen zu dem Vorfall am 28. Februar 2018 öffentlich gemacht hatten, wurden umgehend die vorbereiteten Sofortmaßnahmen zur Bereinigung eingeleitet. Zusätzliche Schutzmaßnahmen zur Unterbindung der Angreifer-Kommunikation wurden etabliert. Die betroffenen Systeme der Hochschule des Bundes wurden in der Folge ebenfalls abgeschaltet.

Empfehlung
Der Sachverhalt zeigt eindringlich das aktuell bestehende Bedrohungspotenzial durch gezielte Angriffe auf die Bundesverwaltung. Die finanziellen, zeitlichen und technischen Ressourcen, die von Angreifer-Seite in Vorbereitung und Durchführung des Angriffs investiert wurden, verdeutlichen das hohe Interesse des Angreifers an seinem Ziel.

Der Vorfall veranschaulicht nachdrücklich, dass mehrstufige Schutzkonzepte notwendig sind und Schutzmaßnahmen gegen gezielte Angriffe konsequent umgesetzt werden müssen. Der Vorfall belegt jedoch auch die Wirksamkeit dieser Maßnahmen: Vergleichbare Vorfälle haben in der Vergangenheit weitaus gravierendere Auswirkungen auf die Betroffenen gehabt.

Die Herausforderungen, vor denen die Ressorts und Bundesbehörden, aber auch die Landes- und Kommunalverwaltungen stehen, führen zu einem höheren Beratungsbedarf durch die Sicherheitsberatung des BSI.

In der Praxis der Sicherheitsberatung ist daher festzustellen, dass die fortgeschrittenen Angriffsmethoden – soweit noch nicht umgesetzt – mit komplexeren Sicherheitsmaßnahmen beantwortet werden müssen. Auch aus Sicht der Sicherheitsberatung wird die Erkennung und Abwehr von Schadprogrammen zu einer Aufgabe, die nicht mehr einfach durch Installation eines Virenschutzprogramms bewältigt werden kann. Zu stetiger Nachfrage führt auch die Einhaltung von Vorschriften und erneuerter Standards der Informationssicherheit, die vor dem Hintergrund einer komplexeren IT aufwändiger wird.

Um nicht bei einem rein reaktiven Vorgehen zu bleiben, kommt dem vorhandenen Managementsystem für Informationssicherheit (ISMS), der Sicherheitskonzeption und der Umsetzung aktueller Sicherheitsmaßnahmen eine hohe Bedeutung zu.

Mit den modernisierten IT-Grundschutz-Standards und der erneuerten Leitlinie für Informationssicherheit der Bundesverwaltung (Umsetzungsplan Bund 2017) ist ein aktuelles Instrumentarium bereitgestellt worden. Hierdurch ergeben sich entsprechende Handlungsanforderungen und -optionen, um bestehenden und künftigen Herausforderungen wirksam begegnen zu können.

1.1.3 Erkenntnisse aus Meldungen der Bundesverwaltung

Nach § 4 Abs. 3 BSIG sind die Bundesbehörden verpflichtet, das BSI unverzüglich zu unterrichten, wenn ihnen Informationen vorliegen, die für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik von Bedeutung sind. Die Einzelheiten des Meldeverfahrens, insbesondere hinsichtlich der Frage, welche Informationen für die Arbeit des BSI bzw. den Schutz der Informationstechnik des Bundes relevant sind, hat das Bundesministerium des Innern nach Zustimmung durch den Rat der IT-Beauftragten der Ressorts (IT-Rat) in einer allgemeinen Verwaltungsvorschrift zur Durchführung der Regelung § 4 Abs. 3 BSIG festgelegt. Sie ist am 1. Januar 2010 in Kraft getreten.

Diese Aufgabe wird durch das Referat „Zentrale Meldestelle und Nationales IT-Lagezentrum“ als organisatorischer Teilbereich des BSI wahrgenommen. Ziel ist es, jederzeit über ein verlässliches Bild der aktuellen IT-Sicherheitslage in Deutschland 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

SOFORT-Meldungen sind vorfallsbezogen und daher in ihrer Häufigkeit unregelmäßig. Grundsätzlich ist jedoch auch das zahlenmäßige Aufkommen der Meldungen ein zusätzlicher Indikator, um die Bedrohungslage zu bewerten.

Im Jahr 2017 wurden insgesamt 157 SOFORT-Meldungen an das Referat „Zentrale Meldestelle und Nationales IT-Lagezentrum“ gemeldet.

Bei den Meldungen blieb Ransomware 2017 weiterhin das maßgebliche Thema. Gemeldet wurde die Ausnutzung von Telefon-/Videokonferenzanlagen für Schadprogramminfektionen. Mitte des Jahres erfolgte ein Cyber-Angriff mit dem Verschlüsselungstrojaner *NotPetya*. Dies zeigt, dass im Umfeld von ALL-IP-Anschlüssen und VoIP-TK-Anlagen immer wieder die Frage nach einer sicheren Konfiguration und nach regelmäßig durch fachkundiges Personal vorgenommenen Sicherheitsaktualisierungen gestellt werden muss.

Es gingen nur noch halb so viele Meldungen zu DDoS-Angriffen wie im Vorjahr ein. Das im Jahr 2016 stark vertretene *Mirai*-Botnetz verlor nach dem 1. Quartal 2017 an Bedeutung.

1.2 Gefährdungslage KRITIS und Wirtschaft

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 und durch ihre Auslandsaktivität interessante 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.

1.2.1 Erkenntnisse aus KRITIS-Meldungen

Die Gefährdungslage in den Kritischen Infrastrukturen ist insgesamt auf hohem Niveau, aber in den verschiedenen Branchen unterschiedlich ausgeprägt. Im Berichtszeitraum erreichten das BSI 145 Meldungen aus den KRITIS-Sektoren; die meisten aus dem Bereich IT und Telekommunikation, die zweitmeisten aus dem Energiesektor.

KRITIS-Betreiber wie zum Beispiel Energieversorger (siehe Vorfall EnBW/Netcom) sehen sich, zusätzlich zu normalen Angriffen aus dem Internet, auch neuen oder fortschrittlicheren Angriffen ausgesetzt. Andere Branchen stehen eher in den hinteren Reihen. Sie sehen sich mit Attacken konfrontiert, die in den exponierteren Branchen schon beobachtet wurden. Die verwendeten Methoden wurden aber mittlerweile automatisiert und können von Angreifern nun flächendeckend eingesetzt werden.

Auch wenn die Aufteilung in exponierte und weniger exponierte Branchen relativ stabil ist, darf nicht davon ausgegangen werden, dass dies unveränderlich ist. Gesellschaftliche und politische Ereignisse können die Motivationslage der Angreifer ändern, so dass grundsätzlich alle KRITIS-Unternehmen im Fokus von fortschrittlicheren Angreifern stehen können und sich dagegen wappnen müssen.

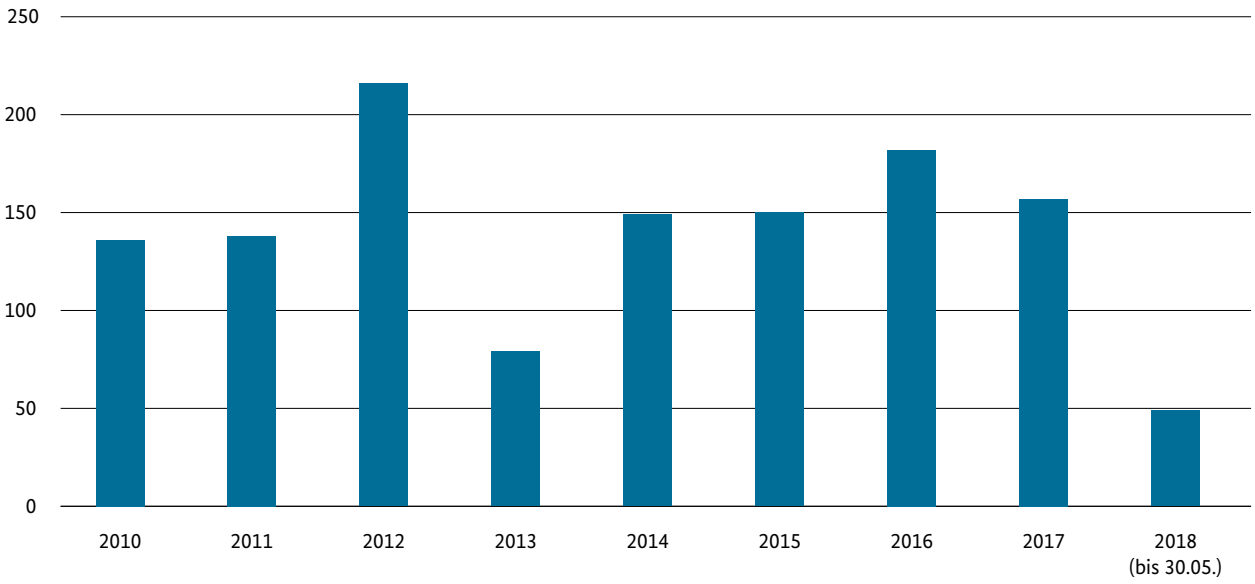


Abbildung 01 Abgegebene SOFORT-Meldungen nach § 4 Abs. 3 BSIG

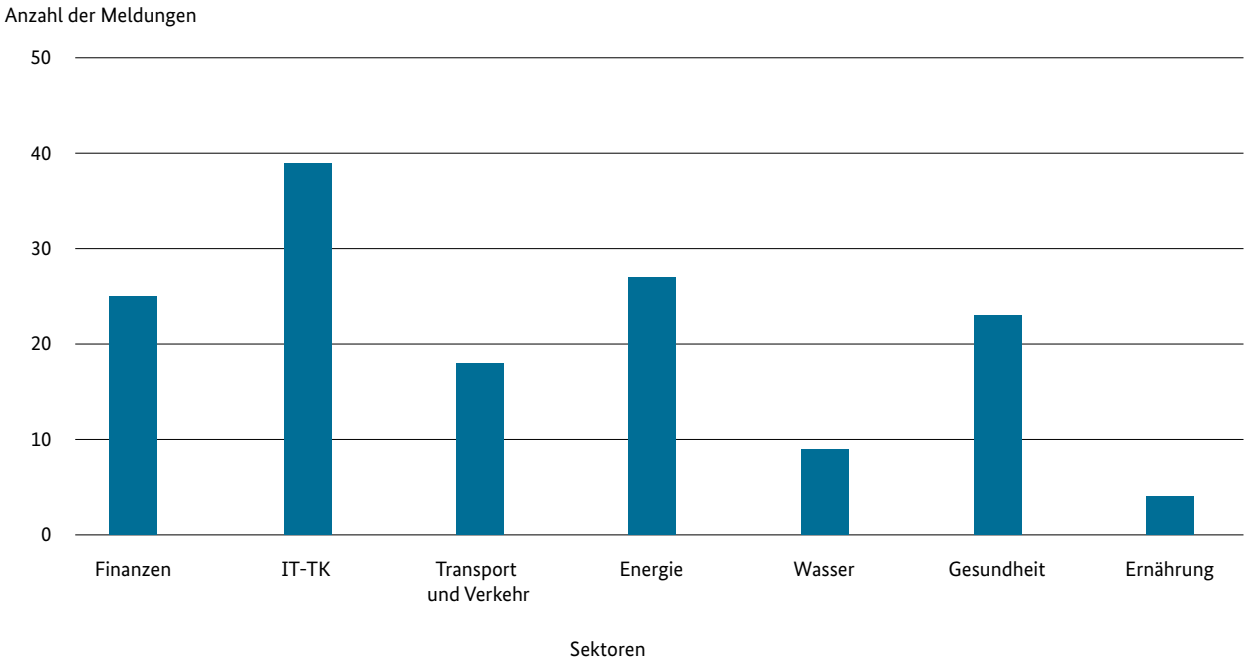


Abbildung 02 Meldeaufkommen von KRITIS-Betreibern (freiwillige und verpflichtende Meldungen nach § 8b BSIG) im Berichtszeitraum vom 01.06.2017 bis 31.05.2018

Angriff in das Netz eines regionalen Telekommunikationsunternehmens

Sachverhalt

Seit einigen Jahren zeichnet sich ab, dass eine oder mehrere Gruppen Schadsoftware entwickeln, die speziell für Angriffe auf Prozesssteuerungsanlagen (ICS) geeignet ist. Bereits im Jahr 2014 wurde die Schadsoftware Havex entdeckt, die weltweit zu Infektionen führte und in Netzwerken nach ICS-Systemen und Informationen über deren Konfiguration suchte https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf. Der genaue Zweck dieser Kampagne war damals nicht ersichtlich, da es keine Hinweise gab, dass wirtschaftlich oder politisch verwertbare Informationen gestohlen wurden. Berichte über destruktive Aktionen dieser Schadsoftware gab es ebenfalls nicht.

Seit 2015 gab es mehrere Angriffe auf Kritische Infrastrukturen in der Ukraine, die mittels modifizierter Varianten von Black-Energy durchgeführt wurden. Diese Schadsoftware hatte zwar keine ICS-spezifischen Funktionen, sie wurde aber eingesetzt, um den Tätern Zugriff auf Steuerungssysteme von Stromnetzbetreibern zu ermöglichen. Die Täter hatten zudem ausreichend Kenntnisse über die Systeme und Prozesse der Betreiber, um durch manuelle Änderungen großflächige Stromausfälle zu bewirken https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

Mitte Juni 2017 wurde erstmals über eine Schadsoftware namens Industroyer bzw. CrashOverride https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf berichtet, die die Funktionalität aufweist, über ICS-spezifische Protokolle Steuerungsanlagen zu kontrollieren. Diese wurde Ende 2016 für Angriffe gegen die Stromversorgung der Ukraine eingesetzt. Die modulare, erweiterbare Architektur sowie die detaillierten Implementationen von ICS-Protokollen legen den Schluss nahe, dass diese Tätergruppe über aufwändige Testumgebungen verfügt und das langfristige Ziel verfolgt, in ICS-Netzwerke einzudringen und diese gegebenenfalls zu sabotieren.

Berichte über Spearphishing- und Watering-Hole-Angriffe auf amerikanische und europäische Energiefirmen und Kernkraftwerksbetreiber https://www.ci-project.org/blog/2017/7/10/document-indicates-campaign-may-have-targeted-europe-an-energy-and-critical-infrastructure-in-march-2017 fügen sich ebenfalls in das Gesamtbild ein. Auch wenn hierbei Kompromittierungen bisher nur in Büronetzen gefunden wurden, sind die ausgewählten Watering-Holes für die ICS-Supply-Chain relevant. Es ist anzunehmen, dass in den Büronetzen zunächst Informationen für weitere Angriffe gesammelt werden sollen.

Das BSI geht davon aus, dass all diese Angriffe auf zwei bestimmte Gruppen zurückzuführen sind, die möglicherweise dieselben strategischen Ziele verfolgen. In Medien- und Analyseberichten werden diese Gruppen als *EnergeticBear/Dragonfly* und *Sandworm/VodooBear* bezeichnet. Die Sicherheitslage verschärfend ist zu berücksichtigen, dass im Mai 2017 ein Mann verhaftet wurde, der offenbar vertrauliche Informationen über europäische Energietransportwege an einen russischen Agentenführer verkauft haben soll.

Im Sommer 2017 schließlich drangen unbekannte Hacker in das Netz eines regionalen Telekommunikationsunternehmens ein, einer Tochterfirma eines Stromkonzerns. Der Betreiber erhielt vom Bundesamt für Verfassungsschutz eine Warnung über den Angriff, meldete den Sicherheitsvorfall beim BSI und bat um Unterstützung. Der Vorfall wurde vom BSI im Rahmen des Nationalen Cyber-Abwehrzentrums in Zusammenarbeit mit dem betroffenen Unternehmen analysiert und bearbeitet.

Ursache/Schadenswirkung
Bezüglich des zuletzt geschilderten Vorfalls gibt es derzeit keine Erkenntnisse, die auf eine Beeinträchtigung kritischer Versorgungsdienstleistungen hindeuten.

Dennoch muss die oben beschriebene Bedrohungslage ernst genommen werden. Mit entsprechender Fachexpertise und entsprechendem Ressourcenaufwand systematisch ausgeführte Angriffe haben durchaus das Potenzial, die Energieversorgung zu gefährden. Auch eine bereits bestehende konsequente Absicherung muss auf dem aktuellen Stand gehalten werden, um erfolgreichen Angriffen, wie z. B. denen auf die Stromversorgung in der Ukraine in den Jahren 2015 und 2016, entgegenzuwirken.

Reaktion
Das BSI hatte bereits frühzeitig potenziell betroffene Betreiber Kritischer Infrastrukturen über Angriffskampagnen gegen Energiefirmen informiert.

Aufgrund von weitergehenden Informationen, die im Laufe der Zeit von betroffenen Unternehmen und Partnerbehörden zur Verfügung gestellt wurden, konnte das BSI diese Warnung mit neuen Erkenntnissen anreichern und im Anschluss branchenübergreifend verteilen.

Darüber hinaus unterstützte das BSI den Betreiber bei der technischen Analyse. Die Namen betroffener Unternehmen werden vom BSI nicht ohne deren Zustimmung veröffentlicht.

Empfehlung
Sobald Betreiber Auffälligkeiten entdecken, die auf einen Angriff hinweisen könnten, sollten Informationen darüber möglichst umgehend an das BSI weitergeleitet werden. Hierdurch wird anderen Betreibern beim Schutz ihrer Anlagen geholfen, da das BSI diese Informationen in Form von Warnungen sanitarisiert weitergibt, so wie im oben genannten Fall geschehen.

Zum Schutz von ICS-Systemen und -Netzen empfiehlt das BSI weiterhin die Umsetzung der Maßnahmen aus den folgenden Dokumenten:

- BSI Grundschutz: IND - Industrielle IT (Bausteine und insbesondere Umsetzungshinweise) https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/IND/IND_Uebersicht_node.html
- BSI ICS-Kompendium https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf
- Fernwartung im industriellen Umfeld https://www.bsi.bund.de/ACS/DE/_/downloads/BSI-CS_108.html

1.2.2 Erkenntnisse aus Meldungen aus der Wirtschaft

Unternehmen sind grundsätzlich den gleichen Gefahren ausgesetzt wie jeder andere Nutzer von IT und Internet. Zusätzlich sehen sie sich aber Angriffen ausgesetzt, die im privaten Umfeld nicht vorkommen. Hierzu gehören u. a. die Cyber-Erpressung und die Cyber-Spionage.

Große Aufmerksamkeit erlangten Mitte 2017 die Cyber-Angriffe „*WannaCry*“ und „*NotPetya*“. *WannaCry* trat zum ersten Mal am 12. Mai 2017 (Verweis JLB 2017) in Erscheinung, *Petya* (auch: *NotPetya*, ExPetr, DiskCoder.C) Ende Juni 2017. Diese Angriffe haben eindrucksvoll verdeutlicht, wie anfällig viele Unternehmen in Bezug auf die Risiken der Digitalisierung sind und welche Auswirkungen es hat, wenn man Cyber-Sicherheit nicht als unabdingbare Voraussetzung einer erfolgreichen Digitalisierung versteht.

Analysen von IT-Sicherheitsforschern legen nahe, dass im Fall von *Petya*/*NotPetya* bereits seit April 2017 in mehreren Wellen unterschiedliche Schadsoftwarevarianten über die Update-Funktion der in der Ukraine weit verbreiteten Buchhaltungssoftware M.E.Doc verteilt wurden. Damit konnten auch Unternehmen von diesem Cyber-Angriff betroffen sein, die M.E.Doc einsetzen, aber augenscheinlich nicht vom öffentlich bekanntgewordenen Verschlüsselungstrojaner *Petya* betroffen waren. Die unterschiedlichen Schadsoftwarevarianten ermöglichen das Ausspähen von Daten aus den betroffenen Firmennetzwerken.

Die Verbreitung von *Petya* betraf ursprünglich vor allem Russland und die Ukraine. Im Anschluss wurden Computer in Polen, Italien, Großbritannien und Frankreich infiziert. Später erreichte die Erpresser-Software die USA und breitete sich auch in Asien aus. Auch in Deutschland waren Unternehmen betroffen. Der Konsumgüterkonzern Beiersdorf bestätigte, er sei Ziel des Angriffs geworden, IT- und Telefon-Systeme seien ausgefallen.

Auch wenn es im Fall von *WannaCry* gelang, die Schadwirkung durch Registrierung einer URL („Kill-Switch“) zu begrenzen, ist Schadsoftware vom Typ *WannaCry* weiterhin virulent. Anfang 2018 erreichten das BSI noch Meldungen aus der Wirtschaft, die einen Befall von Rechnern mit der *WannaCry*-Schadsoftware anzeigten (siehe Vorfall Seite 14). Diese späten Infektionen stehen, insbesondere hinsichtlich ihrer Auswirkungen, deutlich hinter der ersten *WannaCry*-Welle zurück.

WannaCry hat die Fähigkeit, sich selbstständig weiter zu verbreiten. Dadurch kommt es immer wieder zu sporadischen, aber begrenzten Infektionen, sobald infizierte, aber nicht auffällig gewordene Rechner Kontakt zu anderen Netzwerken bekommen. Sicher geglaubte interne Netze, die sich auf die Sicherheitsmaßnahmen ihres Umfeldes verlassen, lassen dem Schädling leider nur zu häufig viel Freiraum für eine Weiterverbreitung.

Die Fälle zeigen, dass sie für einzelne Betreiber durchaus zu einem ernstzunehmenden Problem werden können. Gerade Embedded-Systeme mit älteren und eventuell ungepatchten Betriebssystemen sowie Steuerungen von Industrieanlagen können noch anfällig sein für die Verbreitungswege, die *WannaCry* nutzt. Manchen Geräten sieht ein Betreiber auch nicht unbedingt sofort an, welche Prozesse auf diesen Geräten laufen; dies gilt auch für Patchstand oder Konfiguration.

Insgesamt ist der Schaden immens, den *WannaCry* verursacht hat: Die Schätzungen reichen weltweit von einigen Hundert Millionen Dollar bis zu vier Milliarden Dollar. Mehr als 200.000 Rechner in 150 Ländern wurden infiziert. Im Vergleich dazu ist der Erpressungserlös der Angreifer gering. Nach Ablauf der Deadline für die Lösegeldzahlung sind auf den der anonymen Hackergruppe zuzurechnenden drei wallets – digitale Bitcoin-Geldbörsen – Bitcoins im Wert von knapp 93.000 Euro eingegangen.

Ransomware-Angriffe wie *WannaCry*, *NotPetya* und Bad Rabbit brachten 2017 viele Unternehmen in Bedrängnis, darunter z. T. Kritische Infrastrukturen wie Betriebe im Gesundheitswesen und in der Logistik. Insgesamt haben Ransomware-Vorfälle Unternehmen im Jahr 2017 nach publizierten Schätzungen weltweit mehr als 8 Milliarden Dollar gekostet.

Diese Bedrohung durch Ransomware setzt sich 2018 fort, wenn auch in geringerem Umfang, da einerseits eine Verlagerung zu bzw. Ergänzung durch Krypto-Mining zu beobachten ist und andererseits diversifizierte gezieltere Angriffe durchgeführt werden. Dies führt zu einem hohen Druck auf Unternehmen, angemessene Reaktionsstrategien zu entwickeln, um die Auswirkungen eines Angriffs besser begrenzen zu können.

Infektionen mit *WannaCry*-Schadsoftware

Sachverhalt
Anfang des Jahres 2018 erreichte das BSI die Meldung eines KRITIS-Betreibers im Sektor Ernährung. Mehrere Rechner in einer Produktionsanlage fielen häufig aus und mussten neu gestartet werden. Wenige Tage später wurde dem BSI ein weiterer Fall gemeldet, diesmal von einem Anlagenbauer, der Anlagen an mehreren Standorten betreut. Auch im Februar 2018 erreichte eine Meldung das BSI. In einem Krankenhausverbund kam es zu *WannaCry*-Infektionen auf Medizingeräten an mehreren Standorten. Auch in Großbritannien waren zahlreiche Kliniken betroffen.

Ursache/Schadenswirkung
Im Falle des Anlagenbauers waren die Rechner so konfiguriert, dass sie nach einem Neustart wieder in einen definierten Ursprungszustand zurückversetzt wurden. Dies erleichtert im Störungsfall die Wiederaufnahme des Betriebs. Wie der Betreiber schnell herausfand, war die *WannaCry*-Schadsoftware die Ursache für die vielen Ausfälle. Einem mit *WannaCry* infizierten Rechner gelang es, einen der Steuerungsrechner über das Netzwerk zu erreichen. Der Wurm infizierte den Steuerungsrechner, verbreitete sich von dort aus weiter und startete die Verschlüsselung des Dateisystems. Das führte zum Ausfall der Rechner. Der Betreiber konnte zwar den Steuerungsrechner durch Neustart wieder in einen produktiven Zustand versetzen, hierdurch war die eigentliche Fehlerursache jedoch nicht beseitigt. Danach begann der Ablauf wieder von neuem, wahrscheinlich sogar durch Rückinfizierung eines anderen Steuerungsrechners im selben Netzwerk. So konnten die Steuerungsrechner zwar immer wieder in einen produktiven Zustand zurückversetzt werden, aber bis zu einer konzertierten Bereinigung des gesamten Netzwerkes konnte *WannaCry* immer wieder erneut Steuerungsrechner infizieren.

Beim zweiten Fall untersuchte ein Mobile Incident Response Team (MIRT) des BSI in Absprache mit dem betroffenen Betreiber und dem betreuenden Unternehmen die Lage vor Ort. Nach eingehender Analyse, insbesondere durch den Anlagenbauer, wurde klar, dass es eine gemeinsame Ursache gab. Es wurde ein Fehler in einer Netzwerkkomponente gefunden, die Teil der Wartungsinfrastruktur des Anlagenbauers war. Durch diesen funktionierte die Netzwerktrennung nicht wie konfiguriert, sondern ermöglichte es *WannaCry*, diese zu überwinden. Der Anlagenbauer nahm daraufhin Kontakt mit dem Hersteller der Netzwerkkomponente auf, sodass dieser die Lücke schließen konnte.

Beim Krankenhausverbund schließlich wurde bei der Analyse des Infektionsweges deutlich, dass ein vom Hersteller zur Verfügung gestelltes Testgerät infiziert war. *WannaCry* konnte sich aus dem Testnetz auf andere Standorte verteilen, weil nicht alle Firewalls so konfiguriert waren, dass eine Weiterverbreitung verhindert wurde. Nach Auskunft des Krankenhausbetreibers wurden die Geräte glücklicherweise nur infiziert, es kam aber nicht zu Schadwirkungen, d. h. *WannaCry* nahm keine Verschlüsselung der Dateisysteme vor. Dennoch nahm die Bereinigung der Geräte viele Arbeitsstunden in Anspruch.

Empfehlung
Das BSI rät zu besonderer Vorsicht, wenn Geräte neu in Netzwerke eingebunden werden oder neue Kommunikationsverbindungen zwischen Netzwerken oder einzelnen Geräten entstehen. Der Verbreitungsweg von *WannaCry*, auch innerhalb von abgeschotteten Netzwerken, sollte nicht unberücksichtigt bzw. unkontrolliert bleiben.

1.2.3 Gefährdungslage Wirtschaft: Erkenntnisse aus der Cyber-Sicherheits-Umfrage der Allianz für Cyber-Sicherheit

Cyber-Angriffe haben erhebliche Konsequenzen für die Wirtschaft. Das geht aus der Cyber-Sicherheits-Umfrage 2017 hervor, die das BSI im Rahmen der Allianz für Cyber-Sicherheit durchgeführt hat. Mit der Cyber-Sicherheits-Umfrage untersucht das BSI seit 2014 jährlich die subjektive Gefährdungslage und Betroffenheit deutscher Institutionen durch Cyber-Angriffe sowie den Umsetzungsstand entsprechender Schutzmaßnahmen. Im Zeitraum vom 04.10.2017 bis 30.11.2017 haben sich nahezu 900 Unternehmen und Institutionen an der öffentlichen Online-Umfrage auf www.allianz-fuer-cybersicherheit.de beteiligt. Die Umfrage war anonym, ein Rückschluss auf die teilnehmenden Institutionen ist nicht möglich. Die Ergebnisse der Umfrage machen deutlich, dass Cyber-Risiken als eine der größten Bedrohungen für den Erfolg der Digitalisierung wahrgenommen werden.

Knapp 70 Prozent der Unternehmen und Institutionen in Deutschland sind in den Jahren 2016 und 2017 Opfer von Cyber-Angriffen geworden. In knapp der Hälfte der Fälle waren die Angreifer erfolgreich und konnten sich zum Beispiel Zugang zu IT-Systemen verschaffen, die Funktionsweise von IT-Systemen beeinflussen oder Internet-Auftritte von Firmen manipulieren. Jeder zweite erfolgreiche Angriff führte dabei zu Produktions- bzw. Betriebsausfällen. Hinzu kamen häufig noch Kosten für die Aufklärung der Vorfälle und die Wiederherstellung der IT-Systeme sowie Reputationsschäden.

Von den verschiedenen Angriffsarten fanden Malware-Infektionen am häufigsten statt. Knapp 57 Prozent der berichteten Angriffe waren Infektionen, bei denen Schadprogramme in betriebliche IT-Systeme eindrangen, um schädliche Operationen auszuführen. Hacking-Angriffe, wie beispielsweise die Sabotage von industriellen Steuerungssystemen, Datendiebstahl oder die Manipulation von Internet-Auftritten, machten 19 Prozent, DDoS-Attacken, die durch Überlastung zum Ausfall von Webseiten und anderen Netzinfrastrukturen führen, machten 18 Prozent der erfolgreichen Angriffe aus.

Das Bewusstsein für die Gefahren, die den Unternehmen aus dem Cyber-Raum drohen, ist hoch. So schätzten insgesamt rund 92 Prozent der Befragten die Gefahren als kritisch für die Betriebsfähigkeit ihrer Institution ein. Nur knapp 42 Prozent gingen davon aus, dass der Betrieb im Fall eines Cyber-Angriffs durch Ersatzmaßnahmen aufrechterhalten werden könnte. Als besonders gefährdet betrachteten sich große Konzerne. Von diesen glaubten nur knapp 38 Prozent, dass der Betrieb im Fall eines Cyber-Angriffs fortgeführt werden könnte.

Viele Betriebe haben bereits umfassende Cyber-Sicherheitsmaßnahmen eingeleitet. 89 Prozent der Befragten gaben an, dass Maßnahmen wie Segmentierung oder die Minimierung von Netzübergängen ergriffen wurden, um die Netze abzusichern. Auch Maßnahmen zur Abwehr von Viren fanden häufig Anwendung (86 Prozent). Dabei kamen sowohl Maßnahmen zur zentralen Detektion, wie etwa Scans am Sicherheitsgateway, an Mailservern usw., als auch dezentrale Maßnahmen wie Scans auf Client-/Server-Systemen zum Einsatz.

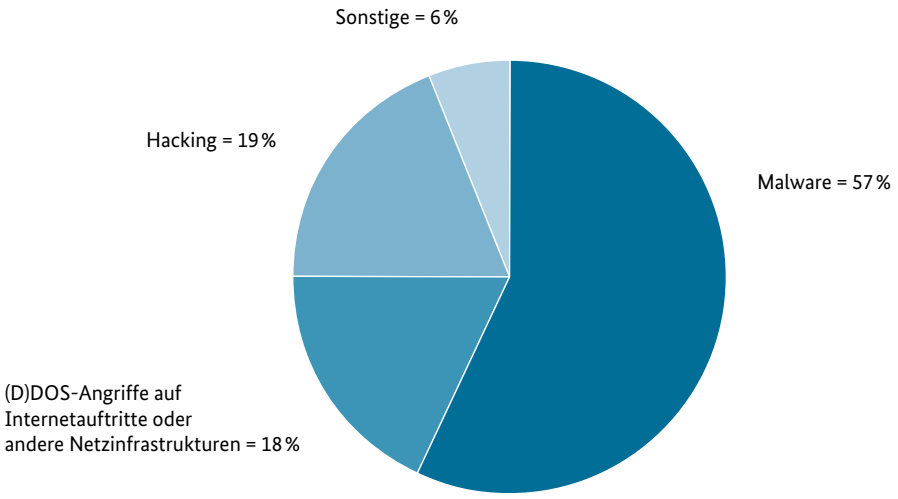


Abbildung 03 Welcher Art waren die Angriffe?

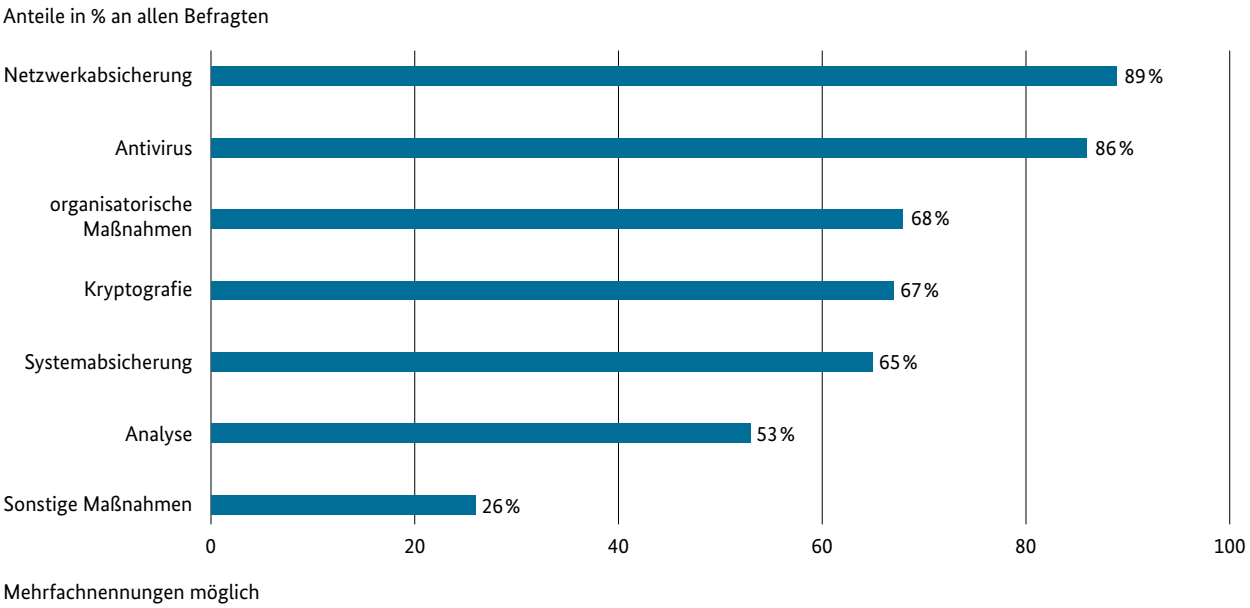


Abbildung 04 Welche Maßnahmen werden aktuell in Ihrer Institution zum Schutz gegen Cyber-Angriffe umgesetzt?

Über die bereits umgesetzten Maßnahmen hinaus, sind in vielen Betrieben (71 Prozent) weitere Verbesserungen der Cyber-Sicherheit geplant. Von ihnen gaben rund 13 Prozent an, dass sogar kurzfristig dringende Verbesserungen in kritischen Bereichen geplant sind. Ein Teil der Unternehmen hat erkannt, dass für eine ganzheitliche Informationssicherheit auch der Faktor Mensch von Bedeutung ist. So führen mehr als die Hälfte der Unternehmen regelmäßige Schulungen ihrer Beschäftigten zu Fragen der Cyber-Sicherheit durch. Weitere knapp 20 Prozent der befragten Unternehmen planen entsprechende Maßnahmen. Allerdings sagten knapp 30 Prozent der Befragten, dass IT-Sicherheits-Schulungen nicht stattfinden und auch nicht geplant sind.

Ein Viertel der befragten Unternehmen verfügt heute über ein Cyber-Sicherheits-Monitoring. 29 Prozent der großen

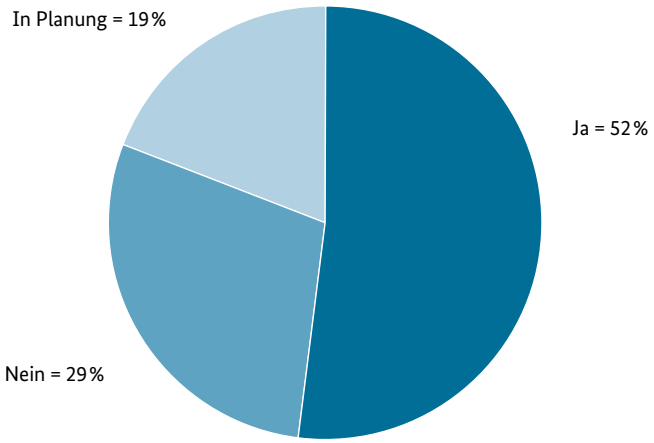


Abbildung 05 Wird das Personal in regelmäßigen Abständen in Bezug auf die IT-Sicherheit geschult und die Durchführung dieser Schulungen dokumentiert?

Unternehmen und 23 Prozent der Kleinen und Mittleren Unternehmen (KMU) werten Log-Dateien regelmäßig und systematisch aus. Gut die Hälfte aller Unternehmen untersucht Log-Files nur bei konkreten Anlässen. Ein Nachholbedarf kleiner und mittlerer Unternehmen lässt sich bei den Planungsaktivitäten erkennen. Während rund 17 Prozent der großen Unternehmen plant, Log-Daten zu nutzen, trifft dies nur auf elf Prozent der kleinen und mittleren Unternehmen zu.

Besondere Aufmerksamkeit widmen die Unternehmen nach eigenen Angaben reaktiven Maßnahmen für den Fall eines Cyber-Angriffs. So gaben rund 58 Prozent der Befragten an, dass Richtlinien wie etwa Notfallpläne oder Störfallanweisungen existieren, die die Wiederherstellung des Betriebs nach einer schwerwiegenden Betriebsstörung beschreiben. Dabei traten erneut Unterschiede zwischen kleinen, mittleren und großen Unternehmen zutage. Während zwei von drei großen Unternehmen über eine solche Richtlinie verfügen, traf dies nur auf gut jedes zweite kleine oder mittlere Unternehmen zu.

Adäquate und aktuelle Notfallpläne sind eine besonders wichtige Maßnahme zur Erhöhung des Sicherheitsniveaus. Letztlich wird hier die Qualität der Resilienz entscheidend geprägt. Der Schlüsselfaktor Resilienz, der in Zukunft immer bedeutsamer wird, sollte sowohl bei großen Unternehmen als auch bei KMU mehr Bedeutung bekommen. Vorfalltrainings sind hier ein wichtiger Faktor. Der Anteil der hier gut aufgestellten Unternehmen muss weiter verbessert werden, die Allianz für Cyber-Sicherheit und viele Kräfte des BSI setzen sich hierfür kontinuierlich ein.

1.3 Gefährdungslage Gesellschaft

Die Digitalisierung durchzieht zunehmend den Alltag. Sie bietet neue Möglichkeiten für die Zivilgesellschaft, weist system- und technologiebedingt aber auch Risiken auf. Durch die zunehmende Vernetzung nahezu aller Lebensbereiche erhalten die Bürgerinnen und Bürger stetig mehr Zugang zu digitalen Infrastrukturen, Dienstleistungen, Endgeräten und Datenquellen, mit denen sie täglich interagieren. IT-Lösungen sind ein selbstverständlicher Faktor in vielen gesellschaftlichen Lebensbereichen. Sie erleichtern die medizinische Versorgung, sie steuern die Stromnetze, verbessern die Nutzung erneuerbarer Energien und machen unsere Fahrzeuge umweltschonender. Daneben eröffnet die Digitalisierung individuelle Handlungsmöglichkeiten. Hierzu zählen gestalterische Möglichkeiten wie die Verbreitung von Informationen, aber auch zerstörerische Handlungen wie Manipulationen oder Datendiebstahl. Cyber-Sicherheit im Sinne von umfassenden IT-Sicherheitsvorkehrungen ist daher die Voraussetzung für eine erfolgreiche Digitalisierung.

1.3.1 Ergebnisse und Erkenntnisse aus Umfragen

Im Rahmen ihrer Kooperation haben das BSI und das Programm Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) im Oktober 2017 durch eine repräsentative Onlinebefragung erheben lassen, ob und wie sich die Befragten vor Gefahren im Internet schützen und ob sie schon einmal Opfer von Kriminalität im Internet geworden sind. Dabei stellte sich heraus, dass für 97 Prozent der Internetnutzer in Deutschland Sicherheit bei der Nutzung des Internets von großer Bedeutung ist. Allerdings stehen das Informationsverhalten und die tatsächlich genutzten Schutzmaßnahmen diesem hohen Sicherheitsbedürfnis teils diametral entgegen:

Die der Informationssicherheit zugestandene hohe Bedeutung führt nicht zwangsläufig zu einem sicherheitsbewussten Verhalten der Nutzer. Nur rund jeder Dritte (30 Prozent) informiert sich gezielt zum Thema IT-Sicherheit. Sicheres Surfen interessiert die Bürger vor allem dann, wenn es um finanzielle Aspekte geht: Für 71 Prozent aller Befragten ist speziell beim Online-Banking die Sicherheit besonders wichtig, nur noch 45 Prozent sind beim Online-Shopping auf eine sichere Abwicklung bedacht. Die sichere Nutzung von sozialen Netzwerken (elf Prozent), Cloud-Diensten (acht Prozent) und vernetzten Heimgeräten zur Haussteuerung (vier Prozent) ist den Befragten dagegen kaum bis gar nicht wichtig.

Über die Hälfte der Befragten informiert sich nur im Problemfall zum Thema IT-Sicherheit. Während zwei Drittel der Befragten Antivirenprogramme und eine Firewall nutzen, werden andere essentielle Schutzmaßnahmen von deutlich weniger Nutzern in die Tat umgesetzt. So achtet weniger als die Hälfte auf eine sichere Übertragung persönlicher Daten (45 Prozent), lediglich 37 Prozent installieren verfügbare Updates sofort. Und nur etwa jeder fünfte Nutzer (21 Prozent) legt regelmäßig Sicherheitskopien seiner Daten an.

Nach eigenen Aussagen waren 59 Prozent der Befragten noch nie Opfer von Kriminalität im Internet. 19 Prozent geben an, Opfer von Schadsoftware geworden zu sein, acht Prozent von Betrug beim Online-Shopping und sechs Prozent von Phishing. Von den 823 Befragten, die Opfer von Kriminalität im Internet geworden sind, hat über die Hälfte (52 Prozent) IT-Probleme selbst gelöst, rund ein Viertel (24 Prozent) bat Familie, Freunde oder Bekannte um Hilfe und nur rund jeder Fünfte (19 Prozent) erstattete Anzeige bei der Polizei. Die Ergebnisse der Umfrage fließen in die weitere gemeinsame Aufklärungsarbeit von Polizei und BSI ein.

1.3.2 Sicherheit von Medizinprodukten

Mit fortschreitender globaler Digitalisierung hält diese auch Einzug in das Gesundheitswesen, so dass vermehrt vernetzte Medizinprodukte entwickelt und in Verkehr gebracht werden. Diese Produkte weisen verschiedene Arten von Schnittstellen auf, die sich auf unterschiedliche Weise in Netzwerke einbinden lassen und zum Teil mit mobilen Anwendungen (Apps) zur Verwaltung von personenbezogenen Daten verknüpft werden können. Vor allem eine gesteigerte Funktionalität und ein höheres Maß an Komfort für den Patienten begünstigen diese Entwicklung, denn die Vernetzung garantiert einen nahezu uneingeschränkten und ortsungebundenen Zugriff auf die eigenen Daten. Durch kabellose Technologien ist auch für Ärzte der Zugriff auf dokumentierte Patientendaten und die Kommunikation mit dem System selbst viel einfacher. Besonders bei implantierbaren aktiven Medizinprodukten, wie Herzschrittmachern, Defibrillatoren (implantierbarer Kardioverter-Defibrillator, ICD), Neurostimulatoren und Cochlea-Implantaten zeigen sich klare Vorteile gegenüber älteren Systemen, denn die kabellose Kommunikation lässt früher zusätzlich erforderliche operative Eingriffe am Patienten, z. B. zur Prüfung der Funktionsweise des Gerätes, überflüssig werden. Solche aktiven Medizinprodukte haben einen hohen Sicherheitsanspruch, da sie im Normalfall eine relativ lange Lebens- beziehungsweise Verweildauer im Körper des Patienten haben und oft lebensnotwendige Funktionen übernehmen. Deswegen ist es wichtig, mögliche Sicherheitsbedrohungen frühzeitig zu erkennen, zu bewerten und entsprechende Gegenmaßnahmen zu entwickeln, um die Patientensicherheit über einen langen Zeitraum hinweg gewährleisten zu können.

Mit steigendem Vernetzungs- und Verbreitungsgrad von „smarten“ Medizinprodukten ist davon auszugehen, dass sich nicht nur das Produkt- und Anwendungsportfolio erhöht, sondern auch das Risiko eines Cyber-Angriffs größer wird, verbunden mit einer möglichen Gefährdung der Patientensicherheit. Vorwiegend in den USA, aber auch in Deutschland, konnte unter Laborbedingungen bereits nachgewiesen werden, dass die verschiedenen medizinischen Geräte (Herzschrittmacher, Defibrillatoren, Beatmungsgeräte, Infusionspumpen) nicht sicher vor einem Cyber-Angriff sind. So wurde am Beispiel eines Defibrillators (implantierbarer Kardioverter-Defibrillator, ICD) gezeigt, dass dieser, lediglich durch Kenntnis der Modell- und Seriennummer, ferngesteuert und umprogrammiert werden konnte. Die IT-Sicherheit muss daher auch bei der Entwicklung und Herstellung von Medizinprodukten von Anfang an eine wichtige Rolle spielen („security by design“ und „security by default“), damit ein sicherer Einsatz jederzeit gewährleistet werden kann.

Oftmals sind die Authentisierungsmechanismen von digitalisierten Medizinprodukten nicht ausreichend gesichert und es werden schwache oder überhaupt keine Verschlüsselungstechniken für die Kommunikation und Speicherung von Daten verwendet. In solchen Fällen wäre es möglich, dass sich in Unwissenheit des Patienten unbefugt Zugriff verschafft und das Gerät manipuliert werden könnte. Um jedoch in einem Notfall als Arzt möglichst schnellen Zugriff auf beispielsweise einen implantierten Defibrillator zu haben, wurden die Sicherheitsmechanismen teilweise bewusst niedrig gehalten, da komplizierte Zugriffsmechanismen zeitaufwändig sind und die Bedienung des Medizinproduktes unter Zeitdruck in einer solchen Notfallsituation schlimmstenfalls zu Lasten des Patientenwohls gehen würden. Am Beispiel des implantierbaren Defibrillators wird zudem deutlich, dass es nicht unproblematisch ist, stärkere Sicherheitsmerkmale zu implementieren. Ein solcher Defibrillator hat die Größe einer Streichholzschachtel und ist batteriebetrieben. Die Batterielebensdauer beträgt etwa 4 bis 6 Jahre, so dass ICD-Patienten regelmäßige operative Eingriffe für den Austausch einplanen müssen. Sobald mehr Speicherplatz oder bessere Verschlüsselungstechniken eingesetzt würden, ginge dies zu Lasten der Größe des Defibrillators und/oder der Batterielaufzeit. Dies bedeutet, dass sich die Verweildauer des Medizinprodukts im Patienten verkürzt und eine zusätzliche Operation notwendig wäre. Der Kompromiss zwischen Funktionalität und ausgereifter IT-Sicherheitstechnik wird hier besonders deutlich.

Da die Gefährdungslage prinzipiell als kritisch zu betrachten ist, sind in Zukunft verstärkt geeignete IT-Sicherheitsmechanismen für Medizinprodukte zu entwickeln. Das BSI reagiert in Zusammenarbeit mit den zuständigen Aufsichtsbehörden auf diese Entwicklungen. Weitere Sicherheitseigenschaften von Medizinprodukten sollen in demnächst startenden Projekten ermittelt und genauer untersucht werden.

1.3.3 Sicherheit von Mobile Banking

Im Internet werden verschiedenste Zahlungsdienste angeboten. Es gibt Anbieter von Zahlungskonten für Händler und Kunden wie Paypal, Kreditkartenlösungen wie 3D-Secure, lastschriftenbasierten Lösungen wie bei Amazon sowie Ausführungen wie z. B. giropay oder iDeal, die die Kunden zu einer Bankwebseite weiterleiten. Dazu zählt auch die SofortÜberweisung der Sofort GmbH (jetzt Klarna), die den Zahlungsauftrag zu dem kontoführenden Zahlungsdienstleister weiterleitet.

Die Zahlungen erfolgen jedoch nicht mehr nur mittels eines PCs, sondern vermehrt mit mobilen Geräten wie Smartphones oder Tablets.

Immer mehr Banken bieten Online-Banking-Anwendungen (Online-Banking-Apps) für mobile Geräte an. Neben den eigenen Apps der größeren Banken werden auch freie multibankfähige Apps angeboten, die es ermöglichen, Konten bei verschiedenen Banken zu verwalten. Zusätzlich werden diese Banking-Apps häufig mit einer zweiten Anwendung kombiniert, der sogenannten TAN-App. Diese generiert eine Transaktionsnummer (TAN), um die in der Banking App getätigte Transaktion abzusichern.

Die einzelnen Bezahlverfahren sind mit den unterschiedlichsten Risiken für den Nutzer, die Händler und auch die Kreditinstitute des Kunden verbunden. Dabei sind Sicherheit und Komfort die wichtigsten Aspekte, die Nutzer des Mobile Bankings von ihrem Bezahlverfahren/ihrer Banking App erwarten.

Zur Sicherheit trägt beispielsweise die Art und Weise der Anmeldung an der Banking App und natürlich die Art der Transaktionsabsicherung bei. Aus vermeintlichen Komfortgründen wird dabei gerne auf das Ein-Geräte-Banking zurückgegriffen. Hierbei laufen die Banking App und die App zur Generierung der TAN auf dem gleichen Gerät. Doch die Installation der Banking- und der TAN-App auf einem Gerät birgt Risiken: Ist das mobile Gerät kompromittiert, kann ein Angreifer möglicherweise Zugriff auf beide Apps erhalten und hat damit volle Kontrolle über das Konto.

Hack der Promon-Shield-Lösung

Während des 34. Chaos Communication Congress (34C3) im Dezember 2017 in Leipzig zeigte der Erlanger Sicherheitsforscher und Doktorand Vincent Haupert, wie sich die Sicherheitslösung der Firma Promon, das sogenannte Promon Shield, auf einfache Weise umgehen lässt.

Sachverhalt
Das Promon Shield ist eine Sicherheitslösung des norwegischen Unternehmens Promon, die direkt in Anwendungen, Webservices oder Apps integriert werden kann. Sie soll dafür sorgen, dass diese gegen Angriffe von Schadsoftware geschützt sind.

Dazu sind keine Signaturen einer Schadsoftware notwendig. Eingesetzt wird die Sicherheitslösung von verschiedenen Banken zum Schutz ihrer Banking Apps, d. h. es wird eine Sicherheitslösung in verschiedenen Anwendungen eingesetzt.

Durch die Härtung mit der Sicherheitslösung sollen die entsprechenden Apps gegen Angriffe geschützt sein. D. h. die Software soll das Banking auf kompromittierten Geräten verhindern und interagiert dafür mit der TAN-App. Der mit dem Promon Shield eingebaute Schutzmechanismus wird wirksam und ermöglicht einen sicheren Zugriff. Insgesamt verwenden 31 verschiedene Apps für das Online-Banking das Promon Shield zur Absicherung.

Ursache/Schadenswirkung
Durch einen Hacking-Angriff mit dem Tool Nomorp gelang es deutschen Informatikern, die Schutzmechanismen von Promon Shield auszuschalten und Transaktionsvorgänge zu manipulieren.

Dies gelang durch Sicherheitslücken, durch die die Schutzmechanismen von Promon ausgehebelt werden konnten. Ein von den Hackern entwickelter Beispielcode erlaubte es, die Kontrolle über die Banking-App eines Opfers zu erhalten und Transaktionen zu verändern.

Reaktion
Das BSI wird sich in einem gerade gestarteten Projekt mit der Vielfalt der verschiedenen mobilen und auch online zu nutzenden Bezahlverfahren beschäftigen. Ziel ist es, die allgemeinen Sicherheitseigenschaften in einer Sicherheitsbetrachtung zu untersuchen und Handlungsempfehlungen zu formulieren.

Empfehlung
Das BSI empfiehlt beim Online-Banking den Einsatz der sogenannten Zwei-Faktor-Authentifizierung, bei der die Transaktionsnummer (TAN) auf einem separaten Gerät erzeugt wird. Die Verwendung einer Banking-App und einer TAN-App auf demselben Gerät ist nicht sicher. Wer nicht auf Mobile Banking verzichten möchte, sollte zur Generierung einer TAN ein zweites Gerät z. B. auch einen ChipTAN Generator einsetzen. Im genannten Fall liegt eine sichere Zwei-Faktor-Authentifizierung nur vor, wenn die TAN auf einem separaten Gerät erzeugt wird.

1.3.4 Smart Home und das Internet der Dinge

Im Internet der Dinge (Internet of Things, IoT) lassen sich immer mehr beliebige Gegenstände durch immer erschwinglichere Hardware und steigende Akkuleistung bei gleichzeitig sinkendem Stromverbrauch untereinander und mithilfe von Apps vernetzen. Beliebte Anwendungsbereiche von IoT-Geräten sind Haushaltsgeräte, die Hausüberwachung oder das Gesundheitsmanagement (z. B. Wearables). Stetig kommen neue Anwendungen und vernetzte Geräte auf den Markt, die zuvor analoge Welten mit der digitalen verbinden. Eine wachsende Anzahl von Herstellern beginnt damit, ihre Produktpalette um smarte Lösungen zu erweitern. Für den Benutzer trägt dies in vielen Fällen zur Komfortsteigerung und Kontrolle in seinem Heim oder seiner Umgebung bei.

Für eine Kaufentscheidung des Kunden sind in der Regel die Gerätefunktionalität und der damit verbundene Komfortgewinn sowie der Kaufpreis ausschlaggebend, weniger hingegen Fragen der IT-Sicherheit. Feststellbar ist jedoch, dass häufige Berichte über IT-Sicherheitsvorfälle bei Verbrauchern und Herstellern zu einem wachsenden Bewusstsein für die Risiken durch vernetzte Geräte beigetragen haben. Viele Frameworks und Protokolle, die im Internet der Dinge eingesetzt werden, bieten mittlerweile mehr Sicherheitsfunktionen und setzen diese ein. Außerdem wird schneller auf Schwachstellen in den Geräten reagiert. Dennoch bietet allein die schiere Anzahl der mit dem Internet verbundenen und nicht ausreichend gesicherten Geräte weiterhin ein lohnendes Ziel, das von Cyber-Kriminellen für ihre Zwecke genutzt werden kann.

Offene OBD-II-Schnittstelle in Fahrzeugen

Sachverhalt
Die OBD-II-Schnittstelle (On-Board-Diagnose) ist eine Schnittstelle, die in allen seit 2003 hergestellten und in Europa zugelassenen Kraftfahrzeugen vorhanden ist. Sie bietet den Zugriff auf die CAN-Busse, die alle elektronischen Komponenten des Fahrzeugs verbinden. Die ursprüngliche Funktion der Schnittstelle liegt in der Überwachung von Abgasvorschriften, jedoch kann und wird sie seither für weitere Kontrollen des Fahrzeugs genutzt, wie z. B. für die herstellerspezifische Fehlerdiagnose in Werkstätten.

Eine weitere Nutzungsmöglichkeit ist der Anschluss sogenannter Dongles. Diese werden an die OBD-II-Schnittstelle angebracht und schicken, z. B. während der Fahrt per Mobilfunkverbindung, Diagnosedaten an Versicherer oder Autovermietungen. Dadurch erhält das fahrzeuginterne Netzwerk zusätzlich eine drahtlose Schnittstelle.

Ursache/Schadenswirkung
Bauartbedingt können über OBD-II nicht nur Daten aus dem Fahrzeug ausgelesen werden, sondern auch Befehle in das interne Netz eingespielt werden. Die Dongles unterliegen jedoch keinerlei Zulassungskontrollen. Da sie Schnittstellen in das Fahrzeug bieten, die nicht immer durch das Sicherheitskonzept des Fahrzeugherstellers abdeckt werden können, eröffnen sich dadurch zusätzliche Risiken. 2015 zeigten Forscher, dass sie in der Lage sind, manipulierte SMS an bestimmte Dongles zu verschicken und so Einfluss auf die Bremsfunktionen bei niedrigen Geschwindigkeiten zu nehmen. Im Jahr 2017 wurde nachgewiesen, dass die Bluetooth-Verbindung eines Dongles angegriffen werden konnte und auch so Einfluss auf Fahrfunktionen genommen werden konnte.

Reaktion
Eine unmittelbare Reaktion des BSI war in diesem Fall nicht erforderlich. Zur genaueren Einschätzung der Bedrohungslage wird das BSI künftig entsprechende Sicherheitsanalysen der Schnittstellen von Kraftfahrzeugen durchführen. Ziel ist es, Sicherheitslücken in enger Abstimmung mit den Herstellern zu entdecken und zu beheben, bevor diese ausgenutzt werden können.

Empfehlung
Grundsätzlich sollten Fahrzeugbesitzer klar über die möglichen Folgen einer Integration von ungeprüften Zubehörteilen wie z. B. OBD-II-Dongles in die Fahrzeugelektronik informiert werden. Es wird angeregt, speziell die Dongles zukünftig ebenso Prüfungen zu unterziehen, wie es auch schon bei anderen Fahrzeugkomponenten im Rahmen der Typgenehmigung der Fall ist. Eine Möglichkeit hierzu wäre der Einsatz von Zertifizierungsstandards wie Common Criteria.

Im Gegensatz zu herkömmlichen mit dem Internet verbundenen Geräten wie PCs, Laptops und Servern, besitzen IoT-Geräte häufig keine eigenen Angriffspräventionssysteme. Im Vergleich mit PCs stehen ihnen, um Kosten zu reduzieren und die Akkulaufzeit zu erhöhen, in der Regel deutlich knappere Ressourcen für Sicherheitsmechanismen zu Verfügung. IoT-Geräte können darum nicht nur einfacher kompromittiert werden, es ist auch deutlich schwerer, diese Kompromittierungen zu erkennen. So bemerken die Besitzer von infizierten IoT-Geräten häufig keine Veränderungen, solange das Gerät noch seine reguläre Funktion ausführt.

Durch IP- und Port-Scans u.a. mit speziellen Suchmaschinen lassen sich mit überschaubarem Aufwand über das Internet genügend IoT-Geräte finden und anschließend kompromittieren, um beispielsweise schlagkräftige Botnetze aufzubauen. Zudem sind Angriffswerkzeuge bekannt geworden, die automatisiert Schwachstellen ausnutzen. Neben Angriffen über das Internet können auch lokale Funk- oder Kabelschnittstellen von einem Angreifer für unterschiedliche Zwecke missbraucht werden.

Zwei Gefährdungslagen

Zu unterscheiden ist zwischen zwei Gefährdungslagen: Bei der ersten Gefährdungslage wird das IoT-Gerät kompromittiert, um dem Nutzer direkt oder indirekt einen Schaden zuzufügen. Zu den Bedrohungen in dieser Gefährdungslage gehören:

- Manipulation von Daten:
  Ein Angreifer kann sich z. B. durch eine manipulierte Zutrittssteuerung unerlaubten Zutritt zum Gebäude verschaffen oder über manipulierte Daten in der Hausklimatisierung Schaden anrichten.

- Ausspähen von Daten:
  IoT-Geräte können über verschiedenste Sensoren verfügen. Ein kompromittiertes Gerät kann entsprechende Daten an den Angreifer weiterleiten, der auf diese Weise an sensible Informationen gelangen kann.

- Sabotage von IoT-Geräten:
  Das Gerät wird durch den Angreifer außer Betrieb gesetzt und ist für den Besitzer zumindest vorübergehend nicht mehr nutzbar. Je nach Gerät kann es dabei ebenfalls zu relevanten Einschränkungen für den Besitzer kommen.

- IoT-Geräte als Hintertür:
  Man kann unzureichend gesicherte IoT-Geräte als Hintertür nutzen, um sich Zutritt zum Heim- oder Firmennetzwerk zu verschaffen.

Bei der zweiten Gefährdungslage wird das IoT-Gerät kompromittiert, um Angriffe auf weitere Ziele vorzubereiten. Das Gerät selbst ist nicht das Hauptziel des Angreifers, sondern Webservices oder Infrastrukturen von Dritten. Der Angriff auf das Gerät bleibt dabei häufig unbemerkt, da in diesem Fall die eigentliche Funktionalität nicht verändert werden muss. Zu den Bedrohungen in dieser Gefährdungslage gehören:

- Aufbau von Botnetzen:
  Das massenhafte Kapern von unzureichend gesicherten IoT-Geräten ermöglicht den Aufbau von großen Botnetzen, die dazu fähig sind, mittels DDoS-Attacken Webseiten und Webservices Dritter zu stören.

- Identitätsverschleierung:
  Kompromittierte Geräte können als Proxy zur Verschleierung weiterer Angriffe genutzt werden.

- Krypto-Mining:
  Die gesammelte Rechenleistung aller gekaperten IoT-Geräte kann genutzt werden, um z. B. Bitcoins zu erzeugen. Dies wurde z. B. mit dem bekannten Mirai-Botnetz versucht, aber scheinbar aufgrund mangelnder Effizienz wieder verworfen. Denkbar ist jedoch, dass bei steigender Rechenleistung auch dieses Potenzial weiter zunehmen könnte. Ein solcher Missbrauch ist jedoch einfacher feststellbar, da die Geräte unter Volllast laufen müssen und für den eigentlichen Nutzen dann merklich langsamer reagieren.

- Klickbetrug bei Werbebannern:
  Der Angreifer nutzt die vielen verschiedenen IP-Adressen von gekaperten IoT-Geräten, um Klicks auf Werbebanner, Videos oder Sozial Media Inhalte zu erzeugen. Auf diese Weise kann sich bei einer klick-bezogenen Abrechnung eine unberechtigte Provision erschlichen werden. Zudem entsteht dem Werbetreibenden ein direkter Schaden durch die Auszahlung einer Provision für simulierte Klicks.

Somit sind die möglichen Auswirkungen von Angriffen auf IoT-Geräte ebenso vielfältig wie bei PCs. Auch hier können alle IT-Schutzziele wie Vertraulichkeit, Verfügbarkeit und Integrität betroffen sein. Durch DDoS-Attacken oder die Manipulation von Daten kann es zu hohen wirtschaftlichen Schäden für direkt Betroffene, Dritte oder sogar zu Beeinträchtigungen an Kritischen Infrastrukturen kommen.

1.3.5 Identitätsmissbrauch durch Fernidentifizierungsverfahren

Um ihre Kunden bei Online-Transaktionen identifizieren zu können, bieten Banken, Telekommunikationsunternehmen oder andere Dienstleister zunehmend Online-Verfahren an. Während mit der Online-Ausweisfunktion des Personalausweises oder elektronischen Aufenthaltstitels ein hohes Sicherheitsniveau erreicht werden kann, sind weiterhin auch Verfahren im Einsatz, deren Sicherheit nicht das Niveau einer persönlichen Identifizierung und Überprüfung eines Ausweisdokuments erreicht.

Unsichere Identifizierung über Videokanal

Insbesondere die in einigen Anwendungsgebieten weiterhin angebotenen Verfahren, die eine Identifizierung innerhalb eines Videochats ermöglichen sollen, bieten Missbrauchspotenzial. Ein mit dem Smartphone aufgenommenes Videobild des Nutzers und seines Ausweises ist in Bezug auf Eindeutigkeit und Sicherheit nicht vergleichbar mit einer Identifizierung bei physischer Anwesenheit. Ohnehin lassen sich über einen Videokanal höchstens Sicherheitsmerkmale prüfen, die sich bei bestimmten Lichtverhältnissen unter Bewegung des Ausweises ver-

Ein Beispiel zu ID-Diebstahl

Sachverhalt
Das Bundeskriminalamt (BKA) veröffentlichte am 05. Juli 2017 in einer Kurzmeldung den Fund von knapp 500 Millionen Datensätzen bestehend aus E-Mail-Adressen und dazugehörigen Passwörtern https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/170705_HackerSammlung.html . Die Herkunft des gefundenen Datensatzes sowie dessen Alter waren nicht bekannt.

Ursache/Schadenswirkung
Wenn es sich bei den bekannt gewordenen Daten um die Zugangsdaten für ein E-Mail-Konto handelt, könnte ein Angreifer diese für unterschiedliche Zwecke verwenden. So können etwa Spam-Nachrichten bzw. Schadsoftware im Namen der angegriffenen Person versendet werden. Des Weiteren können die im Kontaktbuch hinterlegten Adressen zum Ziel von Spam-, Schadsoftware- oder Social-Engineering-Angriffen werden. Sollte es sich bei den veröffentlichten Daten aber auch um Zugangsdaten für Shops, soziale Medien oder andere Plattformen handeln, könnte ein Angreifer zum Beispiel Chat-Verläufe mitlesen und hinterlegte Kreditkarten oder weitere persönliche Informationen wie Telefonnummer, Anschrift usw. erhalten.

Reaktion
Das BSI erhält häufig Hinweise auf Funde von Identitätsdaten im Internet, z. B. durch Strafverfolgungsbehörden oder eigene Beobachtungen. In den meisten Fällen ist jedoch nicht erkennbar, inwieweit es sich bei den gefundenen Daten um veraltete oder aus anderen Gründen nicht mehr relevante Datensätze handelt. Die Ursache dafür ist, dass die gefundenen Daten häufig aus verschiedenen, bereits anderweitig veröffentlichten Daten-Leaks stammen, einfach zusammengelegt und anschließend als „neu“ angepriesen werden. Dadurch entstehen große Datenbanken mit mehreren Millionen Einträgen.

Empfehlung
Das BSI empfiehlt, die Angebote der Internet-Provider der Internetdienste zur Absicherung von Konten zu verwenden: Viele Internetdienste bieten ihren Kunden an, zusätzliche Sicherheitsschritte zu unternehmen, um sich vor unkontrolliertem Zugriff zu schützen. Ein Beispiel dafür ist die Zwei-Faktor-Authentisierung (meist Handynummer bzw. mittels App), um somit sicherzustellen, dass ein Zugriff nur vom Eigentümer des Kontos geschehen kann. Bei Informationen über einen Datenfund sollte der betroffene User prüfen, für welchen Dienst diese Daten gültig waren oder sind. Unterschiedliche Dienste speichern im Internet veröffentlichte Daten-Leaks und ermöglichen damit interessierten Nutzern zu überprüfen, ob ihre eigene E-Mail-Adresse schon in einem Leak vorgekommen ist. Zum Schutz der digitalen Identität im Netz können verschiedene Schutzmechanismen verwendet werden https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/ID-Diebstahl/Schutzmassnahmen/id-dieb_schutz_node.html. Hilfreich ist auch die Verwendung von unterschiedlichen Passwörtern für jeden Dienst https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html. Des Weiteren ist die Verwendung eines Passwortmanagers sinnvoll, um die unterschiedlichen Zugangsdaten einfacher zu verwalten https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/Umgang/umgang.html.

ändern, wie das holografische Porträt oder das Laserkippbild auf der Rückseite des deutschen Personalausweises. Haptische Merkmale oder auch die nur im infraroten oder ultravioletten Licht erscheinenden Sicherheitsmerkmale können aus der Ferne nicht überprüft werden.

Im Rahmen von Sicherheitsanalysen hat das BSI nachgewiesen, dass es bereits mit Standardequipment effektiv möglich ist, einen gefälschten Ausweis zu erstellen und mit diesem im Rahmen einer Videoübertragung in Echtzeit den Eindruck entsprechender individueller, optisch variabler Sicherheitsmerkmale zu erzeugen. Nach neuesten Erkenntnissen reichen auch die bisher gefundenen und verbindlich vorgeschriebenen Gegenmaßnahmen nicht mehr aus, um erfolgreiche Angriffe zu verhindern bzw. Angriffsversuche zu erkennen.

Perspektivische Entwicklung von Fernidentifizierungsverfahren

Das BSI hat die zuständigen Aufsichtsbehörden über die veränderte Bedrohungslage informiert und befasst sich mit der Entwicklung wirksamer Gegenmaßnahmen, auch in Zusammenarbeit mit den Anbietern solcher Identifizierungsdienste. Nach den bisherigen Erfahrungen ist jedoch nicht davon auszugehen, dass damit Angriffe auf hohem Angriffsniveau dauerhaft erfolgreich verhindert werden können.

Daher empfiehlt und fördert das BSI den Einsatz sicherer Alternativen, die dem Vertrauensniveau notifizierter elektronischer Identifizierungssysteme entsprechen. So wird die eID-Funktion des Personalausweises bei allen öffentlichen Einrichtungen der Europäischen Union ab dem 29. September 2018 verpflichtend anerkannt – mit der mobilen Version der AusweisApp besonders benutzerfreundlich. Mit den 2017 eingeführten Änderungen am Personalausweisgesetz sind auch die Hürden für Diensteanbieter zur Einführung der eID-Funktion deutlich gesunken, und durch die garantierte Interoperabilität ist die Anbindung aller im Ausland notifizierten eID-Systeme ohne zusätzlichen Aufwand möglich.

1.4 Angriffsmethoden und -mittel

Ein wirksamer Schutz vor Cyber-Angriffen ist nur möglich, wenn allgemeine Gefährdungen im Cyber-Raum sowie die eigene konkrete Gefährdungslage zumindest im Überblick bekannt sind. Dieses Wissen ist Voraussetzung, um geeignete präventive und reaktive Maßnahmen auszuwählen und eine Basis für eigene Risikoanalysen zu schaffen.

Ein wesentlicher Baustein der Cyber-Sicherheit ist die Abwehr von Angriffen. Aufgrund der dynamischen Entwicklung der Cyber-Sicherheitslage muss dieser Aspekt regelmäßig und gezielt neu bewertet werden. Angriffswerkzeuge und -methoden sind einfach und kostengünstig verfügbar und beschaffbar. Immer wieder werden neueste Erkenntnisse über Schwachstellen bei Soft- und Hardware bereits nach kurzer Zeit für Cyber-Angriffe genutzt. Doch trotz der großen Anzahl unterschiedlicher Angriffsziele und möglicher Angriffsmethoden lassen sich Trends und Tendenzen erkennen, die beim Aufbau einer erfolgreichen Abwehr berücksichtigt werden sollten.

1.4.1 Advanced Persistent Threats

Im Folgenden sollen unter Advanced Persistent Threats (APTs) zielgerichtete Cyber-Angriffe auf ausgewählte Institutionen und Einrichtungen verstanden werden, bei denen sich ein Angreifer persistenten (dauerhaften) Zugriff zu einem Netzwerk verschafft und diesen in der Folge auf weitere Systeme ausweitet.

Noch stärker als bei anderen Themen der IT-Sicherheit liegt die Aufmerksamkeit bei APTs meist auf den neuesten Methoden und Entwicklungen, auch wenn diese nicht notwendigerweise repräsentativ für die Gesamtsituation sind.

Zugenommen hat in der initialen Phase der Angriffe die Verwendung von Installer- und Update-Hijacking. Dabei werden auf den Webseiten oder Update-Servern von Software-Herstellern Installationsarchive mit Schadcode versehen. Wenn die Nutzer die Programme herunterladen und installieren, wird dadurch auch ein eingeschleustes Schadprogramm ausgeführt, das wiederum weitere Module nachladen kann.

Für die Täter ist diese Methode effizient, da die Nutzer die eingefügten Schadprogramme (nichtwissentlich) selbst installieren, und je nach Art des legitimen Programms, eine größere Zahl von Zielen kompromittiert werden kann. Durch die letztere Eigenschaft steigt jedoch auch die Wahrscheinlichkeit, dass die Kampagne von Sicherheitsfirmen entdeckt wird. Nachhaltig lässt sich dieser

Angriffsweg vor allem durch die Hersteller von Software verhindern, indem diese ihre Webseiten vor Angriffen schützen, die dort bereitgestellte Software signieren und die Signatur-Schlüssel nur auf isolierten Systemen lagern. Beispiele für Installations-Hijacking-Angriffe sind Shadowpad, *NotPetya*, sowie Angriffe auf CCleaner sowie zwei weitere legitime Programme (ein Administrations-Werkzeug und ein Textverarbeitungsprogramm). Mitunter wird diese Vorgehensweise auch Supply-Chain-Angriff genannt. Genaugenommen versteht man darunter jedoch, dass die Täter zunächst Zulieferer des eigentlichen Ziels angreifen, um dann dessen Netzwerkzugänge zu nutzen, um in das eigentliche Zielnetzwerk zu gelangen. Auch dies ist eine aktuelle Vorgehensweise, die u.a. von Gruppen wie APT10 im Rahmen der CloudHopper-Kampagne eingesetzt wird.

Neben diesen aktuellen Trends sind in der initialen Phase eines Angriffs weiterhin Spearphishing-Mails mit maliziösen Links oder Anhängen üblich. Die Links können entweder auf Schadcode verweisen oder auf Phishing-Seiten für Zugangsdaten von Webmail-Postfächern oder VPNs. Im Nahen Osten sind mehrere Fälle bekannt, in denen vermeintlich legitime Smartphone-Apps in App-Stores von Drittanbietern mit Schadcode versehen wurden.

Eine der späteren Phasen von APTs ist das Lateral Movement, bei dem sich die Täter innerhalb des betroffenen Netzwerks ausbreiten. Hier setzt sich der Trend der letzten Jahre fort, möglichst mit den Ressourcen zu arbeiten, die bereits auf den kompromittierten Rechnern vorhanden sind. Die Täter nutzen legitime Administrations-Werkzeuge wie PowerShell und Windows Management Instrumentation (WMI). Dadurch sind ihre Aktivitäten weniger auffällig. Ein anderer Trend ist die Verwendung von öffentlich verfügbaren Werkzeugen, die anders als die Administrationswerkzeuge nicht auf Standard-Installationen vorhanden sind. Mehrere Tätergruppen setzen beispielsweise unabhängig voneinander öffentlich verfügbare Versionen des Penetrationstest-Werkzeugs Cobalt Strike ein. Dies kann wie eine komfortable Backdoor verwendet werden. Andere öffentlich verfügbare Werkzeuge sind Powershell Empire und Koadic. Für die Täter hat dies zwei Vorteile: Zum einen sparen sie Entwicklungsaufwand, zum anderen erschwert dies die Zuordnung von Angriffen.

Allerdings sollte dieser Trend nicht überbewertet werden. Öffentlich verfügbare Schadprogramme werden nach Einschätzung des BSI niemals eigene Entwicklungen komplett ersetzen. Zum einen haben Täter immer wieder spezielle Anforderungen, um die zielgerichteten Angriffe möglichst effizient durchführen zu können, zum anderen steigt durch den Einsatz von bekannter Schadsoftware die Wahrscheinlichkeit der Detektion durch Sicherheitsprodukte. Dementsprechend ist zu beobachten, dass Tätergruppen weiterhin eigene Schadsoftware entwickeln und diese parallel zu öffentlich verfügbaren Werkzeugen einsetzen.

Als Schutz vor APTs kann nur ein ganzheitliches Sicherheitskonzept dienen. Einige zentrale Maßnahmen sind dabei die folgenden:

- Als Schutz vor Phishing ist die Zwei-Faktor-Authentifizierung für VPN und Webmail geeignet.
- Das Blacklisten von Dokumentenverzeichnissen kann die initiale Ausführung von Schadprogrammen aus Mailanhängen oder dem Browser erschweren.
- Die Kommunikation zwischen Clients auf wirklich benötigte Funktionalitäten einzuschränken, erschwert den Tätern das Lateral Movement.
- Ein Schichtenmodell im Active Directory stellt sicher, dass hochprivilegierte Zugangsdaten nicht auf niedrig privilegierten Systemen verwendet werden, sodass Täter nur mit viel Aufwand an hochprivilegierte Zugangsdaten gelangen können.

Organisationen sollten unbedingt professionelle und verlässliche Fachinformationen zu Rate ziehen, um ihre eigene Gefährdungslage einzuschätzen. Denn derzeit berichten Medien verstärkt über Angriffe, die politische Relevanz haben. Die kontinuierlichen Angriffe auf Unternehmen zum Zweck der Wirtschaftsspionage erhalten hingegen wenig Aufmerksamkeit. Die öffentliche Berichterstattung ist nicht zwangsläufig repräsentativ oder umfassend.

Zur Abwehr von APT-Angriffen sollten Unternehmen und Institutionen idealerweise zunächst allgemeine (täter-agnostische) Standard-Techniken der IT-Sicherheit umsetzen. Dabei ist es wichtig, entweder standort- und ggf. länderübergreifend ein einheitliches Sicherheitsniveau zu erreichen oder konsequent Netzbereiche mit unterschiedlichem Sicherheitsniveau voneinander zu isolieren. Wenn die Standard-Techniken flächendeckend umgesetzt wurden, können ggf. zusätzliche (täter-spezifische) Maßnahmen umgesetzt werden, die auf der branchen- und regionsspezifischen Bedrohungslage beruhen. Einen Überblick über die Täter-Gruppen, die in verschiedenen Branchen relevant sind, bietet die folgende Grafik.

Regierungseinrichtungen	Militär/ Rüstung	Opposition	Medien	Energie	Finanzen	Telko	NGO	Universitäten	High-Tech	Transport/ Logistik	Luft- und Raumfahrt	Gesundheit	Kanzleien
APT12/ NumberedP. APT28/ Sofacy APT29/ CozyBear APT32/ OceanLotus APT37/ Reaper Bahamut BlueMushroom Cadelle/ Chafer Callisto CharmingKitten DarkCaracal DarkHotel DroppingElephant EmissaryPanda ExtremeJackal Gamaredon GazaCybergang Greenbug HammerPanda Infy KeyBoy Lapis/ TransparentTr. Longhorn LotusPanda Machete Micropsia MuddyWater Naikon/ OverrideP. Leviathan OilRig OperationCleaver ProjectSauron Shamoon Snake Sowbug Tick TidePool/ Ke3chang Tonto TranspanentTribe TropicTrooper/ PirateP. Vermin ViceroyTiger	APT28/ Sofacy APT37/ Reaper AridViper BlueMushroom Callisto CharmingKitten C-Major/ PureStrike DarkCaracal DroppingElephant Gamaredon GazaCybergang HammerPanda HelixKitten LotusPanda Machete Naikon/ OverrideP. Leviathan OilRig OperationCleaver ProjectSauron Snake	Ahtapot APT32/ OceanLotus Bahamut BlackOasis Bookworm CharmingKitten DarkCaracal EnergeticBear FlyingDragon Group5 Infy Neodymium OperationCleaver Operation Manul Promethium ScarCruft Sima StealthFalcon SunTeam TemperPanda ZooPark	APT28/ Sofacy APT32/ OceanLotus Bahamut BlackOasis BugDrop Callisto CharmingKitten DarkCaracal DarkHotel DroppingElephant GazaCybergang Infy OlympicDestroyer Operation Manul Sandworm ScarCruft ShroudedCrossbow StealthFalcon SunTeam Tick	APT10 APT18/ Wekby APT29/ CozyBear CharmingKitten ElectricPowder EmissaryPanda EnergeticBear Gaza-Cybergang Greenbug HelixKitten Kraken/ Laziok Longhorn Machete MuddyWater OnionDog OperationCleaver Sandworm Shamoon TropicTrooper/ PirateP.	APT18/ Wekby APT29/ CozyBear BlueMushroom DarkCaracal DroppingElephant EmissaryPanda EnergeticBear EquationGroup GazaCybergang HammerPanda Longhorn OilRig Sandworm	APT18/ Wekby Codoso EmissaryPanda HammerPanda HelixKitten Longhorn Machete MuddyWater OilRig ProjectSauron Thrip	APT29/ CozyBear APT37/ Reaper Callisto CharmingKitten DarkHotel HammerPanda Honeybee Infy NilePhish OperationCleaver RocketKitten	APT10/ menuPass BugDrop CharmingKitten Codoso DarkCaracal DarkHotel Greenbug DarkHotel Longhorn Leviathan RocketKitten	APT18/ Wekby CharmingKitten Codoso LEAD/ Winnti Tick	Cadelle/ Chafer NanHaiShu OilRig OnionDog ProjectSauron Shamoon	APT28 DroppingElephant EmissaryPanda Leviathan HammerPanda Greenbug Longhorn	APT10/ menuPass Leviathan LEAD/ Winnti	APT29/ CozyBear Codoso DarkCaracal DeepPanda Leviathan

Abbildung 06 Auflistung der APT-Gruppen, die zwischen 01.01.2017 und 31.05.2018 in verschiedenen Branchen aktiv waren (Quelle: BSI, Auswertung öffentlicher Berichte)

1.4.2 Angriffe auf Industrial Control Systems

Produktionssysteme sind im letzten Jahr häufig Opfer von ungezielten Angriffen gewesen. Vielfach wurden Bedienstationen oder andere Steuerungskomponenten von Ransomware befallen. Dies kommt oft vor und ist nicht spezifisch für Industrial Control Systems (ICS), führte aber gleichwohl zu zum Teil mehrwöchigen Ausfällen der entsprechenden Produktionsanlagen. Eintrittsvektor war meistens, wie auch in Office-Umgebungen, eine Phishing-Mail oder ein Wechseldatenträger. Zudem gab es auch Fälle, in denen eine Ausbreitung über fehlerhaft konfigurierte Fernwartungssysteme stattgefunden hat. Die Schadsoftware nutzt bekannte Schwachstellen in veralteter Software und unzureichende Segmentierung zwischen Office-IT und Produktionsnetzen bzw. innerhalb der Produktionsnetze, um sich auszubreiten. Diese Art der Vorkommnisse wird auch in den kommenden Jahren eine erhebliche Gefahr für ICS darstellen. Der Grund dafür sind die zum Teil sehr alten Systeme, für die es keine Updates mehr gibt oder bei denen für vorhandene Updates keine Freigabe durch den Hersteller oder Integrator/Maschinen-/Anlagenbauer erteilt wurde. Maßnahmen zum Schutz auch von Bestandsanlagen werden in den IT-Grundschutz-Bausteinen für industrielle Systeme und dem ICS-Security-Kompendium gegeben. Konkret werden Hinweise gegeben, wie Systeme zu separieren und das Netzwerk zu segmentieren ist, um unberechtigte Zugriffe zu verhindern.

Zielgerichtete Angriffe auf ICS, um diese zu manipulieren, sind die Ausnahme. Ende 2017 wurde der erste dokumentierte Angriff auf ein Safety-System unter dem Namen TRITON bekannt. Dabei sollte eine Steuerung, die für die funktionale Sicherheit zuständig war und damit Schaden von Menschen und Umwelt abwenden soll, umprogrammiert werden. Dies schlug fehl und die Anlage wurde in einen sicheren Zustand heruntergefahren.

Triton – Cyber-Angriff auf das Safety-System einer Industrieanlage im Nahen Osten

Sachverhalt

Am 14. Dezember 2017 veröffentlichte die Firma FireEye einen Bericht (https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html; https://dragos.com/blog/trisis/TRISIS-01.pdf), der den Angriff auf ein Safety Instrumented System (SIS) einer Industrieanlage beschrieb. Am gleichen Tag bestätigte Dragos den Vorfall durch einen Bericht (https://dragos.com/blog/trisis/TRISIS-01.pdf), der als Standort der angegriffenen Anlage den Nahen Osten nannte. SIS haben den Schutz von Mensch, Anlage und Umwelt zum Ziel und unterliegen daher besonderen Anforderungen an funktionale Sicherheit. In industriellen Automatisierungssystemen, die auch in Kritischen Infrastrukturen und der Prozessindustrie zum Einsatz kommen, werden SIS im Regelfall getrennt vom Leitsystem aufgebaut, d. h. sie haben eine rein beobachtende Funktion und greifen nur im Anforderungsfall ein. Für die verwendete Schadsoftware gibt es derzeit drei Namen: FireEye verwendet den Namen Triton, die Firma Dragos nennt ihn Trisis und das NCCIC (vormals ICS-CERT) HatMan.

Ursache/Schadenswirkung

Die Angreifer verschafften sich zunächst Zugang zu den IT-Servern des Opfers. Anschließend bewegten sie sich hauptsächlich mit eigenentwickelten Tools durch die Demilitarisierte Zone (DMZ) der Betriebstechnik (engl. Operational Technology, OT) und die Rechner der OT zum SIS-Netzwerk. Dort wurde die Engineering Workstation infiziert, also der Computer, der für die Programmierung der Safety Controller verwendet wird. Die im Verlauf der Analyse ermittelten forensischen Artefakte legen nahe, dass der Angriff lange vorbereitet wurde und die Angreifer im Besitz eines baugleichen Safety Controllers waren oder Zugriff darauf hatten. Von dem infizierten Rechner aus wurden dann die einzelnen Safety Controller infiziert. Der Angriff lief zweistufig ab: Zunächst wurde an das reguläre Applikationsprogramm zusätzlicher Code angehängt, der sich die erforderlichen erweiterten Rechte verschaffte. Dadurch konnte im zweiten Schritt die Firmware des Safety Controllers verändert und ein nicht persistenter Remote-Access-Trojaner (RAT) installiert werden. Begünstigt wurde der Angriffsablauf, weil der Schlüsselschalter, der vor einer Veränderung der Speicherinhalte des Safety Controllers schützen sollte, sich im Status „Programmieren“ befand. Dadurch wurde der erste Schritt nicht unterbunden. Bei mindestens einem Safety Controller schlug jedoch im Verlauf des Angriffs eine Gültigkeitsprüfung des Applikationsprogramms zwischen den unabhängigen, redundant arbeitenden Prozessoren fehl. Daraufhin wurde ein Fehlerzustand erkannt und die Anlage durch das Safety-System in den sicheren Zustand überführt; das heißt trotz Manipulation des Steuerprogramms waren die Geräte im Stande, ihre Funktion zu erfüllen.

Reaktion
Der betroffene Anlagenbetreiber leitete daraufhin eine Untersuchung ein, in die sowohl der Hersteller der Safety Controller, Schneider Electric, als auch zahlreiche Analysefirmen sowie das NCCIC eingebunden wurden. Der Untersuchung folgte eine koordinierte Veröffentlichung der bis dahin gewonnenen Erkenntnisse am 14. Dezember 2017. Daraufhin hat das BSI eine Cyber-Sicherheitswarnung an die Betreiber Kritischer Infrastrukturen versandt, in welcher der Sachverhalt dargestellt und bewertet sowie Maßnahmen empfohlen wurden. Eine breite Diskussion des Vorfalls unter Fachexperten fand unter anderem auf der S4x18 in Miami statt, an der auch ein Vertreter des BSI teilgenommen hat.

Empfehlung
Angriffe auf Safety-Systeme stellen, aufgrund der möglichen Auswirkungen für Mensch und Umwelt, eine ernstzunehmende Bedrohung dar. Wenngleich Triton für bestimmte Firmware-Versionen des Models Triconex 3008 von Schneider Electric maßgeschneidert wurde, so hat doch die Veröffentlichung des Frameworks dazu geführt, dass die Schwelle für derartige Angriffe gesenkt wurde. Es ist davon auszugehen, dass in naher Zukunft auch Angriffe auf SIS anderer Hersteller stattfinden werden.

Das BSI empfiehlt daher, das SIS-Netzwerk vollständig getrennt vom Netzwerk der OT und dem Internet zu betreiben. Die Betreiber sollten überprüfen, ob die bereits im Safety-System integrierten Schutzmöglichkeiten des Applikationsprogramms und dessen Parameter in angemessenem Umfang eingeschaltet sind. Insbesondere sollte ein eventuell am Gerät vorhandener physikalischer Schutz gegen Veränderung des Controllers aktiviert sein. Dieser darf nur während der Programmierung oder Konfiguration des Controllers ausgeschaltet werden, welche zusätzlich automatisch in der Leitwarte signalisiert werden sollte.

Als praktische Empfehlungen hat das BSI den Grundschutzbaustein „Safety Instrumented Systems“ veröffentlicht sowie weitere Bausteine zum sicheren Betrieb industrieller Anlagen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html veröffentlicht. Zudem wird empfohlen, das OT-Netzwerk vom IT-Netzwerk bestmöglich zu trennen und eine Defense-in-Depth-Strategie zu betreiben. Dazu zählt neben einer Überwachung des IT-Netzwerks auch die Etablierung von IT-Sicherheit im OT-Netzwerk. Darüber hinaus stellt das BSI zur Überwachung der Kommunikation im SIS-Netzwerk Snort-Regeln für das TriStation-Protokoll bereit. https://www.bsi.bund.de/RAPSN_SETS.

Des Weiteren hat die Interessengemeinschaft Automatisierungstechnik der Prozessindustrie (NAMUR) mit dem kostenpflichtigen Arbeitsblatt 163 https://www.namur.net/de/arbeitsfelder-u-projektgruppen/af-4-betrieb-und-instandhaltung/ak-418-automation-security.html eine Methode zur IT-Risikobeurteilung von PLT-Sicherheitseinrichtungen erstellt. Eine Checkliste zur konkreten Beurteilung ist frei verfügbar www.namur.net/fileadmin/media_www/Dokumente/AK-PRAXIS_4.18_NA163_Checkliste_DE_2017_12_15.xlsx.

Aufgrund der im Rahmen der Digitalisierung weiter zunehmenden Vernetzung steigt die Exposition vorhandener Systeme. Viele Systeme werden mit veralteter Software betrieben. Angreifer können auf bestehende Angriffswerkzeuge zurückgreifen, was den Aufwand erheblich reduziert. Es ist davon auszugehen, dass zunächst Angriffe ohne spezifisches Know-how über den Produktionsvorgang zunehmen werden. Mit steigendem Wissen auf Angreiferseite werden auch gezielte Manipulationen an Maschinen oder Anlagen zunehmen, die Einfluss auf den Prozess oder die Produkte haben.

Mit fortschreitender Einführung von Industrie 4.0 bieten sich für Angreifer zudem neue Ansatzpunkte für kriminelle Aktivitäten. In Verbindung mit der gleichfalls steigenden Exposition stellt die Absicherung und der vertrauenswürdige Betrieb von ICS eine bedeutende Herausforderung dar und nimmt eine Schlüsselrolle für den weiteren Erfolg der digitalen Transformation ein.

1.4.3 Botnetze

Durch die Nutzung von Botnetzen können Cyber-Kriminelle in großem Umfang auf fremde Computersysteme zugreifen, um persönliche Daten zu stehlen oder deren Ressourcen wie beispielsweise Rechenleistung oder Netzwerkbandbreite für kriminelle Zwecke zu missbrauchen. Hierzu ist es nicht erforderlich, eigene Botnetze aufzubauen. Vielmehr können auch technische Laien aufgrund

der Professionalisierung im Cybercrime-Umfeld auf fertige Lösungen zurückgreifen und Botnetz-Kapazitäten vergleichsweise einfach und günstig anmieten.

Die verwendete Schadsoftware auf Clientseite ist typischerweise modular aufgebaut und verfügt über die Möglichkeit, flexibel einzelne Funktionalitäten von dem steuernden Command-and-Control-Server (C&C-Server) nachzuladen. Somit kann ein Botnetz dynamisch seinen Einsatzzweck ändern oder erweitern.

Im Berichtszeitraum wurden Botnetze hauptsächlich zum Informationsdiebstahl, für Distributed-Denial-of-Service-Angriffe (DDoS-Angriffe) auf Computersysteme sowie zum Spamversand und zur Verteilung von Schadprogrammen genutzt. Auffällig ist 2017/2018 das gesteigerte Aufkommen von IoT-Botnetzen (Internet-of-Things-Botnetzen), die internetfähige Heimelektronik kompromittieren und als Bots missbrauchen.

Im Zeitraum dieses Berichts wurden von Sicherheitsforschern täglich bis zu 10.000 Botinfektionen deutscher Systeme registriert und über das BSI an die deutschen Internet-Provider gemeldet. Die Provider informieren dann ihre Kunden über die Infektion und bieten zum Teil auch Hilfestellung bei der Bereinigung der Systeme an. Die Detektion erfolgt hierbei über sogenannte Sinkhole-Systeme, die anstelle der regulären Command-and-Control-Server die Kontaktanfragen von Bots entgegennehmen. Die Höhe der sichtbaren Infektionen wird durch verschiedene Faktoren, wie Auswahl der beobachteten Botnetze und der zugehörigen Steuerungsdomänen, beeinflusst und schwankt deshalb sehr stark. Aufgrund der Erfahrungen aus erfolgreichen Botnetz-Abschaltungen ist davon auszugehen, dass die Dunkelziffer deutlich höher liegt und sich die Gesamtzahl der infizierten deutschen Systeme mindestens in einem sechsstelligen Bereich bewegt.

Schwerpunkt IoT-Botnetze

Vernetzte Geräte und Assistenten im Internet der Dinge verfügen über eine große Angriffsfläche, die von Cyber-Kriminellen bereits seit Jahren aktiv ausgenutzt wird (siehe Kap 1.4). Neben Angriffen auf die Verfügbarkeit der Geräte ist durch maßgeschneiderte Schadprogramme auch eine komplette Steuerung der kompromittierten Systeme möglich. Die übernommenen Geräte werden hierzu zu einem Botnetz zusammengeführt, das von zentraler Stelle seine Befehle entgegennimmt. Aufgrund der Modularität aktueller Schadprogramme können benötigte Funktionalitäten der Bots, wie beispielsweise Komponenten zum Informationsdiebstahl oder Spamversand, flexibel nachgeladen werden. Typischerweise verfügen IoT-Bots in der Regel über Wurmfunktionalität und sind somit in der Lage, weitere potenziell verwundbare Systeme zu finden und zu infizieren.

Als eines der ersten IoT-spezifischen Schadprogramme wurde im Januar 2012 die als „Linux.Aidra“ bezeichnete Malware entdeckt. Diese verbreitete sich aktiv über unzureichend abgesicherte Telnet-Logins und erhielt in einer späteren Version die Funktionalität Bitcoins zu generieren. Sicherheitsforscher fanden bereits damals eine große Anzahl infizierter Endgeräte verschiedener Geräteklassen wie beispielsweise Heimrouter, Fernsehgeräte, TV-Receiver, DVR, VoIP-Geräte, IP-Kameras und Media Center. In den folgenden Jahren gab es zahlreiche weitere größere IoT-Botnetze, die vorrangig genutzt wurden, um Kryptowährungen zu generieren und DDoS-Attacken auszuführen, aber im Wesentlichen nur bei Sicherheitsforschern Beachtung fanden.

Große mediale Aufmerksamkeit erreichte im August 2016 das *Mirai*-Botnetz durch massive DDoS-Angriffe von bisher unbekannter Bandbreite. So wurde das IT-Sicherheitsblog https://krebsonsecurity.com des Sicherheitsforschers Brian Krebs von einer massiven DDoS-Attacke mit etwa 620 Gigabit pro Sekunde getroffen. Die Veröffentlichung des *Mirai*-Quellcodes im Herbst 2016 hat seitdem zur Entstehung zahlreicher *Mirai*-Varianten geführt, die zusätzliche Funktionalitäten beinhalten. Im Berichtszeitraum sind vor allem die *Mirai*-Nachfolger IoT-Reaper, Satori sowie Okiru aufgefallen. Diese Varianten nutzen fortgeschrittene Methoden zur Verbreitung, indem sie neben dem einfachen Ausprobieren von Passwörtern für den Telnet-Dienst, spezifische Exploits verwenden, um potenzielle Schwachstellen der Zielsysteme auszunutzen. Im Fall von Okiru wurde mit ARC-Prozessoren zudem eine weitere Zielplattform angegriffen, die bisher noch nicht im Fokus von IoT-Malware lag.

Abseits von *Mirai* wurden aber auch neue IoT-Botnetze bekannt wie beispielsweise HNS (Hide‘n‘Seek), die neue Alleinstellungsmerkmale mit sich bringen. So verfügt der HNS-Bot über die Möglichkeit, sich auf einem Teil der befallenen Systeme dauerhaft zu verankern und somit auch Neustarts der Geräte zu überstehen.

Die vorgenannten Beispiele zeigen, dass die Entwicklung im Bereich der IoT-Schadprogramme kontinuierlich weitergeht und bereits vorhandene Funktionalitäten zur Kompromittierung und Ausnutzung verwundbarer Systeme fortlaufend ausgebaut und verfeinert werden. Da die Zahl der an das Internet angebundenen IoT-Geräte unaufhörlich steigt, verbreitert sich somit auch die Angriffsfläche zunehmend. Auch wenn bei den vorgenannten Botnetzen von hohen Infektionsraten im

Missbrauch von memcached-Instanzen für DRDoS-Angriffe

Sachverhalt

Memcached ist ein Open-Source-Cache-Server zum einfachen Hinterlegen und Abholen von Daten aus dem Arbeitsspeicher. Er wird häufig in Verbindung mit Web-Applikationen eingesetzt. Seit Anfang 2018 werden in großem Maße offen aus dem Internet erreichbare memcached-Instanzen für DRDoS-Angriffe missbraucht. Dabei wird memcached über UDP statt TCP angesprochen. Eine Erreichbarkeit über UDP war bis einschließlich Version 1.5.5 in der Standardkonfiguration enthalten.

Ursache/Schadenswirkung

Bei gängigen Protokollen, welche für DRDoS-Angriffe missbraucht werden (etwa DNS oder SSDP), kann der Verstärkungsfaktor Werte von etwas über 50 erreichen. Bei memcached kann der Faktor 51.000 betragen. Ein Angreifer kann also mit wenigen kleinen Anfragen eine enorme Bandbreite für seinen Angriff erzeugen. So wurde unter Nutzung von memcached mit 1,7 TBit/s ein neuer Rekord für DDoS-Bandbreiten aufgestellt.

Es ist deshalb nicht verwunderlich, dass sich memcached seit dem Bekanntwerden dieser Möglichkeit einer sehr hohen Beliebtheit bei Angreifern erfreut. Die Tatsache, dass UDP-basierte Protokolle für DRDoS-Angriffe missbraucht werden, ist allerdings nicht neu.

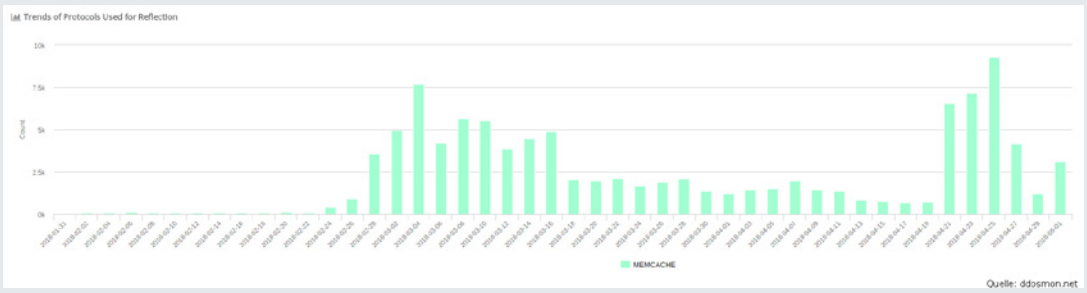


Abbildung 07 Protokolltrends bei Reflection

Reaktion

Das BSI informiert deutsche Netzbetreiber bereits seit Anfang 2015 über offen erreichbare memcached-Instanzen in ihren Netzen. Bisher lag der Fokus der Informationen durch das BSI auf der Erreichbarkeit der Instanzen über TCP.

Das BSI hat Ende Februar 2018 seine Benachrichtigungen um UDP offen erreichbare memcached-Instanzen erweitert. Alle großen deutschen Hosting-Anbieter haben zügig reagiert, so dass die Anzahl der für Angriffe in Deutschland ausnutzbaren memcached-Instanzen von anfänglich über 2700 auf unter 130 (Stand 31. Mai 2018) geschrumpft ist. Entwarnung kann dennoch nicht gegeben werden, da weltweit noch zahlreiche Instanzen verfügbar sind und weiterhin für Angriffe genutzt werden.

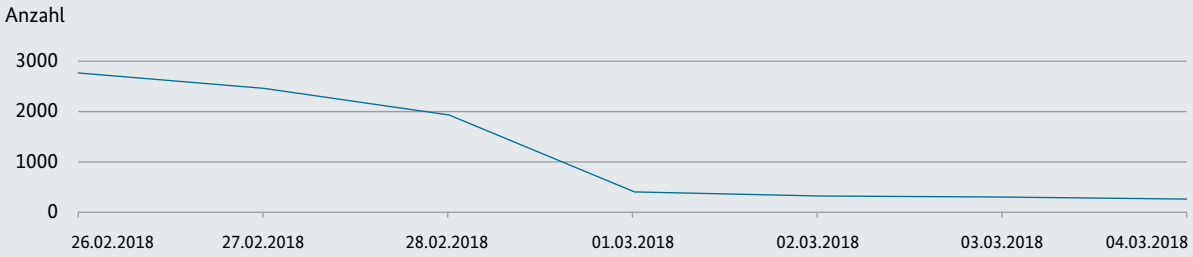


Abbildung 08 Zügiger Rückgang offener memcached Instanzen in der ersten Woche der Benachrichtigungen

Empfehlung

Für die Funktion von memcached ist eine Erreichbarkeit über UDP nicht zwingend erforderlich. Dies sollte bei eigenen Systemen geprüft und ggf. abgeschaltet werden https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/CERT-Bund/CERT-Reports/HOWTOs/Offene-Memcached-Server/Offene-Memcached-Server_node.html. Grundsätzlich sollten memcached-Instanzen nicht aus dem Internet erreichbar sein.

teilweise sechsstelligen Bereich berichtet wird, ist die unmittelbare Betroffenheit in Deutschland gering. Dies ist der Tatsache geschuldet, dass die Internetzugänge von Endkunden in der Regel über Heimrouter realisiert sind, die das interne Netz vor dem Internet abschotten und dass eventuell vorhandene IoT-Geräte im Heimnetz ohne aktives Zutun des Endanwenders nicht direkt aus dem Internet ansprechbar sind. Ungeachtet dessen schützt dies jedoch nicht vor den Bedrohungen, die von den IoT-Botnetzen mittelbar ausgehen wie beispielsweise DDoS-Angriffe oder Spamversand.

Schwerpunkt Android

Die gemeldeten Infektionen verteilten sich im Berichtszeitraum auf über 130 verschiedene Botnetzfamilien. Auffällig ist hierbei, dass im Vergleich zum Vorjahreszeitraum zunehmend mehr Botnetze Android-Systeme befallen (ca. 25 Prozent), während die übrigen Botinfektionen überwiegend auf Microsoft-Windows-Systemen zu verzeichnen sind. Die folgende Grafik zeigt eine Verteilung der Versionsstände infizierter Android-Geräte anhand einer Stichprobe Ende Mai 2018. Als Datenbasis dienen die Botnetzfamilien, die das verwendete Betriebssystem des Opfersystems an einen Sinkhole-Server übertragen.

Eine nähere Betrachtung der Botnetz-Familien zeigt, dass alle über die Funktionalität verfügen, Informationen wie beispielsweise International Mobile Equipment Identity (IMEI), International Mobile Subscriber Identity (IMSI) oder Standort abfließen zu lassen und auch weitere Schadprogramme nachzuladen. Ein Teil der Familien greift Daten zum Onlinebanking ab oder ist in der Lage, hochpreisige Premium-SMS zu verschicken.

Der größte Teil der Android-Infektionen lässt sich dabei auf maliziöse Apps zurückführen, die aus Drittanbieterquellen bezogen wurden. Neben der aktiven Installation zweifelhafter Apps sind aber auch Infektionen ohne Zutun des Anwenders möglich. So liefern viele Hersteller von Android-Systemen die Geräte bereits ab Werk mit einer veralteten Softwareinstallation aus und stellen keine oder nur zeitlich begrenzt Sicherheitsupdates zur Verfügung. Somit bieten diese Geräte mit zunehmendem Alter durch die steigende Anzahl vorhandener Schwachstellen eine größere Angriffsfläche (siehe Abb. 09) So läuft der größte Anteil der infizierten Systeme (> 40 Prozent) noch mit einer Version von Android 4, die bereits seit geraumer Zeit nicht mehr von Google unterstützt wird. Aktuelle Varianten wie Android 7 sind mit nur 3,7 Prozent vertreten. Infizierte Android 8-Systeme stellen den geringsten Anteil mit ca. 0,2 Prozent.

Wie auch in den Vorjahren finden sich bei den infizierten Betriebssystemen auch linuxbasierte Webserver sowie vereinzelt auch kompromittierte Systeme auf Basis von Mac OS X.

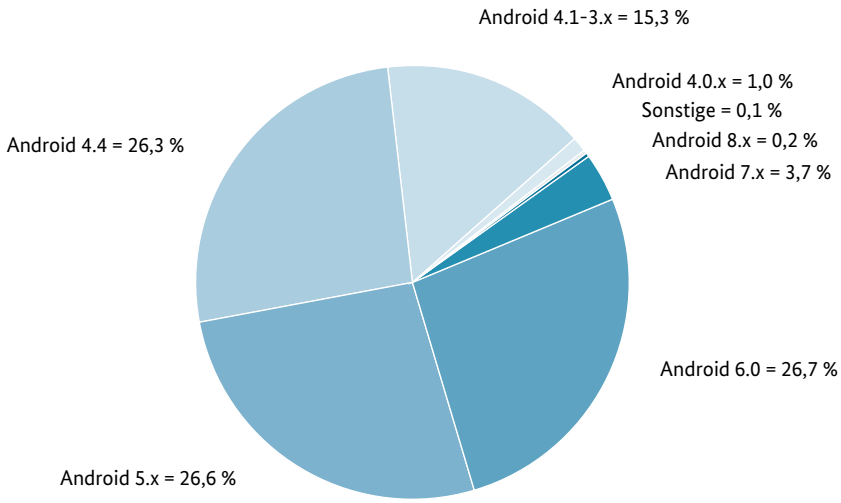


Abbildung 09 Versionsstände infizierter Android-Systeme, Quelle: BSI, 22.05.2018

Bedrohungslage bleibt weiterhin hoch

Wie die aktuellen Entwicklungen zeigen, ist die Bedrohungslage durch Botnetze anhaltend hoch. Standen bis vor einigen Jahren primär klassische Computersysteme (oftmals auf Windows-Basis) im Fokus der Angreifer, so zeigt sich nun eine Umorientierung in Richtung mobile Endgeräte sowie Geräte aus dem Internet der Dinge. Die Angreifer passen sich somit den aktuellen Marktentwicklungen an und erweitern das Spektrum um mehrere Millionen potenzielle Opfersysteme.

Bereits 2016 hat das IoT-Botnetz *Mirai* die Bedrohung, die in diesem Zusammenhang von dem Internet der Dinge ausgeht, eindrucksvoll veranschaulicht. Das berichtete hohe Aufkommen weiterer IoT-Botnetze mit Botnetz-Kapazitäten im sechsstelligen Bereich lässt die Eintrittswahrscheinlichkeit und die potentielle Auswirkung von DDoS-Angriffen weiterhin steigen.

Avalanche: Ausweitung der Schutzmaßnahmen

Ein Jahr nach der Zerschlagung der weltweit größten Botnetzinfrastruktur Avalanche, die am 30.11.2016 initiiert wurde, hat das BSI die Schutz- und Informationsmaßnahmen ausgeweitet und verlängert. Analysen hatten gezeigt, dass trotz Benachrichtigung durch die Internet-Provider noch immer eine große Anzahl infizierter Systeme vorhanden ist: In Deutschland haben sich die festgestellten Infektionszahlen nach einem Jahr um 61 Prozent reduziert, was verglichen mit der weltweiten Entwicklung – einer Reduzierung um 45 Prozent – ein großer Erfolg ist. Andererseits bedeutet das aber auch, dass immer noch viele betroffene Anwender ihre Systeme nicht bereinigt haben.

Zusätzlich zur Verlängerung der Maßnahmen wurde das im Zuge der Avalanche-Abschaltung aufgesetzte Sinkholing-System um Domänen des Andromeda-Botnetzes erweitert. Analysen hatten ergeben, dass insbesondere bei der Schadsoftware Andromeda weltweit eine sehr hohe Zahl von Systemen infiziert war. Als Hauptangriffsziele der als Andromeda bzw. auch Gamarue bezeichneten Schadsoftware wurden Asien, Nordamerika und in Europa im Schwerpunkt die Länder Rumänien, Italien, Deutschland und Polen identifiziert. Dieses weltweit agierende Botnetz wurde am 30. November 2017 in internationaler Kooperation durch Ermittler zerschlagen. Dabei koordinierte die europäische Justizbehörde Eurojust die Maßnahmen der weltweit beteiligten Staatsanwaltschaften. Federführend in Deutschland war die Zentrale Kriminalinspektion Lüneburg unter Sachleitung der Staatsanwaltschaft Verden.

Durch die Verlängerung und Ausweitung der Schutzmaßnahmen verbinden sich Systeme mit aktiven Infektionen weiterhin zu den Sinkhole-Servern und erhalten keine Steuerbefehle mehr. Informationen zu den an der Sinkhole verzeichneten Infektionen bei deutschen IP-Adressen werden den jeweils zuständigen Internet-Providern zur Verfügung gestellt, die auf dieser Basis ihre Kunden informieren. Informationen zu betroffenen ausländischen IP-Adressen werden über CERT-Bund an die jeweils zuständigen nationalen CERTs in über 80 Ländern weltweit weitergeleitet, damit auch dort betroffene Nutzer informiert werden können.

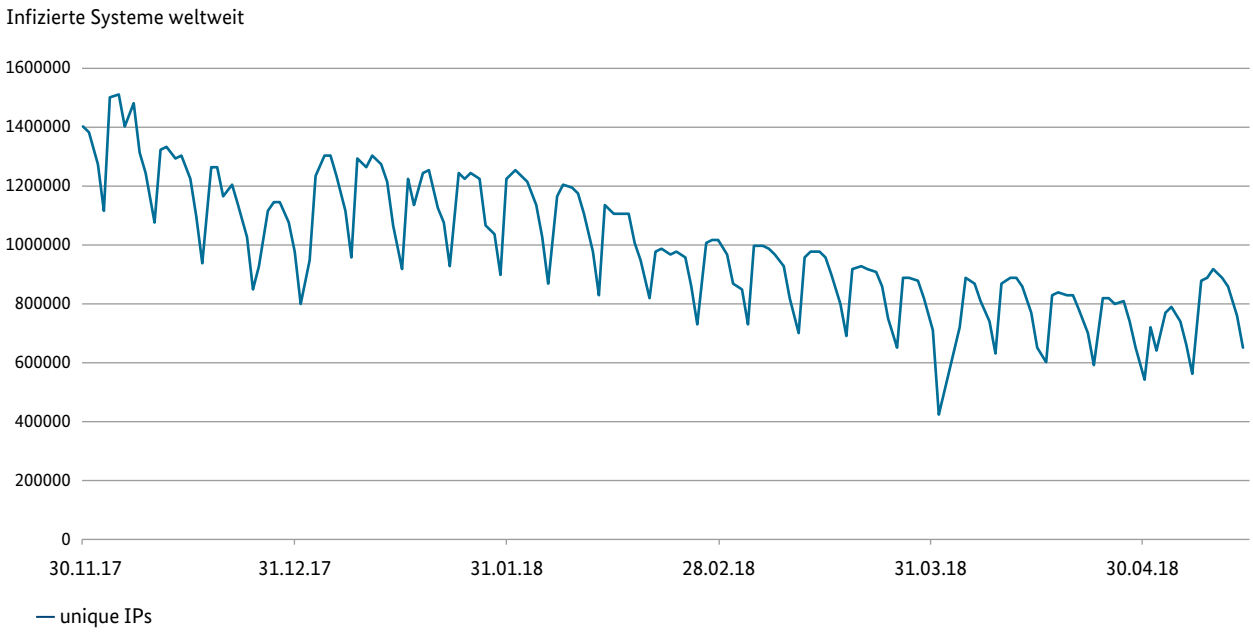


Abbildung 10.1 Infizierte Systeme

Infizierte Systeme Deutschland

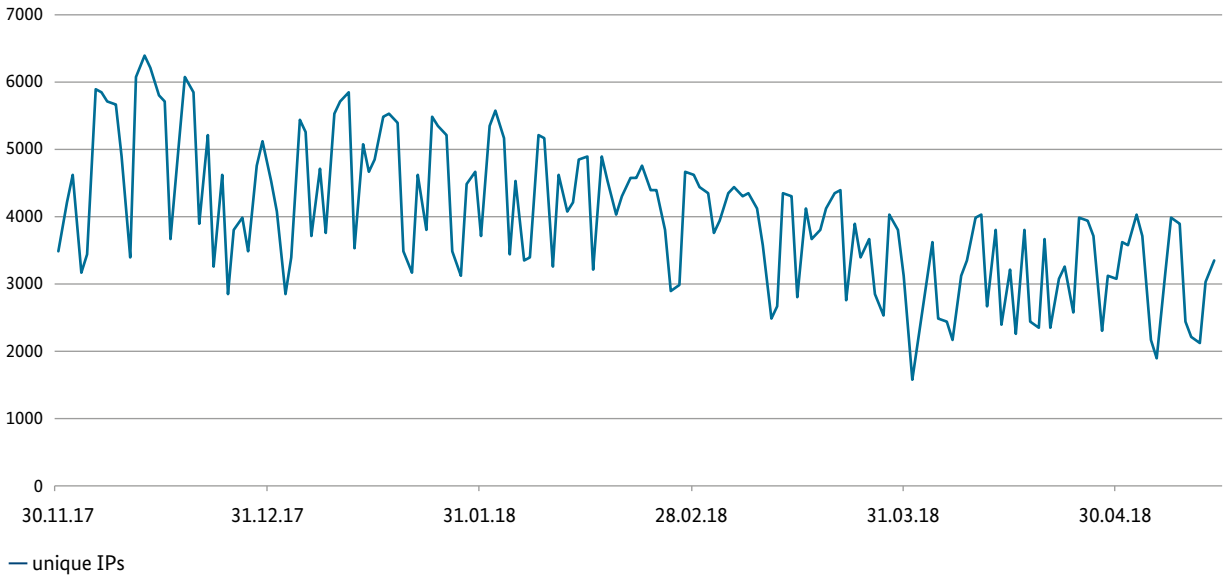


Abbildung 10.2 Infizierte Systeme

DoS-Angriff auf VPN-Router eines KRITIS-Betreibers

Sachverhalt
Ein Betreiber aus dem KRITIS-Sektor Wasser berichtete dem BSI von einem Problem mit den eingesetzten VPN-Routern. Die Geräte seien für einen Denial-of-Service-(DoS)-Angriff anfällig. Eine bestehende IPsec-Verbindung könne von einem Angreifer jederzeit unterbrochen werden. Beim Betreiber sei es zu einer Fehlermeldung in der Leitstelle gekommen, da Messwerte gefehlt hätten und nicht weiter ferngewirkt werden konnte.

Ursache/Schadenswirkung
Die IP-Adressen des VPN-Routers wurden von einer Universität in den USA gescannt und daraufhin erfolgreich angegriffen. Für eine kurze Zeitspanne standen keine Messwerte der Pumpen in der Leitstelle des KRITIS-Betreibers zur Verfügung. Nach Aussage des Betreibers kam es zu keiner Beeinträchtigung kritischer Versorgungsdienstleistungen. Das Problem könne jedoch jederzeit erneut auftreten.

Reaktion
Der Betreiber hatte den Hersteller des Routers kontaktiert. Der Hersteller räumte die Existenz der Schwachstelle ein, allerdings traf er keine Aussage darüber, ob oder wann mit einer Behebung der Schwachstelle zu rechnen sei.

Nachdem das BSI beim Hersteller des Routers um Unterstützung gebeten hatte, wurde ein Firmware-Update erstellt. Über dessen Veröffentlichung informierte das BSI mit einer BSI-Management-Info die Öffentlichkeit.

Empfehlung
Der Zugriff auf Geräte, die aus dem Internet erreichbar sein müssen, sollte nur von bestimmten IP-Adressen aus möglich sein (Whitelist). Weiterhin bietet das BSI grundsätzlich an, bei Kontakten mit Herstellern zu unterstützen.

Am 5. Dezember 2017 konnten weltweit an einem einzigen Tag fast 1,5 Millionen Infektionen erkannt und gemeldet werden. Nach sechs Monaten zeigt sich in Deutschland bei den Tagesmeldungen ein Rückgang um 35 Prozent. Weltweit ist bisher ein Rückgang um 42 Prozent festzustellen.

Bei der Verlängerung der Schutzmaßnahmen um ein weiteres Jahr bis zum 30. November 2017 wurden ca. 848.000 Botnetz-Domänen berücksichtigt, damit die infizierten Systeme nicht von Kriminellen gesteuert werden können. Nach dem Auslaufen der Schutzmaßnahmen zum 1. Dezember 2018 wird keine vollständige Abdeckung aller Botnetzdomänen mehr möglich sein, da ohne richterliche Beschlüsse nur frei verfügbare Domänennamen für Sinkholingmaßnahmen verwendet werden können. Anwender mit infizierten Systemen, die sich mit den Sinkholes verbinden, sollen jedoch auch danach weiterhin gewarnt werden. Auf bereits vergebene und registrierte Domänennamen besteht dann hingegen kein Zugriff mehr. Es besteht somit die Gefahr, dass Kriminelle die Kontrolle über infizierte Rechner zurückgewinnen.

1.4.4 DDoS-Angriffe

Auch 2018 gibt es zahlreiche Medienberichte über Distributed-Denial-of-Service-Angriffe mit Rekordbandbreiten. Im Februar 2018 entdeckten Angreifer, dass sich unter Ausnutzung von memcached sehr hohe Verstärkungsfaktoren erreichen lassen (siehe Vorfall *memcached*). Arbor Networks hat von einem Angriff mit einer Bandbreite von 1,7 Tbit/s (1700 Gbit/s) berichtet. Angriffe dieser Größenordnung sind eine ernst zu nehmende Bedrohung. Bisher sind diese Angriffe allerdings Ausnahmeerscheinungen. In den ersten vier Monaten 2018 lagen lediglich 0,16 Prozent der dem BSI bekannten Angriffe in Deutschland oberhalb von 100 Gbit/s. Der Großteil der DDoS-Angriffe hat nach wie vor eine Bandbreite von weniger als 1 Gbit/s. Während die maximalen Ausschläge für Bandbreite, Paketrate und Dauer stark variieren, sind die durchschnittlichen Werte weitgehend konstant. Es ist jedoch eine Zunahme der Anzahl der Angriffe zu verzeichnen. Mit geeigneten Maßnahmen kann man sich vor den Auswirkungen der meisten DDoS-Angriffe schützen. Informationen hierzu hat das BSI auf einer Themenseite zusammengestellt: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/Themen/DDoS/ddos.html.

Die Bandbreite allein ist jedoch kein geeigneter Indikator für die Schwere eines Angriffs. Bei vorgeschalteten Komponenten wie Load-Balancern oder Firewalls, ist der limitierende Faktor häufig die Anzahl der Pakete, die verarbeitet werden können. Angriffe auf Anwendungsebene, zum Beispiel TCP-Verbindungen oder HTTPS-Anfragen, können sogar mit geringen Bandbreiten und geringen Paketraten einen erheblichen Schaden verursachen.

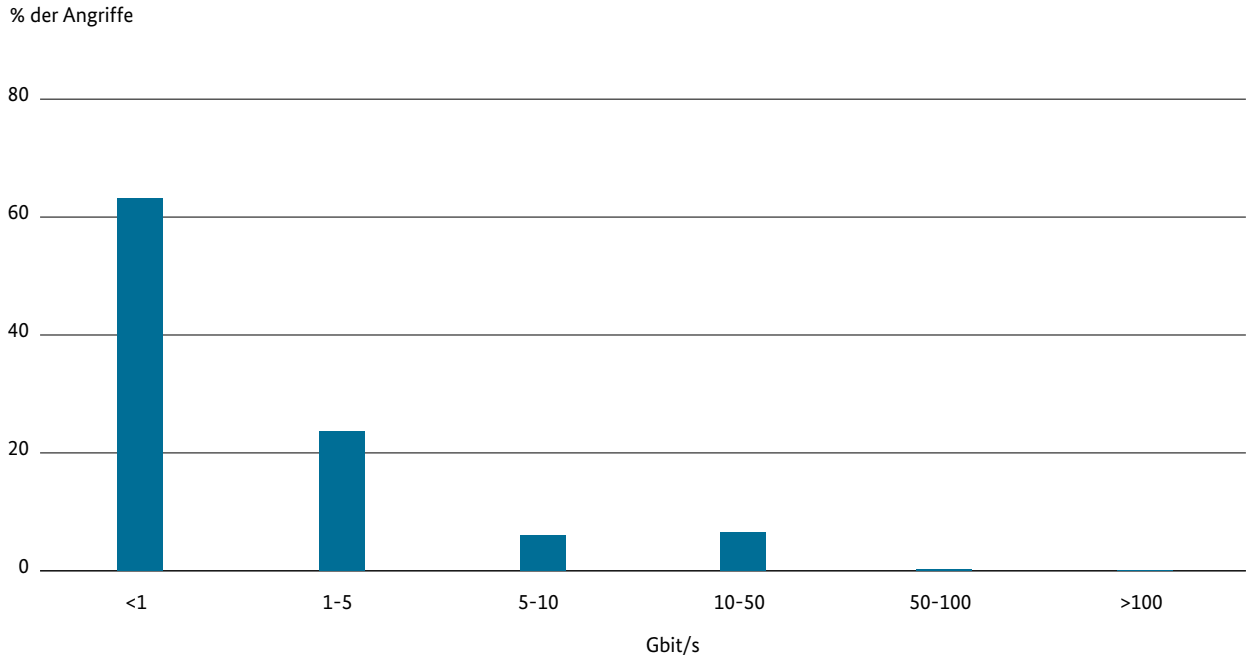


Abbildung 11 Verteilung der Angriffe nach Bandbreite (Januar bis April 2018)

1.4.5 Kryptografie

Kryptografische Mechanismen sind die Grundbausteine für die Wirksamkeit vieler IT-Sicherheitsprodukte. State-of-the-Art-Kryptografie wie beispielsweise das symmetrische Verschlüsselungsverfahren AES oder der asymmetrische Diffie-Hellman-Schlüsselaustausch liefern grundsätzlich ausgezeichnete Sicherheitsgarantien. Das BSI empfiehlt in der Technischen Richtlinie TR-02102 eine Reihe von kryptografischen Algorithmen und Protokollen, die aufgrund von eingehenden mathematischen Analysen (Kryptoanalyse) allgemein als sicher angesehen werden. Bei diesen Analysen wird jedoch eine Reihe von Annahmen getroffen. Für den sicheren praktischen Einsatz muss daher überprüft werden, ob diese Annahmen erfüllt sind, und es müssen gegebenenfalls weitere Absicherungsmaßnahmen getroffen werden.

Verschiedene Aspekte können dazu führen, dass ein kryptografisches System in der Praxis versagt. Neben vielen anderen zählen dazu beispielsweise:

- Sicherheitslücken in der Hardware (z. B. *Spectre* und *Meltdown*),
- Fehler in Implementierungen,
- Fehler auf Protokollebene,
- Verwendung veralteter Standards (z. B. ROBOT, siehe Kasten),
- Schwächen in der Schlüsselerzeugung (z. B. ROCA, siehe Kasten),
- Unzureichende Zufallszahlengeneratoren.

Ein typisches Beispiel ist ein Gerät, das eine Datenverschlüsselung mit einem geheimen Schlüssel durchführt. Hierfür gibt es eine Reihe von gängigen Verfahren, für die gemeinhin angenommen wird, dass ein Angreifer mit Zugriff auf die verschlüsselten Daten weder den geheimen Schlüssel noch den Klartext berechnen kann. Hat der Angreifer jedoch Netzwerkzugriff auf das Gerät oder befindet er sich in räumlicher Nähe, kann er versuchen, durch Beobachtung des Geräteverhaltens im Hinblick auf Berechnungszeiten, Stromverbrauch oder elektromagnetische Abstrahlung Informationen über die geheimen Daten zu sammeln. Diese sogenannten Seitenkanalangriffe sind seit langer Zeit Teil der Sicherheitsbetrachtung bei IT-Systemen. Intensive Forschung zu diesem Thema hat sowohl eine Reihe von Gegenmaßnahmen als auch von neuen Angriffsvektoren hervorgebracht. Die neueste Entwicklung ist der Einsatz von Techniken des Maschinellen Lernens (ML), um Muster in Messdaten zu erkennen. Während der Einsatz von ML unter den Bezeichnungen Pattern Recognition, Data Mining oder Artificial Intelligence in anderen IT-Bereichen schon ein Standardwerkzeug geworden ist, müssen ML-Angriffe als Teil der Sicherheitsbetrachtung von IT-Systemen noch etabliert werden.

Eine weitere Voraussetzung für den Einsatz von Kryptografie, die in der Praxis große Bedeutung hat, ist es, gewisse Gütekriterien erfüllende Zufallszahlen zu erzeugen. Positiv erwähnenswert ist hier die große Anzahl an Produkten, die über eine nach deutschem CC-Schema zertifizierte physikalische Rauschquelle verfügen. Aufgrund der Strukturverkleinerung von Halbleiterprodukten bzw. der immer größeren Leistungsfähigkeit bei geringem Stromverbrauch verfügen neuere Produkte über eine integrierte kryptografische Nachbearbeitung der Zufallszahlen, die die theoretische Ausnutzbarkeit der bereits sehr kleinen verbleibenden statistischen Schwächen physikalischer Rauschquellen vollends verhindert.

Post-Quanten-Kryptografie

Die Sicherheitsgarantien der heute eingesetzten kryptografischen Mechanismen gelten allerdings höchstens solange, bis ein „hinreichend großer“ (gemessen in der Anzahl der verschränkten logischen Qubits) Quantencomputer zur Verfügung steht. Schon seit den 1990ern sind Quantenalgorithmen bekannt, die das Sicherheitsniveau der klassischen Verfahren ungefähr halbieren (Grover-Algorithmus für symmetrische Kryptoverfahren) bzw. diese Verfahren vollständig brechen (Shor-Algorithmus für asymmetrische Kryptoverfahren). Ein weiterer Quantenalgorithmus von Brassard, Hoyer und Tapp findet eine Kollision einer n-Bit Hashfunktion nach ungefähr 2^(n/3) Schritten.

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 zu lösen sind. Einen Beweis für die Quantencomputerresistenz dieser Verfahren gibt es allerdings nicht. 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 Abschnitt 2.4). Eine wichtige Aufgabe des BSI wird in den nächsten Jahren sein, diese Aktivitäten aktiv zu begleiten und eigene Projekte umzusetzen.

ROCA

Unter dem Titel „Return of Coppersmith's Attack" (ROCA) haben tschechische Forscher im November 2017 eine Schwachstelle bei der RSA-Schlüsselerzeugung in einer Kryptobibliothek des Smartcard-Herstellers Infineon veröffentlicht. Für die RSA-Verschlüsselung bzw. -Signatur werden zwei geheimgehaltene, große (z. B. 1024 Bit) Primzahlen benötigt, deren Produkt den öffentlich bekannten RSA-Modul bildet. Die betroffene Bibliothek von Infineon erzeugt Primzahlen, die eine sehr spezielle Struktur besitzen. Dies führt dazu, dass die so erzeugten Primzahlen mittels einer seit den 1990er bekannten Methode von Don Coppersmith aus dem öffentlichen Modul rekonstruiert werden können. Die spezielle Gestalt der Primzahlen überträgt sich zudem auf den Modul, so dass für einen öffentlichen RSA-Schlüssel schnell festgestellt werden kann, ob er auf diese Weise erzeugt wurde und somit angreifbar ist.

ROBOT

Das Akronym ROBOT steht für „Return Of Bleichenbacher's Oracle Threat". Der von Hanno Böck, Juraj Somorovsky und Craig Young im Dezember 2017 veröffentlichte Angriff beschreibt eine Schwachstelle in gängigen TLS-Implementierungen, die RSA-Verschlüsselung in Verbindung mit einem veralteten Padding-Verfahren (PKCS#1 v1.5) einsetzen. Der ursprünglich von Daniel Bleichenbacher beschriebene Angriff ist bereits 20 Jahre alt. Bleichenbacher hatte TLS-Fehlermeldungen als Orakel dafür verwendet, ob das Padding einer Nachricht korrekt war oder nicht. So konnte er mittels eines adaptiven Chosen-Ciphertext-Angriffs verschlüsselte Nachrichten sukzessive entschlüsseln. Daraufhin wurden im TLS-Standard Empfehlungen gemacht, wie Implementierungen gegen den Bleichenbacher-Angriff abgesichert werden können. Die Autoren von ROBOT haben gezeigt, dass eine Vielzahl von TLS-Implementierungen dennoch weiter verwundbar ist.

Entwicklungsstand Quantencomputer

Um eine fundierte Einschätzung zum aktuellen Entwicklungsstand bzw. der potenziellen zukünftigen Verfügbarkeit eines Quantencomputers zu erhalten, wurde vom BSI die Studie „Entwicklungsstand Quantencomputer" an Forscher der Universität des Saarlandes und der Florida Atlantic University in Auftrag gegeben. Konkret werden in dem Bericht aktuelle technologische Ansätze und quantenalgorithmische Innovationen intensiv beleuchtet und deren Implikationen im Kontext aktuell eingesetzter Public-Key-Verfahren erörtert. Die Studie und eine Zusammenfassung stehen zum Download auf der Webseiten des BSI unter http://www.bsi.bund.de/qcstudie zur Verfügung.

1.4.6 Ransomware

Der Begriff Ransomware umfasst Schadsoftware, die den Zugriff auf einen Rechner verwehren bzw. einschränken, oder vorgeben, Gleiches zu tun. Eine solche Software verspricht in einer Textnachricht, bei Zahlung eines Lösegelds (Ransom = Lösegeld) die Ressourcen wieder freizugeben.

Dabei unterscheidet man die folgenden Varianten:

- Ransomware, die den Zugang bzw. die Nutzung des Systems durch Manipulation des Betriebssystems sperrt und stattdessen den Text mit der Forderung anzeigt (ScreenLocker).
- Ransomware, die Nutzerdaten in Form von Dateien bestimmter Formate verschlüsselt und die Entschlüsselung nach Zahlung des Lösegelds in Aussicht stellt. Zu den verschlüsselten Dateien gehören eine Vielzahl von Formaten für Text, Audio-, Video- und Präsentations-Inhalte, aber auch für Tabellenkalkulation und Datenbanken, die in der Regel einen hohen Wert für den Nutzer darstellen. Die generelle Lauffähigkeit des Systems ist dabei normalerweise nicht betroffen.

Ransomware verbreitet sich inzwischen über verschiedene Angriffsvektoren:

- SPAM-Mails mit Schadsoftware, die sich im Anhang befindet oder über URLs referenziert wird.

- Drive-By-Exploits nutzen Schwachstellen in Browsern, Browser-Plugins oder Betriebssystemen, die durch den Aufruf einer infizierenden Web-Site bzw. darauf platzierter Werbung (u.U. ohne weitere Interaktion durch den Nutzer) ausgelöst wird.

- 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.

- Ausnutzung von Schwachstellen oder Erraten von schwachen Passwörtern in öffentlich zugänglichen Web-Servern. Für das Ausspähen weiterer Passwörter im internen Netz gibt es ebenfalls bekannte Software.

- 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 teilweise Schwachstellen im Betriebssystem, um als scheinbar legitimer Prozess nicht frühzeitig entdeckt zu werden.

Lösegeldzahlungen werden dabei häufig in digitalen (virtuellen) Währungen wie z. B. Bitcoin und Ethereum oder über anonyme Webseiten im Tor-Netzwerk abgewickelt, um die Strafverfolgung zu erschweren.

Gefährdungsentwicklung

Seit 2016 ist ein starker Anstieg der Gefährdung durch Ransomware festzustellen. In Erinnerung sind hauptsächlich die großen Ransomware-Kampagnen aus dem Jahr 2017 wie *WannaCry* und *NotPetya*/ExPetr. Bei der letztgenannten handelte es sich vermutlich eher um einen Sabotageakt als um echte Ransomware, da bei den Betroffenen keine Erpressungsmeldung einging und den Nutzern keine Möglichkeit gegeben wurde, die verschlüsselten Dateien zu entschlüsseln.

Die neueren Vorfälle aus dem Jahr 2018 haben die Öffentlichkeit nicht in dem gleichen Maß erreicht wie die früheren Angriffe, weisen aber auf verschiedene Entwicklungen hin:

- Am 26. Januar 2018 wurde erstmals eine neue Erpresser-Software namens GandCrab entdeckt, die neben lokal aktiven Kampagnen (Magniber) als erste eine breite Verbreitung per Exploit-Kit erfährt.

- Die Ransomware SamSam attackiert über Schwachstellen öffentlich zugänglicher Softwarekomponenten (Web-Server) oder durch das Erraten schwacher Passwörter in der verwendeten Benutzerverwaltung. Mit dieser Ransomware wurde am 22. März 2018 die Stadt Atlanta (Georgia) angegriffen, weite Bereiche der externen und internen Dienste wurden lahmgelegt.

- Die Ransomware XiaoBa beinhaltet zusätzlich Software, die Coin-Mining (bzw. Krypto-Mining) betreibt, d. h. ausführbare Programme so verändert, dass sie Infrastrukturaufgaben für Kryptowährungen übernimmt und damit (sicheres) Geld verdient.

- Im April 2018 wurde Ransomware beobachtet, die kein Lösegeld verlangt, sondern dazu animiert, Computerspiele zu spielen.

- Die Ransomware RanSIRIA gibt vor, das Lösegeld für die Unterstützung syrischer Flüchtlinge zu verwenden.

- Ebenfalls im April 2018 nutzte eine Ransomware Schwachstellen in HPE Integrated Lights-Out, um Bitcoin-Zahlungen zu erpressen.

- Seit Mai 2018 ist bekannt, dass die Ransomware SynAck eine Technik verwendet, die „Process Doppelgänging“ genannt wird. Es werden auch diverse weitere Techniken verwendet, die sowohl die Detektion als auch die Analyse erschweren (Protokolle löschen, Sprungadressen errechnen, Hash statt des Originalstrings verwenden).

Diese Vorfälle und weitere Informationen aus der IT-Sicherheitsbranche weisen auf folgende Entwicklungen hin:

- Ähnlich den Botnetz-Diensten, die für DDoS-Attacken zur Verfügung stehen, gibt es inzwischen Ransomware-as-a-Service-Angebote. Dabei muss der Nutzer der Dienste nicht mehr alle Details des Angriffsvektors selbst verstehen und kann nach dem Baukasten-Prinzip Variationen bestehender Ransomware erzeugen. Auch Auftragsarbeiten für spezielle Eigenschaften sind möglich. Dies erleichtert es einem größeren Kreis von Angreifern, individuelle Angriffsszenarien durchzuführen.

- Es zeichnet sich eine Zersplitterung der Ransomware-Familien ab. Dies macht einzelne Angriffe zwar nicht unbedingt für die Gesamtbevölkerung oder die gesamte Wirtschaft gefährlicher, trägt aber zu einer unübersichtlichen Gefährdungslandschaft bei, so dass weniger denn je punktuelle schwerwiegende Folgen ausgeschlossen werden können. Nicht nur die Angriffsverfahren werden immer aufwändiger, auch die Vorkehrungen zur Verschlei-

CEO Fraud: BSI warnt Unternehmen gezielt vor akutem Risiko

Sachverhalt
Als „CEO Fraud“ werden Social-Engineering-Angriffe bezeichnet, bei denen sich die Betrüger als Geschäftsführer (Chief Executive Officer) oder Vorstandsmitglied eines Unternehmens ausgeben. Bei den Angriffen, welche meist per E-Mail erfolgen, adressieren sie gezielt Mitarbeiter der Finanzabteilungen von Unternehmen und versuchen diese zu verleiten, hohe Geldbeträge vom Geschäftskonto des Unternehmens auf ein fremdes Konto zu überweisen. Dabei werden die Opfer häufig unter Zeitdruck gesetzt und zur Verschwiegenheit angewiesen, da es sich vorgeblich um ein geheimes oder vertrauliches Projekt des Unternehmens handele.

Ursache/Schadenswirkung
Die Kontaktdaten der Zielperson und des vorgetäuschten Absenders werden häufig durch öffentlich verfügbare Informationen auf der Webseite des Unternehmens, in Online-Karriereportalen, in Sozialen Netzwerken, in Handelsregistereinträgen oder auch durch direkte Anrufe im Unternehmen gewonnen. Die Angreifer nutzen diese Informationen, um den Inhalt der E-Mail sowie den Stil der Kommunikation im Unternehmen glaubwürdig nachzuahmen und den Empfänger dazu anzustiften, Geldbeträge zu überweisen. Laut Bundeskriminalamt (BKA) sind durch CEO-Fraud in den letzten Jahren Schäden in mehrstelliger Millionenhöhe entstanden.

Reaktion
Im Rahmen eines Ermittlungsverfahrens gegen die organisierte Kriminalität ist es Strafverfolgungsbehörden im Juli 2017 gelungen, in den Besitz einer Liste mit rund 5.000 potenziellen Zielpersonen für CEO-Fraud-Angriffe zu gelangen. Diese Liste wurde dem BSI zur Warnung der potenziell Betroffenen übermittelt. Das BSI veröffentlichte am 10.07.2017 eine Pressemitteilung zu diesem Sachverhalt https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2017/CEO_Fraud_10072017.html. Zusätzlich wurden die potenziell betroffenen Zielpersonen bzw. Unternehmen direkt informiert. Einige Unternehmen bestätigten, kurz zuvor Opfer von CEO-Fraud-Angriffen geworden zu sein. Eine vom BSI durchgeführte Stichprobe zeigte, dass zu vielen in der Liste enthaltenen Zielpersonen Profile in Karriereportalen oder Sozialen Netzwerken existierten, in denen der Name des Unternehmens und die Position als Mitarbeiter der Finanzabteilung benannt waren.

Empfehlungen
Die öffentliche Angabe von Kontaktdaten des Unternehmens sollte sich auf allgemeine Kontaktadressen beschränken. Unternehmen sollten ihre Mitarbeiter für diese und andere Risiken der Digitalisierung sensibilisieren und im sicheren Umgang mit Informationstechnik regelmäßig schulen. Bei ungewöhnlichen Zahlungsanweisungen sollten vor Veranlassung der Zahlung Kontrollmechanismen greifen. Die Zahlungsaufforderung sollte durch Rückruf oder schriftliche Rückfrage beim vermeintlichen Auftraggeber verifiziert, Absenderadresse und die Plausibilität des Inhalts der E-Mail sollten sorgfältig überprüft werden. Die Geschäftsleitung oder der Vorgesetzte sowie der IT-Sicherheitsbeauftragte sollten über derartige Angriffe informiert werden. Von (versuchten) CEO-Fraud-Angriffen betroffene Unternehmen sollten Strafanzeige stellen.

Weitere Informationen und Handlungsempfehlungen hat das Bundeskriminalamt (BKA) in einer Themenbroschüre zusammengestellt: https://www.bka.de/SharedDocs/Downloads/DE/IhreSicherheit/CEOFraud.html.

erung bzw. gegen die Entdeckung durch AV-Software werden immer ausgefeilter. So werden maliziöse Prozesse als Betriebssystem-Prozesse verkleidet, Spuren in Form von Log-Einträgen oder benötigten Zwischendateien gelöscht und Sprungadressen ausgelagert oder erst im Rechenprozess erzeugt, so dass die Forensik erschwert wird.

- Die Zielgruppen bzw. Zielpersonen werden diversifiziert. Einzelnutzer stehen als Lösegeldzahler weniger im Mittelpunkt als früher, da die Monetarisierung hier schwieriger zu sein scheint. Die Forderungen werden daher differenziert mit geschäftsmäßigem Blick auf die monetäre Potenz und die betroffenen Werte der Rechnerinhalte variiert. Es werden neue Zielgruppen gesucht, z. B. potenzielle Spieler als Käufer oder mögliche Opfer für andere Online-Spieler oder Personen, die empfänglich für soziale Fragen sind. Unabhängig davon, ob die Behauptung, das Lösegeld z. B. für Flüchtlinge zu verwenden, wahr ist oder nicht, zeigt sich hier eine starke Innovationskraft, um die Angriffsfläche zu vergrößern.

- Parallel zeichnet sich eine Diversifizierung der Angriffsvektoren ab. Verschiedene Familien verbreiten sich über SPAM, Exploit-Kits, Drive-by-Exploits, Würmer, Fernwartungs-Software. Ransomware scheint in dem Maße abzunehmen, wie sich andere Modelle – wie das Krypto-Mining – finanziell eher lohnen oder konstanteren Gewinn versprechen. Andererseits könnten im Umkehrschluss Änderungen der Ausgangssituation auch wieder eine Zunahme bewirken, etwa fallende Kurse bei Kryptowährungen oder die höhere Bereitschaft, Lösegeldzahlungen zu akzeptieren, da neben dem Entzug von Daten auch deren Veröffentlichung unangenehme und teure Folgen haben kann.

Als Maßnahme gegen Ransomware-Angriffe ist ein regelmäßiges, ausgelagertes Backup (inklusive Test der Wiederherstellbarkeit) essentiell. Dabei sollte die Verbindung zum Backup-Medium nicht permanent beschreibbar sein, da die Ransomware sonst auch das Backup verschlüsseln kann. Updates für Betriebssysteme und Anwendungen sollten regelmäßig und zeitnah eingespielt werden. Eine wichtige Regel ist außerdem höchste Vorsicht beim Umgang mit E-Mails und Links aus unbekannten Quellen. Die Aufrechterhaltung der Wachsamkeit (Awareness), Updates und Backups sollten selbstverständlich sein. Durch die neueren Verbreitungswege für Ransomware und die Fokussierung auf „wertvollere Opfer“ kommt aber noch hinzu, dass für öffentlich erreichbare Endpunkte strenge Passwortrichtlinien gelten müssen und Fernzugriffe sowohl zeitlich als auch in der Zahl der Zugänge auf ein Minimum reduziert und explizit freigegeben werden müssen. Auch muss die verwendete Serversoftware einem besonders intensiven Monitoring in Bezug auf ihre Schwachstellen und Exposition unterzogen werden.

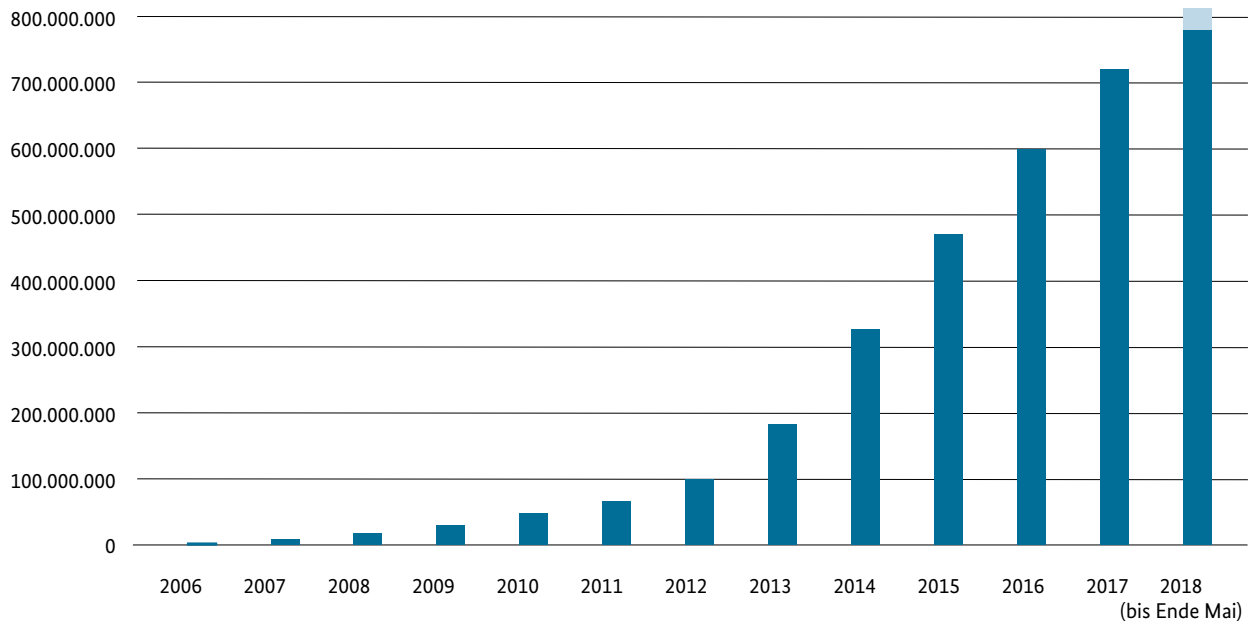


Abbildung 12 Bekannte Schadprogramme, Quelle: AV-Test, Stand: 31.05.2018

1.4.7 Schadprogramme

Unter dem Begriff Schadprogramme (engl. Malware) werden alle Arten von Computerprogrammen zusammengefasst, die unerwünschte und schädliche Funktionen auf einem Computersystem ausführen. Die Begriffe Trojaner, Viren, Würmer etc. werden meist synonym für alle Arten von Schadprogrammen genutzt. Schadprogramme sind fester Bestandteil der meisten Angriffsszenarien – wie z. B. bei der Infektion eines Clients durch Ransomware, bei Botnetzen und bei APT-Angriffen.

Im Berichtszeitraum wurden von dem IT-Sicherheits-Unternehmen AV-Test (https://www.av-test.org/de/) täglich im Durchschnitt rund 390.000 neue Schadprogramme beobachtet.

Zusätzlich zu den Schadprogrammen für PCs wurden innerhalb des Berichtszeitraums pro Monat durchschnittlich etwa 690.000 neue Schadprogramme für das Mobilbetriebssystem Android beobachtet (Quelle: AV-Test). Es wird erwartet, dass noch 2018 die Anzahl von Schadprogrammen für Android auf über 30.000.000 ansteigen wird.

Infektionswege

Im Berichtszeitraum zeichnete sich ein verstärkter Wandel vom Infektionsweg über den Anhang einer E-Mail hin zu E-Mails ab, in denen der E-Mail-Text einen Link auf eine Schadsoftware enthält. Auf diese Weise wird die Schadsoftware nicht direkt auf dem Mailserver gespeichert, wo entsprechende Sicherheitsmaßnahmen diese entdecken und entfernen könnten, sondern die Schadsoftware wird durch diese Methode direkt zum Client transportiert. Dies kann entweder durch einen Download des Schadprogramms und dessen manuelles Ausführen oder mit Hilfe einer Drive-by-Infektion erfolgen.

Krypto-Mining

Ein aktueller Trend ist die Zunahme von Software, mit der Kryptowährungen „geschürft" werden. Diese so genannten Krypto-Miner nutzen die Ressourcen der betroffenen Systeme, um monetären Gewinn in Form von Kryptowährungen zu erzielen. Diese Systeme werden dann Teil eines Netzwerkes, das gemeinsam eine rechen- und ressourcenintensive Dienstleistung im Umfeld von Blockchain-Berechnungen (Validierung von Transaktionen) erbringt und diese Dienstleistung in Form von Kryptowährungen erstattet bekommt. Dabei muss zwischen freiwilligem und unfreiwilligem (verstecktem) Mining unterschieden werden. Im ersten Fall stellt der Nutzer freiwillig die Rechenleistung seines Systems zur Verfügung. Bei der versteckten Nutzung dieser Techniken konnten unterschiedliche Methoden beobachtet werden:

- Krypto-Miner, die Besucher einer Webseite dazu bringen, mit Hilfe von JavaScript-Bibliotheken, die durch den Browser ausgeführt werden, an dem Mining zu partizipieren.
- Schadprogramme, die betroffene Systeme als Teil eines Botnetzes Kryptowährungen schürfen lassen.

Zusätzlich nutzen Kriminelle bereits existierende Schadprogramme, um den Nutzern die geschürfte oder anderweitig erworbene Kryptowährung zu stehlen, indem Zugangsdaten von Speichern für diese Währung (sogenannte Krypto-Wallets) ausgespäht werden.

Krypto-Mining kann auf den unterschiedlichsten Geräten und Systemen erfolgen. Im Berichtszeitraum wurden Vorfälle nicht nur auf normalen PCs, sondern auch auf Servern, Mobilbetriebssystemen, SmartTVs und ICS-Systemen beobachtet. Besonders Unternehmensserver bieten aufgrund ihrer zumeist größeren Ressourcen und der ständigen Verfügbarkeit dieser Ressourcen sehr attraktive Ziele für Kriminelle. Es ist anzunehmen, dass zukünftig noch weitere Ziele und Plattformen genutzt werden (z. B. Webcams, SmartHome-Produkte), sodass auch diese in Hinblick auf eine kriminelle Nutzung überwacht werden sollten. Dies gilt insbesondere, da Krypto-Miner häufig eine lange Zeit unentdeckt bleiben, da sie sich außer durch Performance-Einbußen sowie einen eventuell erhöhten Stromverbrauch bei betroffenen Systemen unauffällig verhalten. Zudem sind diese „Auffälligkeiten" in der Regel so marginal, dass sie als Indikatoren nicht geeignet sind.

Bedrohung weiterhin kritisch

Wie bereits in den Vorjahren sind Schadprogramme auch im aktuellen Berichtszeitraum eine der größten Bedrohungen für Privatanwender, Unternehmen und Behörden. Dies zeigte sich auch in der Cyber-Sicherheits-Umfrage 2017 der Allianz für Cyber-Sicherheit, bei der Malware-Infektionen erneut als die häufigste Angriffsart genannt wurden.

1.4.8 Schwachstellen in Chips

Sicherheitselemente speichern kryptografisches Schlüsselmaterial und implementieren zahlreiche Algorithmen. Sie dienen als Anker für sicherheitskritische Anwendungen, wie sichere Authentifizierung, verschlüsselte Kommunikation oder elektronische Signaturen.

Die verwendeten Algorithmen sind dabei üblicherweise erprobt und teilweise sogar mathematisch beweisbar sicher. Das sichere Speichern des Schlüssels und insbesondere das Verarbeiten von Schlüsselmaterial ist aber nach wie vor eine große Herausforderung, da zwangsläufig messbare physikalische Phänomene entstehen, die einen Rückschluss auf den Schlüssel zulassen.

Bei älteren Chipgenerationen konnte z. B. der Inhalt des ROM einfach mit Hilfe eines digitalen Mikroskops ausgelesen werden, da sich eine gespeicherte ‚1' optisch deutlich von einer ‚0' unterscheidet. Auch durch Messen des Stromverbrauchs während der Verarbeitung kann ein Schlüssel angegriffen werden, da der Stromverbrauch in Abhängigkeit unterschiedlicher Bitfolgen variiert. Gegen solche Seitenkanalangriffe implementieren heutige Sicherheitselemente zwar zahlreiche Gegenmaßnahmen die Angriffe signifikant erschweren, aber gleichzeitig wurden auch die Angriffstechniken in zahlreichen Forschungsergebnissen verbessert. Während Seitenkanalangriffe verhältnismäßig einfach umsetzbar sind, finden invasive Angriffe auf die Hardware, bei denen physische

Key Reinstallation AttaCKs (KRACK) auf WLAN-Schwachstelle

Sachverhalt
Im Oktober 2017 veröffentlichte der Sicherheitsforscher Mathy Vanhoef ein Forschungspapier, das einen mit dem Namen Key Reinstallation AttaCKs (KRACK) bezeichneten Angriff auf das Wi-Fi-Protected-Access-Protokoll (WPA, WPA2) beschreibt. Bei WPA2 handelt es sich um den aktuellen Sicherheitsstandard für Funknetzwerke, der in beinahe jedem WLAN-fähigen Gerät integriert ist. Zurückzuführen ist die dem Angriff zugrundeliegende Schwachstelle auf einen Design-Fehler im Standard IEEE 802.11i, dessen Sicherheitsfunktionen in WPA2 implementiert wurden.

Ursache/Schadenswirkung
Der aktuelle Sicherheitsstandard IEEE 802.11i hat ein mehrstufiges Handshake-Verfahren als Netzwerk-Authentifizierungsprotokoll festgelegt, das eine höhere Sicherheit für den Aufbau und die Nutzung von WLANs bietet. Die Schritte des Vier-Wege-Handshake-Verfahrens bestehen aus einer Kommunikation zwischen Client und Access-Point (Zugangspunkt), in dessen Rahmen wichtige Krypto-Elemente berechnet und ausgetauscht werden. Das Kernziel dieses Austauschs ist, dass der Client sich gegenüber dem Access-Point authentifizieren und eine sichere Verschlüsselung gewährleisten kann. Im Rahmen des Verfahrens wird ein gemeinsamer Sitzungsschlüssel für beide Parteien generiert und installiert. Anschließend können mit dem Schlüssel Daten verschlüsselt werden, um deren Vertraulichkeit und Integrität der Daten zu gewährleisten.

KRACK setzt an der Stelle nach der „Installation" des Sitzungsschlüssels an. Sobald die Nachricht des Access-Points für den Sitzungsschlüssel an den Client gegangen ist, installiert dieser den gemeinsam generierten Schlüssel und bestätigt diesen Schritt an den Access-Point. Da jedoch gelegentlich Nachrichten im Netz verloren gehen oder gelöscht werden können, sendet der Access-Point bei Ausbleiben der Bestätigung durch den Client die Nachricht erneut. In diesem Fall installiert auch der Client ggf. den Sitzungsschlüssel erneut. Gleichzeitig werden die inkrementelle Sendepaketnummer (Nonce) und der Wiedergabezähler, der vom Datenvertraulichkeitsprotokoll verwendet wird, zurückgesetzt. Mit KRACK erzwingt der Angreifer Wiederholungen der Nachricht vom Access-Point, um so das Zurücksetzen des Nonce einzuleiten. Auf diese Weise kann eine erneute Verschlüsselung mit demselben Keystream (da abhängig vom Nonce) erzwungen werden, wodurch z. B. Datenpakete wiedergegeben, entschlüsselt und/oder gefälscht werden können. Jedoch muss sich der Angreifer dafür in Reichweite des Funknetzes befinden. Der Angriff funktioniert vergleichbar auch bei anderen WLAN-Handshake-Verfahren (Peerkey, Group Key, Fast BSS Transition).

Reaktion
Das BSI veröffentlichte zeitnah technische Informationen und eine Pressemitteilung zu dem Angriff. Zusätzlich beobachtete und bewertete das BSI die Bereitstellung der Patches der verschiedenen Hersteller und aktualisierte kontinuierlich die bereitgestellten Informationen für Wirtschaft, Bürger und Behörden.

Empfehlung
WPA2 sollte weiterhin eingesetzt und vom Hersteller bereitgestellte Sicherheits-Updates sollten eingespielt werden. Weiterhin empfiehlt es sich, kabellose Verbindungen durch eine VPN-Verschlüsselung zusätzlich abzusichern.

Sicherheitsprobleme bei macOS

Sachverhalt
Das Betriebssystem macOS High Sierra (Version 10.13) der Firma Apple war von Oktober 2017 bis März 2018 von Sicherheitsproblemen im Zusammenhang mit Passwörtern betroffen.

Die sogenannte „root"-Lücke ermöglichte es einem Angreifer, auf einem entsperrten macOS-Gerät durch Eingabe des Nutzernamens „root" und einer leeren Passwortzeile die Sicherheitseinstellungen von macOS zu überwinden. Anschließend konnte er sich ohne die Eingabe eines Passwortes als Benutzer „root" mit vollen administrativen Rechten auf diesem System anmelden. Dieser Vorgang war unter bestimmten Voraussetzungen auch über das Apple-eigene Remote Access Tool ohne physischen Zugriff auf das Gerät möglich.

Zudem war es möglich, die Systemeinstellungen des Mac App Stores mit jeder beliebigen Zeichenkette zu öffnen. Anschließend konnte ein Angreifer auch weitere Systemeinstellungen öffnen und ändern. Dazu gehörten auch die Netzwerk-Einstellungen, um beispielsweise die DNS-Einstellungen des Systems zu manipulieren, um das Opfer auf nicht vertrauenswürdige Webseiten (z. B. Phishing-Webseiten) umleiten zu können.

In der Betriebsversion macOS High Sierra hat Apple das neue Dateisystem APFS (Apple File System) eingeführt. Hierbei kam es ebenfalls zu Sicherheitsproblemen: Zum einen wurde das Passwort von verschlüsselten APFS-Partitionen in der sogenannten „Merkhilfe" im Klartext gespeichert. Zum anderen konnte sich beim Anlegen von verschlüsselten APFS-Partitionen das Passwort in den Protokolldateien (Log Files) im Klartext befinden.

Ursache/Schadenswirkung
Apple hat insbesondere auf das Sicherheitsproblem der „root"-Lücke schnell reagiert und sowohl Hilfestellungen als auch entsprechende Sicherheits-Updates zur Verfügung gestellt. In einem Statement bedauerte Apple das Sicherheitsproblem und versprach, die Entwicklungsprozesse zu überprüfen.

Reaktion
Das BSI steht im direkten Kontakt mit Apple Deutschland und hat sich unmittelbar nach Bekanntwerden der „root"-Lücke zu diesem Themenkomplex ausgetauscht. Dabei wurden praktische Handlungsempfehlungen zur Abschwächung des Problems identifiziert und schnellstmöglich auf der BSI-Webseite veröffentlicht.

Empfehlung
Das BSI empfiehlt die Vergabe eines starken Passworts für den Root-Account von macOS-Geräten. Des Weiteren sollten die automatischen Updates des Betriebssystems aktiviert werden, damit insbesondere Sicherheits-Updates schnellstmöglich eingespielt werden können.

Manipulationen am Chip beispielsweise per Fehlerinduktion durch Laserbeschuss bis hin zur Modifikation der Schaltkreise vorgenommen werden, aufgrund des damit verbundenen Aufwands keine weite Verbreitung.

Ein weiteres Problem sind algorithmische Schwächen. Zwar sind die verwendeten Verfahren erprobt, jedoch können manchmal kryptografisch sichere Algorithmen aufgrund beschränkter Rechen- und Speicherkapazität von Sicherheitselementen nicht implementiert werden.

Aufgrund der beschränkten Ressourcen von Hardware-Sicherheitselementen müssen komplexe kryptografische Operationen durch in Hardware realisierte Funktionsbausteine beschleunigt werden, dennoch bleiben sehr komplexe Operationen, wie insbesondere die Schlüsselerzeugung bei RSA, in Abhängigkeit von der Schlüssellänge sehr zeitaufwändig, da hierbei große Primzahlen zufällig gesucht werden müssen. Durch die Verwendung von FastPrime, eines proprietären Algorithmus zur Konstruktion von großen Primzahlen wird die Schlüsselerzeugung beschleunigt, allerdings hat sich herausgestellt, dass die so erzeugten Schlüssel, mit wenigen Ausnahmen kryptografisch deutlich schwächer sind als zu erwarten.

Proprietäre Verfahren, die zwar deutlich schneller sind, unterliegen auch keiner Prüfung im Rahmen von Forschung und Sicherheitsevaluierungen. Eine Sicherheitszertifizierung nach Common Criteria etwa bewertet nicht die mathematische Stärke eines kryptografischen Verfahrens selbst, sondern nur die sichere Umsetzung (Seitenkanalresistenz) auf dem Chip.

Die Ende 2017 als ROCA (Return of the Coppersmith Attack) von einem Forscherteam publizierte Schwäche betrifft genau ein solches Verfahren, dass in einer Kryptobibliothek von Infineon auf Smartcards zum Einsatz kam. Aufgrund zu geringer Entropie ließ sich bei so erzeugten RSA-Schlüsseln mit einigem Rechenaufwand der private RSA-Schlüssel aus dem öffentlichen Schlüssel rekonstruieren (siehe auch Vorfall ROCA).

ROCA ist grundsätzlich kein neues Problem, sondern das Resultat der grundsätzlich aufwändigen Schlüsselerzeugung von RSA. Mithilfe des sogenannten Coppersmith Angriffs kann ein RSA Modulus effizient(er) faktorisiert werden, wenn die obersten Bits einer der Primzahlen bekannt sind. Dieser Effekt tritt nicht nur durch die Art der Konstruktion von Primzahlen nach dem proprietären FastPrime-Algorithmus auf, sondern auch wenn schlechte Zufallszahlengeneratoren verwendet werden. Das Problem der schlechten Zufallszahlen hat beispielsweise 2015 zu einem erfolgreichen Angriff auf einen Teil der taiwanesischen ID-Karten geführt.

Auch die längeren Entwicklungs- und Nutzungsszenarien bei Sicherheitselementen stellen ein Problem dar. Während in Softwareprodukten bekannt gewordene Schwächen durch kurzfristige Patches beseitigt werden können, sehen Sicherheitselemente üblicherweise eine Möglichkeit von Updates im Feld vor. Gerade eine Verwendung über mehrere Jahre hinweg – während in dieser Zeit Angriffe deutlich weiterentwickelt werden – führt so bei nicht ausreichender Vorbereitung zu schwer behebbaren Sicherheitslücken.

Seitenkanalanalysen im Bereich symmetrischer Algorithmen (AES) und klassischer asymmetrischer Kryptografie (RSA) sind fortwährend Gegenstand der Forschung. Ältere Sicherheitselemente zeigen oft Schwächen in Bezug auf die Seitenkanalresistenz. Selbst wenn deren Sicherheit ursprünglich nach Common Criteria erfolgreich zertifiziert werden konnte, stellt eine solche Zertifizierung immer nur eine Momentaufnahme des aktuellen Stands der Technik dar. Auch für zertifizierte Sicherheitselemente stellen Seitenkanalangriffe somit mit zunehmendem Alter der Hardware eine Bedrohung in der Praxis dar.

Aus diesem Grund wird die Gültigkeit der Sicherheitszertifikate befristet, für Chipkarten und ähnliche Produkte in der Regel auf fünf Jahre. Für sicherheitsrelevante Anwendungen, die sich eine längere Zeit im Feld befinden, sollten Update-Mechanismen mindestens für die Implementierung der Kryptoverfahren vorgesehen werden. Entsprechende Sicherheitsvorgaben nach Common Criteria werden durch das BSI entwickelt und bereitgestellt. Um Entwickler bei der sicheren Implementierung von Applikationen zu unterstützen, die Sicherheitselemente als Baustein in einem Gesamtsystem einsetzen, geht darüber hinaus der Trend zu modularisierten Komponenten, bei dem kryptografische Services gekapselt über definierte Schnittstellen bereitgestellt werden. Bei Verwendung solcher Schnittstellen ist dann hinreichend garantiert, dass nicht unbeabsichtigt Seitenkanäle in der Implementierung geschaffen werden.

1.4.9 Schwachstellen in Software und Hardware

Die Anzahl der bekannt gewordenen Schwachstellen in vom BSI regelmäßig betrachteten Softwareprodukten war auch im Berichtszeitraum unverändert hoch. Es gibt keine Anzeichen, dass sich diese Lage in den kommenden Jahren ändern wird. Dies gilt auch für andere Software-Produkte und kombinierte Hard- und Softwareprodukte, die nur anlassabhängig und nicht laufend vom BSI betrachtet werden. Zwar werden Softwareentwicklungswerkzeuge (Compiler, IDEs, Quellcode-Analysatoren) verbessert und können Softwareentwickler auf gewisse Fehlerquellen hinweisen, gleichzeitig untergraben aber mehrere Trends die Sicherheit im Endprodukt:

- Massiv gestiegene Komplexität von Endanwendungen,
- Containerisierung mit nur teilweise aktualisierten Softwarekomponenten,
- ungeprüfte Integration von immer mehr externen Abhängigkeiten,
- Geschwindigkeitsoptimierungen zu Lasten der Sicherheit,
- Verzicht auf Fehlerbehebung mit Verweis auf Mitigation-Maßnahmen und
- Verweigerung von Sicherheitsupdates durch viele Hersteller.

Ferner ist es bei Kauf eines Softwareprodukts oder kombinierten Soft-/Hardwareprodukts fast immer vor dem Kauf und oftmals auch nach dem Kauf unmöglich, eine qualifizierte Aussage über die Sicherheit bzw. die Menge der im Produkt vorhandenen bekannten Schwachstellen zu treffen.

Für den betrachteten Zeitraum ist auffällig, dass der Linux-Kernel überdurchschnittlich viele Schwachstellen aufzuweisen scheint. Dies ist darin begründet, dass viele Schwachstellen in Treiber-Modulen gefunden wurden, die auch in Android-Smartphones Verwendung finden. Diese Schwachstellen werden, anders als bei Microsoft Windows, aufgrund der Tatsache, dass sie zusammen mit dem Linux-Kernel gepatcht werden, dem Linux-Kernel zugerechnet. Bei Microsoft Windows ist der jeweilige Treiber-Hersteller in der Pflicht, die erforderlichen Updates zu veröffentlichen, die zudem noch manuell durch den Endnutzer einzeln eingespielt werden müssen.

Wie auch in den Vorjahren war festzustellen, dass im betrieblichen Umfeld Sicherheitsupdates häufig verzögert oder gar nicht eingespielt werden oder eingesetzte Produkte keine Sicherheitsupdates mehr vom Hersteller erhalten. Es kommt oft zu Verzögerungen bei der Installation von Sicherheitsupdates, da dies mit betrieblichen Prozessen (wie beispielsweise halbjährliche Wartungszyklen) abgestimmt werden muss und in einigen Fällen zusätzlichen regulatorischen Anforderungen unterliegt. Dies betrifft auch Bereiche, in denen vom betreffenden Softwareprodukt direkt oder indirekt Menschenleben

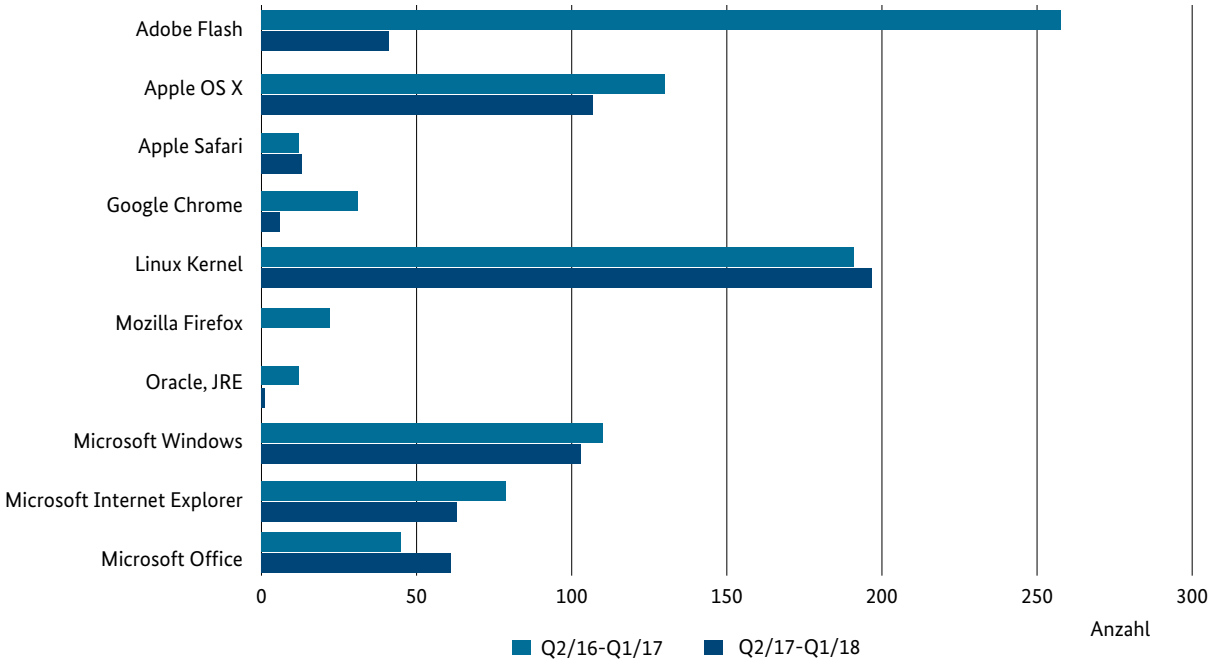


Abbildung 13 Kritische CVE-Einträge, Stand: 31.03.2018

Spectre, *Meltdown* – Angriff auf Hardware-Architekturen

Sachverhalt
Anfang 2018 wurde eine neue Klasse von Angriffen auf Central-Processing-Unit (CPU)-Architekturen einer größeren Öffentlichkeit bekannt. Die unter den Namen *Meltdown* und *Spectre* bekannt gewordenen Schwachstellen sind insofern neuartig, als dass sie architektonische Eigenschaften von modernen CPUs geschickt miteinander verknüpfen, um geschützte Speicherbereiche auslesen zu können. Betroffen sind fast alle aktuellen CPUs der Hersteller Intel, AMD und ARM.

Ursache/Schadenswirkung
Die Schwachstellen nutzen Eigenschaften der Hardware aus, die seit Mitte der 1990er Jahre zunehmend in die Prozessoren eingebaut wurde. Das primäre Ziel war dabei, die Leistungsfähigkeit zu erhöhen und den damit verbundenen Ressourcenaufwand zu minimieren. Technologien wie Out-of-Order-Ausführung von Befehlen oder die spekulative Ausführung von Code gehören hierzu. In Verbindung mit den zeitgleich stetig ausgebauten Cache-Speicherbereichen führte dies zu einem weitgehend unbekannten wie unkalkulierbaren Risiko für den Betreiber der Plattform.

Je nach ausgenutzter Schwachstelle kann ein Angreifer die vom Betriebssystem und/oder der Hardware bereitgestellten Sicherheitsmechanismen überwinden und Daten lesen. Treten hardwarebasierte Probleme auf, sind die dann notwendigen mitigierenden Maßnahmen oft mit einem erheblichen finanziellen und personellen Aufwand oder merklichen Leistungseinbußen verbunden.

Reaktion
Die Neuartigkeit dieser Angriffsklasse widerlegt bisherige Annahmen zu Eigenschaften von Plattformen. Dies muss bei der Sicherheitsanalyse von bestehenden und künftigen Systemen und Produkten Berücksichtigung finden. Früher durchgeführte Analysen müssen daraufhin überprüft werden, ob sie auch nach der jetzt erforderlichen Korrektur entsprechender Grundannahmen weiterhin anwendbar sind.

Empfehlung
Die Problemklasse bleibt, bedingt durch ihre tiefe strukturelle Verwurzelung in der Hardware, bis auf weiteres erhalten. Aktuell ist nicht absehbar, durch welche Änderungen die CPU-Hersteller diese Schwachstelle beseitigen werden. Bis Ende 2018 wird auch neu beschaffte Hardware weiterhin angreifbar bleiben, da neu entwickelte CPUs von Intel und AMD erst für Anfang 2019 angekündigt wurden.

Es ist davon auszugehen, dass mit fortschreitender Analyse der zugrunde liegenden Probleme weitere Angriffsmethoden ähnlicher Art entdeckt werden. Aufgrund der praktischen Relevanz von bisher eher theoretischen Angriffsarten werden die Angriffsmethoden durch Weiterentwicklung sukzessiv Einzug in den Kreis der „üblichen“ und „marktreifen“ Techniken halten. Auf Plattformen mit mehreren Prozessoren kann in bestimmten Fällen ein Sicherheitsgewinn erreicht werden, wenn Prozesse (oder virtuelle Maschinen), die es zu isolieren gilt, an den Ausführungskontext von unterschiedlichen Prozessoren gebunden werden („Pinning“). Hierdurch können Angriffe signifikant erschwert werden.

Moderne Prozessoren und Chipsätze besitzen eine hohe Komplexität; viele interne Mechanismen sind Firmengeheimnisse der Hersteller und werden daher nicht offengelegt. Hieraus folgt, dass diesen zentralen Komponenten nicht vollumfänglich vertraut werden kann und auch künftig nicht abschätzbare Risiken verbleiben. Ob und ggf. wie eine Anwendung betroffen ist und durch welche Maßnahmen dieser Bedrohung entgegengewirkt werden kann, ist vom Einzelfall abhängig und muss sorgfältig geprüft werden. Bis durch die Hardwarehersteller geeignete Lösungen und eine ausreichende Transparenz bereitgestellt werden, können die Auswirkungen auf installierten Systemen zum Teil durch Softwareänderungen abgemildert oder behoben werden. Dies wird durch die kurzfristige Installation verfügbarer Patches für Firmware, Microcode, Betriebssystem und Anwendungsprogrammen erreicht.

abhängen (z. B. Safety-Systeme, Medizinprodukte) oder industrielle Prozesse, bei denen Fehler bei Updates große Kosten verursachen. Ferner sind gerade Geräte mit hohen Investitionskosten oftmals so lange im Einsatz, dass der Hersteller keinen Support mehr anbietet.

Noch schwerer wiegen Fälle, in denen der Hersteller eines Softwareprodukts nicht mehr am Markt vertreten oder nicht feststellbar ist bzw. jeglichen Support verweigert. Hinzu kommen Probleme, bei denen Sicherheitsupdates z. B. nicht in das Betriebssystem installiert werden können, weil davon abhängige Software dann nicht mehr korrekt arbeiten würde.

Neben verzögerten oder nicht eingespielten Sicherheitsupdates trägt die mangelnde Bereitschaft der Hersteller, über den Sicherheitsstatus ihrer Produkte zu informieren und diesen zumindest während der Gewährleistung zu pflegen, wesentlich zur prekären Sicherheitslage bei.

Besonderheiten bei Mozilla Firefox und Google Chrome

Für die beiden vom BSI regelmäßig betrachteten Softwareprodukte Mozilla Firefox und Google Chrome sind im vergangenen Betrachtungszeitraum Auffälligkeiten zu beobachten. So scheint Mozilla seit Oktober 2016 für den Firefox keine Einträge mehr in der MITRE CVE-Datenbank zu pflegen. In den eigenen Veröffentlichungen (Mozilla Foundation Security Advisories) werden weiterhin CVE-Einträge referenziert, die aber in die öffentliche Datenbank nicht eingepflegt werden. Es ist weder eine Beschreibung der Schwachstelle angegeben, noch wird auf den Firefox-Browser als betroffenes Produkt verwiesen. Eine Bewertung der Schwachstelle sowie ein Basescore fehlen.

Google scheint mit ihrem Browser Chrome seit Ende Oktober 2017 ähnlich zu verfahren und auch keine Einträge mehr in der CVE-Datenbank zu pflegen. In den Release Updates zu Chrome nennt Google ebenfalls nach wie vor CVE-Nummern. Die entsprechenden Einträge in der MITRE CVE-Datenbank sind jedoch leer. Auch Google gibt weder eine Beschreibung der Schwachstelle an, noch wird auf den Chrome-Browser als betroffenes Produkt verwiesen. Die Bewertung der Schwachstelle sowie ein Basescore fehlen ebenfalls.

Bei im Betrachtungszeitraum gepflegten CVE-Einträgen zu Google Chrome ist ferner auffällig, dass sie fast ausschließlich mit einem CVSS v2.0 Basescore von 6,8 Medium bewertet werden. Somit erscheinen die gemeldeten Schwachstellen nicht als kritische Schwachstellen, da dafür ein CVSS v2.0 Basescore von 7,0 oder größer zu Grunde gelegt wird.

Für Google Chrome bleibt abzuwarten, ob die zunächst nur reservierten CVE-Einträge nach Ablauf einer internen Sperrfrist in der MITRE CVE-Datenbank aktualisiert werden oder ob Google, wie Mozilla für den Firefox, gar keine offiziellen CVE-Einträge mehr pflegt.

Update-Fähigkeit von Smartphones

Auch Smartphones werden mit öffentlich bekannten Schwachstellen im Handel als neu vertrieben, ohne dass entsprechende Sicherheitsupdates zur Verfügung stehen. Dadurch existieren für Verbraucherinnen und Verbraucher bei der Nutzung teils gravierende Sicherheitslücken.

Ein Beispiel dafür sind die im Juli 2015 unter dem Namen „Stagefright“ bekannt gewordenen Sicherheitslücken im gleichnamigen Multimedia-Framework des Betriebssystems Android von Google. Für Verbraucher sind die Aktualität der Software und fehlende Update-Möglichkeiten kaum zu erkennen. Für eine informierte Kaufentscheidung sind jedoch transparente Informationen notwendig. Diese liefern die Verkäufer oftmals nur unzureichend. Nachdem das BSI bei einem Smartphone Sicherheitslücken festgestellt hatte, nutzte die Verbraucherzentrale NRW ihre Befugnis zur Verbandsklage und leitete ein gerichtliches Unterlassungsverfahren gegen den Verkäufer des betroffenen Geräts wegen unzureichender Verbraucherinformation ein. Das Verfahren ist noch nicht abgeschlossen. Der Koalitionsvertrag zwischen CDU, CSU und SPD sieht vor, den Verbraucherschutz als zusätzliche Aufgabe des BSI zu etablieren.

Käufer haben im Allgemeinen weder Geld noch Zeit noch Expertise, die IT-Sicherheit eines Produktes zu beurteilen und müssen sich entweder auf Herstelleraussagen oder Tests Dritter verlassen. Herstelleraussagen zur IT-Sicherheit der meist im Ausland hergestellten SoHo-Produkte (Small-Office- und Home-Office-Produkte) sind aber oftmals unvollständig. Dies gilt nicht nur für Aussagen, ob das Produkt aktuell verwundbar ist oder es öffentlich bekannte Schwachstellen gibt, sondern insbesondere auch für die Erstellung von Sicherheitsupdates. Produkttests von Dritten haben oftmals einen Fokus auf Funktionalität und nicht auf der Sicherheit des Produkts. Ein Überblick der tatsächlichen Update- und Sicherheitssituation für alle marktrelevanten Geräte einer bestimmten Geräteklasse (z. B. Smartphones, Mediaplayer etc.) existiert nicht. Kunden haben somit vor dem Erwerb eines Produktes keine realistische Möglichkeit, die Sicherheit eines Produktes als Kriterium ihrer Kaufentscheidung zu nutzen. Damit haben Hersteller mit sichereren Produkten keinerlei Vorteile im Markt.

Ein Produkt, welches zum Zeitpunkt des Kaufs öffentlich bekannte Schwachstellen enthält, muss aus IT-Sicherheitsgesichtspunkten als mangelhaft angesehen werden, wenn auf die Schwachstellen nicht ausdrücklich hingewiesen wird oder kein entsprechendes Sicherheitsupdate beim Kauf zur Verfügung steht. Gleiches gilt auch für Schwachstellen, die während der Gewährleistungsfrist des Produkts bekannt werden. Eine Softwarepflege durch den Hersteller einschließlich der Behebung von Schwachstellen ist somit nicht nur „Stand der Technik", sondern sollte durch den Verbraucher auch offensiv als Standardleistung eingefordert werden.

1.4.10 Spam

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

- Klassischer Spam wird häufig für Produkt-, Wertpapier- oder Dienstleistungswerbung benutzt und zudem für Betrugsversuche wie Vorschussbetrug eingesetzt.
- Mit Schadprogramm-Spam (Malspam) 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 bzw. im Anhang erfolgen, der auf ein Schadprogramm oder eine Webseite mit Drive-by-Exploits verweist.
- 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.

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 zusammengeschlossen, was die Vermarktung von Spam als Dienstleistung durch Cyber-Kriminelle erleichtert.

Die Verwendung von persönlichen Daten aus Datenabflüssen bei großen Dienstleistern, Kontakten aus E-Mail-Clients infizierter Systeme oder sogar recherchierten Daten wird derzeit immer häufiger beobachtet. Dies steigert die Wahrscheinlichkeit einer Infektion in erheblichem Maße.

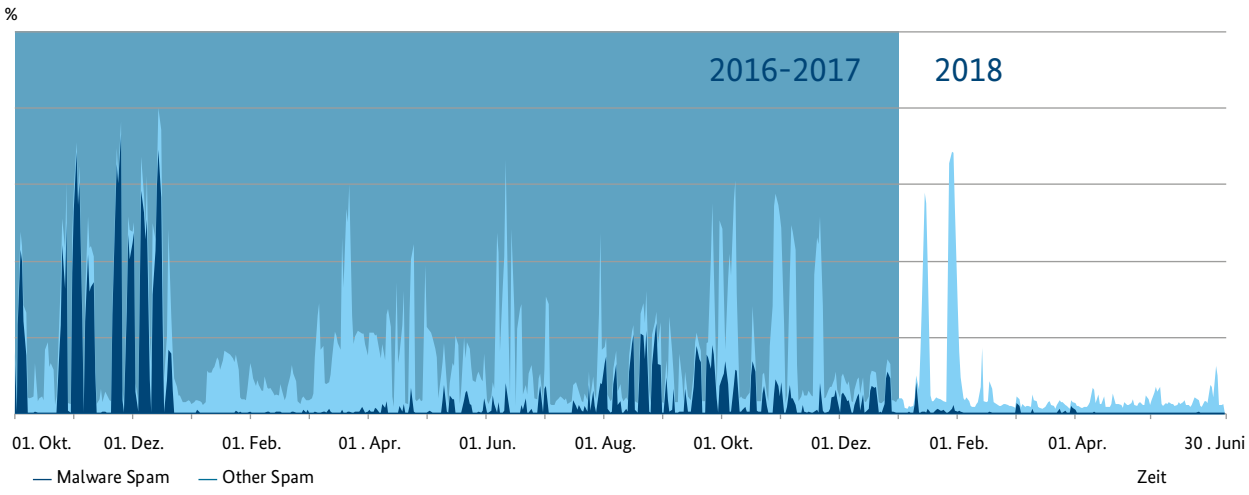


Abbildung 14 Qualitativer Spam- und Malwarespam-Verlauf in Deutschland, 01.20.2016 bis 31.05.2017

Phishing mit BSI-Absender

Sachverhalt
Dem BSI wurde Anfang 2018 gemeldet, dass sich gefälschte E-Mails mit BSI-Absender im Umlauf befänden. Sie enthielten Informationen zum Thema „*Spectre*/*Meltdown*“ sowie einen Link zu einer Nachbildung der „BSI für Bürger-Webseite“. Die URL wies Ähnlichkeit zu offiziellen BSI-URLs auf. Auf der gefälschten Webseite wurde dem Benutzer eine als Update-Tool getarnte Schadsoftware angeboten. Die Webseite selbst war eine Kopie der „BSI für Bürger“-Webseite inklusive eines gültigen SSL-Zertifikates, welches für diese Betrugsseite selbst ausgestellt war. Auf den ersten Blick erweckte diese Seite somit den Eindruck, eine offizielle BSI-Webseite zu sein. Die Webseite selbst enthielt einen Download-Link zu einem angeblichen „Windows-Tool“ zur Beseitigung der „*Spectre*“ und „*Meltdown*“-Schwachstelle.

Ursache/Schadenswirkung
Anfang dieses Jahres wurden die Prozessor-Schwachstellen *Spectre* und *Meltdown* der breiten Öffentlichkeit bekannt. Die Informationen über diese Schwachstellen sickerten für einige Softwarehersteller jedoch zu früh an die Öffentlichkeit durch, sodass diese Hersteller noch keine passenden Updates für ihre Software bereitgestellt hatten. In der Folge lieferten einige Hersteller Updates nach, welche zum Teil wieder zurückgerufen wurden, für andere Systemen wurden überhaupt keine Updates angeboten.

Angreifer machten sich den allgemeinen Wunsch nach Updates der Benutzer zu Nutze und verteilten mit gefälschtem Absender E-Mails im Namen des BSI, die suggerierten, dass das BSI ein Update für die Schwachstellen *Spectre* und *Meltdown* bereitstellen würde.

Reaktion
Nach Bekanntwerden der gefälschten BSI-E-Mails sowie der gefälschten BSI-Webseite wurden mehrere Maßnahmen im BSI getroffen, um die Verbreitung der Schadsoftware möglichst zeitnah zu unterbinden. Die Schadsoftware wurde von Spezialisten analysiert. Domains, mit denen die Schadsoftware kommunizierte, wurden innerhalb der Bundesverwaltung umgehend gesperrt und der Öffentlichkeit bekannt gegeben. Gleichzeitig wurde gegen die Betrugsseite vorgegangen, mit dem Ziel, diese vom Netz zu nehmen. Hierzu wurde mit dem Hoster, dem Domainregistrar sowie der Zertifizierungsstelle Kontakt aufgenommen. Es konnte erreicht werden, dass die Webseite in Googles Safebrowsing als Phishing markiert wurde und somit von Firefox als auch von Google Chrome nur nach einer Phishing-Warnmeldung angezeigt wurde.

Empfehlung
Es ist zu beobachten, dass gefälschte E-Mails sowie Webseiten immer professioneller gestaltet werden. Daher sollten E-Mails und Webseiten immer kritisch betrachtet werden. Bei E-Mails sollte speziell geprüft werden, ob Absenderadresse und E-Mail-Text in Form und Inhalt zum angezeigten Absender passen.

Webseiten zu fälschen ist keine große Herausforderung. Deswegen empfiehlt es sich, die Webseiten-URL genau zu betrachten. Angreifer verwenden oft ähnlich aussehende URLs, z. B. mit Buchstabendrehern oder anderen Top-Level-Domains, beispielsweise „.biz“ statt „.de“. Vorteilhaft ist, wenn die Webseite per HTTPS aufgerufen werden kann. In diesem Fall gibt es ein Zertifikat, das in der Regel von einer dritten Stelle ausgestellt wurde und Informationen zum Domainnamen und dem Inhaber enthält. Sofern die ausstellende Stelle vertrauenswürdig ist – die Browserhersteller achten darauf und entfernen auffällig gewordene Stellen aus den mitgelieferten Listen –, kann davon ausgegangen werden, dass auch die Prüfung der Domain sauber erfolgt ist. Die Vertrauenswürdigkeit wird je nach Browser durch ein Schlosssymbol oder farbige Hinterlegung in Ampelfarben signalisiert.

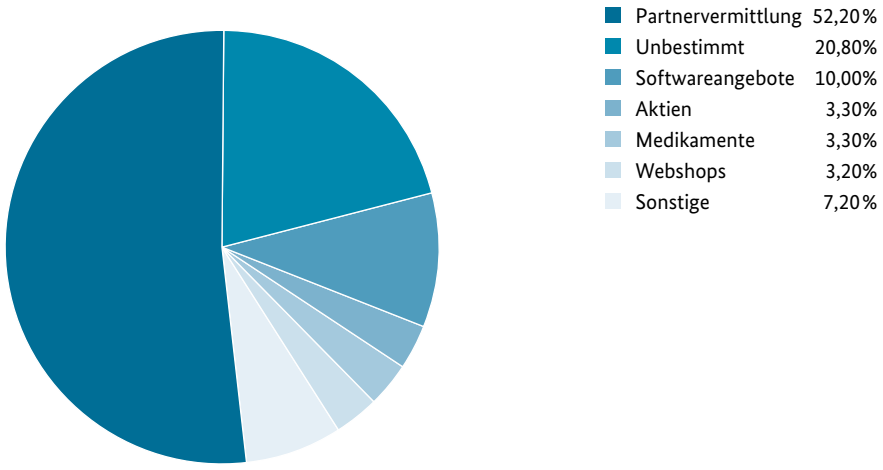


Abbildung 15 Verteilung der Spam-Themenbereiche

Necurs weiterhin dominant

Das *Necurs*-Botnet war weiterhin der größte Versender von Spamnachrichten. Im dritten Quartal 2017 stieg die Anzahl der versendeten *Necurs*-E-Mails mit schadhaftem Anhang an. Allerdings wurde in der Spitze nur etwa ein Drittel des Volumens von Ende 2016 erreicht, dem bislang beobachteten Allzeitmaximum im Malspamversand. Im vierten Quartal stagnierte das Volumen zuerst, um dann im Dezember leicht anzusteigen. Nach der üblichen Weihnachtspause (nach dem orthodoxen Kalender) gab es Mitte Januar nur noch eine größere Malspamwelle. Danach versiegte der Versand fast vollständig.

Im Berichtzeitraum wurde *Necurs* vorwiegend zum Versand von klassischen Spams benutzt. Dabei wurden vor allem russische Dating-Seiten beworben. Einige kleinere Wellen haben versucht den Kurs von Aktien (sog. Penny Stocks) zu manipulieren.

Insgesamt scheint das Botnetz mit dem Spamversand nicht ausgelastet zu sein. Wie die Grafik zeigt, sind im Verlauf einige Spitzen zu sehen, die einen Eindruck über die Gesamtkapazität des Spambotnetzes vermitteln, jedoch in weiten Teilen des Jahres nicht erreicht werden.

Kleine Malware-Spam-Kampagnen

Wie im vergangenen Jahr werden unabhängig vom *Necurs*-Netzwerk weiterhin kleinere Malspam-Kampagnen beobachtet. Besonders auffällig sind hier Spamwellen zur Verbreitung von *Emotet*. Diese Schadsoftware nutzt die bei einer Infektion abgegriffenen Outlook-Daten, um eine E-Mail von einer Person vorzutäuschen, mit der das mögliche Opfer bereits kommuniziert hat. Sehr viele – auch IT-affine – Adressaten, bewerteten diesen Angriff als gezielt. Es handelte sich jedoch um ein Massenphänomen, bei dem der Empfänger dazu bewegt werden sollte, eine Makro-Ausführung im MS-Office-Dokument aus dem Anhang zu aktivieren. Die Makros luden üblicherweise die eigentliche Schadsoftware (*Emotet*) nach.

Zurzeit dominiert der Versand von RTF-Dateien, die eine im November 2017 von Microsoft geschlossene Schwachstelle im MS-Formeleditor (CVE-2017-11882) ausnutzen, um einen schädlichen Code zum Nachladen weiterer Schadsoftware auszuführen.

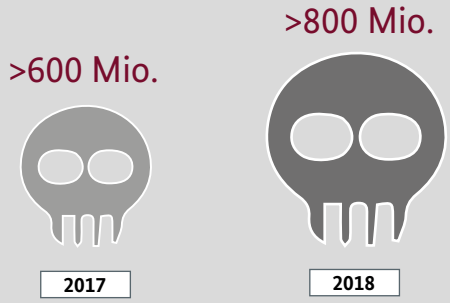
Das Jahr im Rückblick

Erkenntnisse aus dem BSI-Lagebericht 2018

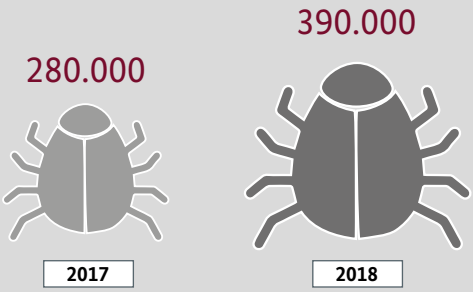
In seinem jährlichen Lagebericht gibt das BSI einen umfassenden Überblick über die IT-Sicherheit in Deutschland. Auf dieser Seite wurden einige Ergebnisse des Lageberichts 2018 zusammengefasst.

BEDROHUNGEN IM NETZ

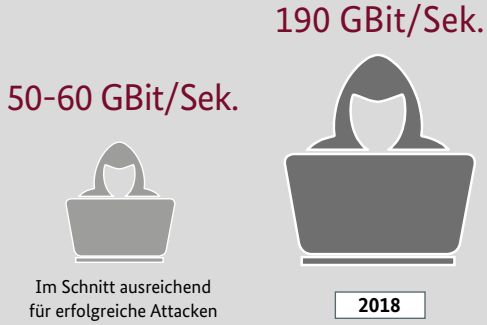
Schadprogramme im Umlauf



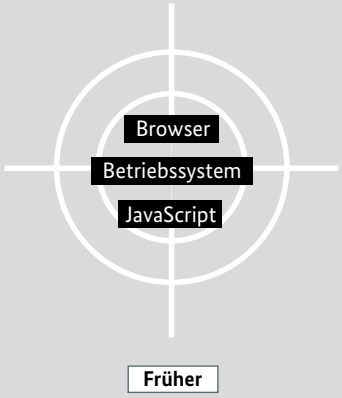
Neue Schadprogramm-Varianten pro Tag

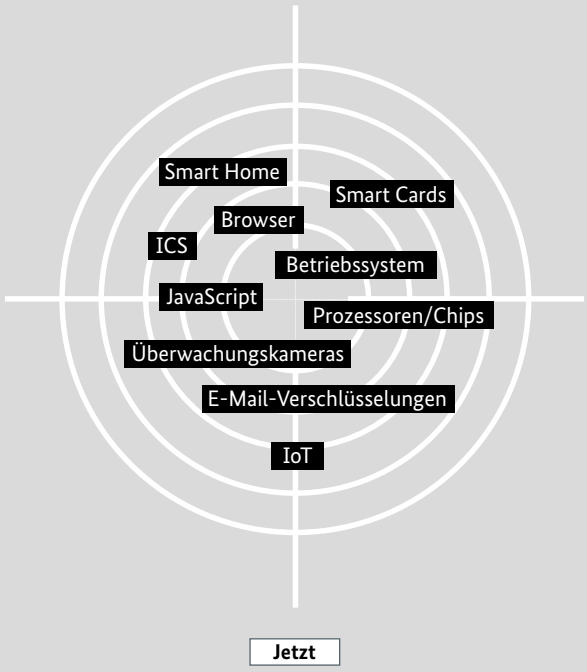


Geschwindigkeit der Angriffe



FOKUS DER ANGRIFFE WIRD BREITER



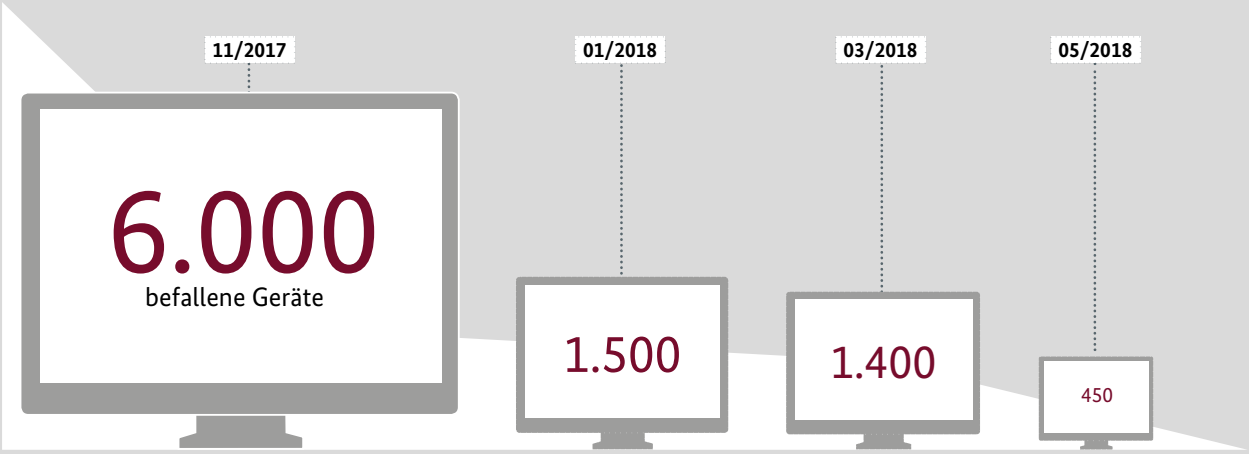


WARNUNGEN ZEIGEN WIRKUNG

Mehr als

16 Millionen Warn-Mails

hat das BSI verschickt, um auf Gefahrensituationen aufmerksam zu machen.



(Bsp: Cisco Smart Install; Die Zahl befallener Geräte sank von über 6.000 auf rund 450 nach regelmäßigen Warnungen durch das CERT-Bund des BSI an deutsche Netzbetreiber)

VERNETZTE ZUSAMMENARBEIT

Allianz für Cyber-Sicherheit

Mehr als

2.700 Institutionen

sind in der Allianz für Cyber-Sicherheit vernetzt, um das Niveau der Informationssicherheit im Unternehmen zu erhöhen und sich wirksam gegen Cyber-Bedrohungen zu schützen.

BSI FÜR BÜRGER
INS INTERNET - MIT SICHERHEIT

Mehr als

100.000 Bürger

lassen sich regelmäßig durch das BSI über Gefahren im Internet informieren.

2 Maßnahmen des BSI

2 Lösungen und Angebote des BSI

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 drei Aufgabenbereichen Staat/Verwaltung, Wirtschaft/Kritische Infrastrukturen und Gesellschaft/Bürger. Um diese Angebote praktisch nutzbar zu machen, wird über Links auf zahlreiche Publikationen und Internetangebote des BSI verwiesen.

2.1 Zielgruppe Staat und Verwaltung

Der Aufgabenbereich des BSI wird in Bezug auf die Zielgruppe Staat und Verwaltung durch das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) festgelegt. Das BSI ist für den Schutz der IT-Systeme des Bundes verantwortlich. Hierbei geht es um die Abwehr von Cyber-Angriffen und anderen technischen Bedrohungen gegen die IT-Systeme und Netze des Bundes.

Seit der Novellierung des BSI-Gesetzes 2009 ist das BSI zentrale Meldestelle für die IT-Sicherheit der Bundesbehörden. In dieser Funktion sammelt das BSI Informationen über Sicherheitslücken und neue Angriffsmuster auf die Sicherheit der Informationstechnik. Hierdurch können ein verlässliches Lagebild erstellt, Angriffe frühzeitig erkannt und Gegenmaßnahmen rechtzeitig ergriffen werden. Darüber hinaus ist das BSI befugt, Protokolldaten sowie Daten, die an den Schnittstellen der Kommunikationstechnik des Bundes anfallen, zu erheben, auszuwerten, zu speichern, zu verwenden und zu verarbeiten. Das BSI ist zudem befugt, einheitliche und angemessene Sicherheitsstandards für die Bundesverwaltung zu definieren und bei Bedarf als zentraler IT-Dienstleister des Bundes geeignete Produkte entwickeln zu lassen beziehungsweise auszuschreiben und bereitzustellen.

So kann verhindert werden, dass ungeeignete Produkte mit Schwachstellen oder manipulierte IT-Komponenten in der Bundesverwaltung und in den Regierungsnetzen zum Einsatz kommen. Das BSI berät andere Behörden und nach Maßgabe von § 3 Abs. 2 BSIG auch die Bundesländer. Es kann die Länder zudem umfassend unterstützen und ihnen seine technische Expertise zur Verfügung stellen.

Produkt- und Dienstleistungsportfolio

Um eine systematische Unterstützung seiner Zielgruppen Staat, Wirtschaft und Gesellschaft durch zielgerichtete Informationen, technische Produkte und Leistungen sicherzustellen, hat das BSI im Berichtszeitraum sein Leistungsangebot in einem Produkt- und Dienstleistungsportfolio zusammengestellt. Es richtet sich

- im Bereich Staat an den Bund, die Länder, die Kommunen und internationale Partner,
- im Bereich Wirtschaft an Betreiber Kritischer Infrastrukturen (KRITIS), IT-Hersteller und Dienstleister sowie Unternehmen aller Branchen und Größen und
- im Bereich Gesellschaft an politische Parteien und parteinahe Stiftungen sowie alle Bürgerinnen und Bürger.

Im Produkt- und Dienstleistungsportfolio wurden sechs Kategorien einheitlich festgelegt. Ausgehend von der Kategorie „Information“, die u. a. Standards wie den IT-Grundschutz, aber auch Lageberichte und Warnungen umfasst, nimmt der Bereitstellungsaufwand mit jeder Kategorie zu (siehe exemplarische Darstellung für die Zielgruppe Länder in Abbildung 16). Neben Aus- und Fortbildungsangeboten im Bereich IT-Sicherheit und Kooperationsplattformen, wie zum Beispiel der Allianz für Cyber-Sicherheit, bietet das BSI auch Beratungsleistungen zu verschiedenen Fragestellungen der Umsetzung von IT-Sicherheit an. Die Möglichkeit der Erbringung konkreter technischer Leistungen, wie die Unterstützung oder gar die Übernahme technischer Schutzmaßnahmen, kann das BSI, auch wenn die rechtlichen Voraussetzungen stimmen, aufgrund des hohen Ressourcenaufwands nur auf Anfrage prüfen.

Indem erprobte Verfahren zum Schutz vor Cyber-Angriffen (z. B. über eine Malware Sharing Information Plattform) bereitgestellt beziehungsweise Beratungsleistungen erbracht werden, können Doppelstrukturen, z. B. auf Landesebene, vermieden werden. Der Zugriff auf die Expertise des BSI wird über die klare Zusammenstellung im Portfolio erleichtert. Das Nationale Verbindungswesen berät die Zielgruppen Staat, Wirtschaft und Gesellschaft zu den einzelnen Produkten und Dienstleistungen des BSI und vermittelt den Bedarf in das BSI. So bildet das Portfolio beispielsweise die Basis für den Ausbau der Zusammenarbeit mit den Ländern.

Abbildung 16 BSI-Angebote für die Länder

2.1.1 CERT-Bund und nationales IT-Lagezentrum

Das Computer Emergency Response Team Bund (CERT-Bund) sammelt in seiner Rolle als nationales CERT sowohl aus eigenen Analysen als auch von Partnern und weiteren vertrauenswürdigen externen Quellen erhaltene Informationen zu Sicherheitsvorfällen in Bezug auf IT-Systeme in Deutschland. Dies umfasst unter anderem Informationen zu Schadprogramm-Infektionen, unzureichend abgesicherten Server-Diensten sowie kompromittierten Systemen bzw. Zugangsdaten. Täglich werden automatisiert mehrere Millionen derartiger Ereignisse ausgewertet und anhand der IP-Adressen betroffener Systeme den jeweils zuständigen Netzbetreibern zugeordnet. Die Netzbetreiber werden anschließend über die Auffälligkeiten in ihren Netzbereichen informiert und, falls es sich um einen Provider handelt, gebeten, die betroffenen Kunden entsprechend in Kenntnis zu setzen.

Das Nationale IT-Lagezentrum des BSI führt eine kontinuierliche Lagebeobachtung der IT-Sicherheit durch. Hierzu wird täglich eine Vielzahl von öffentlichen und nichtöffentlichen Quellen ausgewertet, von Fachmedien über Analysten-Blogs bis hin zu Informationen von IT-Herstellern. Dieses Vorgehen gewährleistet die zeitnahe Reaktion auf neu entdeckte Schwachstellen oder bekannt gewordene IT-Sicherheitsvorfälle. Ergänzt werden diese Erkenntnisse durch die Auswertung der Informationen unterschiedlicher Sensoren u. a. in den Regierungsnetzen sowie weiterführender Analysen. Das Nationale IT-Lagezentrum fungiert als zentrale Meldestelle für IT-Sicherheitsvorfälle u.a. in der Bundes- und Landesverwaltung sowie den Kritischen Infrastrukturen gemäß der gesetzlichen Regelungen der jüngeren Vergangenheit.

Bei schwerwiegenden IT-Lagen kann das Nationale IT-Lagezentrum zum IT-Krisenreaktionszentrum aufwachsen.

Übungen

Im BSI werden die erforderlichen Prozesse regelmäßig geübt – sowohl intern als auch im Rahmen einer Teilnahme an internationalen Cyber-Übungen wie der von ENISA ausgerichteten „Cyber Europe“. Der wesentliche Prozess in übergreifenden Übungen ist der Informationsaustausch, damit aus vielen Beiträgen zügig sowohl ein Überblick über die Lage als auch Hinweise zur Bewältigung gewonnen und weitergegeben werden können.

In verschiedenen Fortbildungsangeboten für Staat und Verwaltung wirbt das BSI kontinuierlich dafür, Übungen und Planbesprechungen durchzuführen, um interne Prozesse auf ihre Funktionsfähigkeit und Aktualität zu überprüfen. Stichworte hierfür sind etwa Notfallmanagement, Business Continuity Management (BCM) und Krisenmanagement.

Für einfache kleinere Übungen hat das BSI Mustervorlagen für IT-Notfall-Übungen erstellt, die z. B. der Bundesverwaltung, aber auch den Mitgliedern der Allianz für Cyber-Sicherheit zur Verfügung stehen. Ausgehend von solchen Mustern können Organisationen oder auch Organisationseinheiten eigene Übungen entwickeln, um etwa die Prozesse im eigenen Notfallmanagement zu überprüfen und zu testen.

Der Übergang vom Notfallmanagement bei Vorfällen im IT-Betrieb oder bei erfolgreichen Cyber-Angriffen mit geringen bis mittleren Auswirkungen zum Krisenmanagement bei schwerwiegenden Auswirkungen nach IT-Vorfällen oder Cyber-Angriffen stellt eine besondere

Herausforderung dar. Als die Schadsoftware *WannaCry* 2017 weltweit Schaden anrichtete, konnten viele Betroffene nicht nur auf vorbereitete IT-Notfall- und BCM-Maßnahmen, sondern auch auf Erfahrungen aus Krisenmanagement-Übungen zurückgreifen. Dabei ist neben etablierten internen Prozessen auch der organisationsübergreifende Informationsaustausch relevant.

2.1.2 Cyber-Abwehrzentrum

Das Nationale Cyber-Abwehrzentrum (Cyber-AZ) wird unter Federführung des BSI auf Basis von Verwaltungsvereinbarungen zwischen den beteiligten Behörden betrieben. Das BSI stellt den Leiter, die Geschäftsstelle samt Personal und die Räumlichkeiten für seine eigenen Mitarbeiter und die Verbindungsbeamten der anderen beteiligten Behörden. Durch kurze Wege zwischen dem Cyber-AZ und dem Nationalen IT-Lagezentrum/IT-Krisenreaktionszentrum, dem CERT-Bund und dem mobilen Einsatzteam des BSI (MIRT) ist eine effiziente Zusammenarbeit auch in Krisensituationen sichergestellt.

Die Arbeit des Cyber-Abwehrzentrums erstreckt sich neben dem Austausch cyber-relevanter Informationen insbesondere darauf, die Bearbeitung von Cyber-Vorfällen in Deutschland zu koordinieren und die operativen Maßnahmen der zuständigen Behörden abzustimmen. In Umsetzung des Koalitionsvertrags wird die Zusammenarbeit von Bund und Ländern bei der Cyberabwehr in Zukunft ausgebaut, verbessert und strukturell neu geordnet. Die Fallbearbeitung wird von den beteiligten Behörden im Rahmen ihrer jeweiligen Aufgaben und Befugnisse durch deren zuständige Fachreferate übernommen. Dabei werden die Ergebnisse kontinuierlich im Cyber-AZ zusammengeführt, bewertet und an die entsprechenden Stellen berichtet. Insofern kann das Cyber-AZ die personellen Ressourcen aller beteiligten Behörden soweit erforderlich einbinden. Die hierfür zur Verfügung stehenden Ressourcen wurden im vergangenen Jahr bei allen Cyber-AZ-Behörden verstärkt.

Einer der im Berichtszeitraum bekannt gewordenen herausragenden Fälle war der Cyber-Angriff auf das Auswärtige Amt. An der im Cyber-AZ unverzüglich eingerichteten Arbeitsgruppe waren mehrere Behörden beteiligt, die erhebliche Personalressourcen in die Vorfallsaufklärung investierten. Beim BSI alleine beliefen sich diese auf etwa 75 Personenmonate. Ein weiterer großer Fall war die durch die „*NotPetya*"-Schadsoftware verursachte weltweite Beeinträchtigung der IT-Systeme von Unternehmen. Darüber hinaus bearbeitete das Cyber-AZ im Berichtszeitraum eine Vielzahl nicht öffentlich bekannt gewordener Vorfälle.

2.1.3 Detektion

Neben der Prävention und der Reaktion ist die Detektion der entscheidende Baustein, um Cyberangriffen frühzeitig begegnen zu können und das Schadensausmaß zu minimieren. Somit lässt sich die Detektion als Qualitätssicherung der Prävention begreifen, die feststellt, an welchen Stellen tatsächlich versucht wird, präventive Maßnahmen zu umgehen. Durch ihre Tatsachenorientierung grenzt sich die Detektion von der Schwachstellenerkennung oder den Penetrationstests ab, kann allerdings immer nur rückwärts gerichtet nach einem Angriff bzw. während eines Angriffs wirken.

Im Berichtszeitraum wurde mit Hilfe der gem. § 5 BSIG möglichen Detektionsmöglichkeiten eine Vielzahl von Angriffen auf die Bundesverwaltung erfolgreich erkannt und abgewehrt. Sowohl die dezentralen als auch die zentralen Detektionskomponenten des BSI nutzen dabei u. a. statistische Analysen und Methoden des Maschinellen Lernens zur Erkennung bislang unbekannter Angriffe.

Um die Detektion von Angriffen zukünftig noch wirksamer zu gestalten, wurde ein Mindeststandard für die Protokollierung und Detektion erstellt. Besonderer Schwerpunkt war hierbei die Berücksichtigung der Anforderungen des Datenschutzes und Fernmeldegeheimnisses bei gleichbleibend hohem Detektionsniveau. Flankiert wurde die Ausarbeitung des Standards durch den Aufbau einer Referenzarchitektur.

Basierend auf diesem Mindeststandard kann das BSI die effiziente Detektion von Angriffen weiteren Behörden als Dienstleistung anbieten.

2.1.4 Lauschabwehr

Das BSI stellt abhörgefährdeten Behörden des Bundes und der Länder Lauschabwehrkonzepte und -dienstleistungen zur Verfügung. Dazu gehören die Herausgabe von Technischen Leitlinien, Beratungen bei Neu- und Umbaumaßnahmen sowie die Durchführung von Erst- und Wiederholungs-Lauschabwehrprüfungen. Darüber hinaus werden aber auch Konferenzen und bilaterale Treffen auf höherer Ebene betreut, bei denen die Gespräche ganz oder teilweise vertraulich bleiben sollen.

Dabei stellen die Lauschabwehr-Prüftrupps sicher, dass keine Abhörgeräte vorhanden sind und dass auch auf anderen Wegen, beispielsweise über manipulierte oder versehentlich aktivierte Mobiltelefone, keine Gesprächsinformationen an Unbefugte gelangen.

2.1.5 Ausbau der Zusammenarbeit zwischen Bund und Ländern

In der Cyber-Sicherheitsstrategie für Deutschland 2016 wurde die Stärkung der Bund-Länder-Zusammenarbeit im Bereich der Cyber-Sicherheit festgelegt. Die rechtliche Grundlage hierfür bildet § 3 Abs. 2 BSIG, nach dem das BSI die Länder in Fragen der Informationssicherheit beraten und warnen sowie auf deren Ersuchen bei der Sicherung ihrer Informationstechnik und Abwehr von Gefahren unterstützen kann. Um die Zusammenarbeit mit den Ländern zu verstärken, hat das BSI im Berichtszeitraum die relevanten Strukturen und Ressourcen weiterentwickelt. Von zentraler Bedeutung waren in diesem Zusammenhang die Erarbeitung des Produkt- und Dienstleistungsportfolios für die Zielgruppe Länder, die Verstärkung der Informationssicherheitsberatung und der Ausbau des Verbindungswesens. Auch im VerwaltungsCERT-Verbund hat das BSI sein Engagement stetig ausgebaut und unterstützt beispielsweise die Einrichtung und Nutzung von MISP (Malware Information Sharing Platform) zum Austausch von Gefährdungsindikatoren in den Ländern.

Übergeordnetes Ziel einer besseren Zusammenarbeit ist die Schaffung eines einheitlichen IT-Sicherheitsniveaus, das angesichts der fortschreitenden Digitalisierung der Verwaltung und einer zunehmenden Vernetzung von IT-Strukturen zwischen Bund und Ländern stetig an Bedeutung gewinnt. Die Sicherheitsberatung und das Verbindungswesen gestalten dabei gemeinsam den Ausbau der Zusammenarbeit des BSI mit den Ländern.

Im Berichtszeitraum hat das BSI den Bedarf der Länder nach Unterstützungsleistungen des BSI durch intensive bilaterale Gespräche und gezielte Bedarfsabfragen erhoben. Im Rahmen von Sondierungsgesprächen wird seit Mitte 2017 der individuelle Kooperations- und Unterstützungsbedarf der Länder erfasst und es werden Modelle für die Umsetzung diskutiert. Ziel der Gespräche sind konkrete Vereinbarungen zur Stärkung der Zusammenarbeit. Auf dieser Basis erfolgt der jeweilige Ausbau der Zusammenarbeit. Ein erster Schritt ist in diesem Zusammenhang die Unterzeichnung von Absichtserklärungen, in denen Kooperations- und Unterstützungsfelder festgelegt sind. Mit den Ländern Hessen, Nordrhein-Westfalen und Rheinland-Pfalz hat das BSI im Berichtszeitraum derartige Modellpartnerschaften initiiert.

Eine Weiterentwicklung dieser Kooperation in Form von Verwaltungsvereinbarungen ist in Vorbereitung. Diese Kooperationsangebote bietet das BSI allen Bundesländern gleichermaßen an, wobei die Schwerpunkte und Unterstützungsleistungen individuell und bedarfsgerecht angepasst werden. Auf diese Weise wird der Auf- und Ausbau von Strukturen zur Stärkung der IT-Sicherheit in den Ländern durch die vorhandene Expertise des BSI gezielt unterstützt.

Im Umfeld der Zusammenarbeit mit den Ländern existieren im BSI Strukturen auf unterschiedlichen Ebenen:

- Die Sicherheitsberatung des BSI stellt die zentrale Anlaufstelle für Beratungsanfragen aus den Bundes- und Landesverwaltungen im Kontext des Informationssicherheitsmanagements dar. Sie ist der zentrale Point-of-Contact für die Informationssicherheitsbeauftragten der jeweiligen Behörden. Die Mitarbeiter des Bereichs Sicherheitsberatung erhalten durch Gremienarbeit, enge Behördenkontakte und über einen effizienten Austausch von IT-sicherheitsrelevanten Informationen einen guten Einblick in die Lage der Informationssicherheit „vor Ort“. Die Sicherheitsberatung unterstützt die Informationssicherheitsbeauftragten der Behörden bei der Umsetzung eines ISMS und der Findung ausgewogener Lösungsansätze in Fragen der Informationssicherheit.

- Das Verbindungswesen des BSI gestaltet die Beziehungen des BSI zu nationalen Partnern in den Bereichen Staat, Wirtschaft und Gesellschaft und damit insbesondere auch zu den Bundesländern. Ein besonderes Merkmal des Verbindungswesens ist die regelmäßige regionale Präsenz in ausgewählten Regionen Deutschlands. Dadurch wird der unmittelbare Austausch erleichtert und eine konkrete Erreichbarkeit des BSI vor Ort geschaffen – zum Nutzen der Kunden und Partner in allen Teilen Deutschlands. Der Ausbau der Kooperation mit den relevanten Ansprechpartnern in den Bundesländern ist ein wichtiger Tätigkeitsschwerpunkt der Verbindungspersonen des BSI. Regelmäßige Treffen, die Teilnahme an Veranstaltungen vor Ort sowie Vortragstätigkeiten gehören hierbei zum Angebotsspektrum des Verbindungswesens in den Bundesländern. So konnte im Berichtszeitraum die Präsenz des BSI bei regionalen Veranstaltungen deutlich erhöht werden.

- Die operative Zusammenarbeit mit den Ländern ist über den VerwaltungsCERT-Verbund (VCV) etabliert. Über den VCV sollen die CERTs des Bundes und der Länder Informationen austauschen, um effektiver und schneller auf IT-Angriffe reagieren zu können. Der IT-Planungsrat hat 2018 ein verbindliches Meldeverfahren zum Informationsaustausch über Cyber-Angriffe beschlossen und somit eine Meldeverpflichtung zwischen Bund und Ländern geschaffen. Das BSI stellt über CERT-Bund Warnungen, Lageberichte sowie Gefährdungsindikatoren bereit, die sich aus den unterschiedlichsten im BSI-Lagezentrum verarbeiteten Quellen speisen. Die Länder leisten durch Beiträge zum Lagebild und Vorfallsmeldungen ihren Beitrag, der für ein ganzheitliches Bild von elementarer Bedeutung ist. Die gegenseitige Meldeverpflichtung bildet hierfür die Basis.

Auch die Kommunen werden bei der Stärkung der Bund-Länder-Zusammenarbeit mit einbezogen. Aufgrund der hohen Anzahl an Kommunen müssen dabei zwingend Multiplikatoren zur Bündelung der Aktivitäten eingebunden werden. Das BSI ermöglicht zudem eine direkte Anbindung aller Kommunen an die Allianz für Cyber-Sicherheit.

2.1.6 Umsetzungsplan Bund 2017

Der Umsetzungsplan Bund 2017 ist die Leitlinie für Informationssicherheit in der Bundesverwaltung (UP Bund 2017). Die Umsetzung der darin enthaltenen Anforderungen und Maßnahmen gewährleistet die Informationssicherheit in der Bundesverwaltung. Mit dem UP Bund 2017 wurde der ursprünglich aus dem Jahr 2007 stammende Umsetzungsplan neu gefasst und vom Bundeskabinett in seiner Sitzung am 19. Juli 2017 beschlossen. Der UP Bund 2017 trat am 1. September 2017 in Kraft und setzt Ziele aus der Cyber-Sicherheitsstrategie 2016 in verschiedenen Handlungsfeldern um. Er ist für alle Ressorts und Bundesbehörden verbindlich. Bei einer wachsenden Abhängigkeit von IT und einer wachsenden Verwundbarkeit der digitalen Infrastruktur der Bundesverwaltung kommt es ganz wesentlich auf ein funktionierendes Informationssicherheitsmanagement und das systematische Erreichen der Schutzziele der Informationssicherheit in der Bundesverwaltung an. Mit dem UP Bund 2017 wurden hierfür die Voraussetzungen geschaffen.

2.1.7 Informationssicherheitsberatung

Die Unterstützung und Beratung zum Aufbau von Informationssicherheits-Managementsystemen (ISMS) ist eine der wesentlichen Kernaufgaben der Informationssicherheitsberatung des BSI. Im Berichtszeitraum wurden die Zielgruppen für diese Dienstleistungen erweitert.

So hat das BSI während der Bundestagswahl 2017 Parteien und parteinahe Stiftungen beraten. Dies soll als dauerhaftes Angebot fortgeführt werden, da auch bei zukünftigen Wahlen die Sicherheit der beteiligten IT-Systeme eine wesentliche Rolle spielen wird.

Im Jahr 2017 wurden außerdem die Planungen für einen Ausbau der Beratung von Bundesländern und Kommunen begonnen. Dafür wurden die BSI-Standards 200-1 und 200-2 auf ihre praxisgerechte Anwendbarkeit geprüft. Der neue Leitfaden des BSI zur Basis-Absicherung nach IT-Grundschutz stellt insbesondere auch für den landesspezifischen und kommunalen Bereich eine überaus geeignete und schnell umsetzbare Einführung in die Informationssicherheit dar.

Die individuelle Beratung der Ressorts und Behörden sowie weiterer Einrichtungen des Bundes hat an Bedeutung zugenommen. Die Modernisierung des IT-Grundschutzes, die Umsetzung des neu konzipierten UP Bund 2017 und die IT-Konsolidierung stellen wichtige Beratungsfelder dar. Hinzu kommen Projekte, in denen das BSI zu Fragen der Informationssicherheit berät.

So werden beispielsweise, um dem Bedarf einer besseren Steuerung von ISMS nachzukommen, durch die Sicherheitsberatung unter anderem Reifegradmodelle untersucht. Damit können die Stärken und Schwächen sowie der Handlungsbedarf in ISMS genauer identifiziert und besser dargestellt werden.

Außerdem erstellt die Sicherheitsberatung kurzgefasste themenspezifische Informationen, zum Beispiel zu sicheren Messenger-Diensten, und bedient damit Nachfragen zu sicherheitsrelevanten Themen. Ziel ist es hierbei, den Sachverhalt möglichst konzentriert auf zwei Seiten im Sinne einer Orientierungshilfe kurz und verständlich darzustellen und ggf. auf wichtige weiterführende Dokumente zu verweisen.

Auf der Grundlage des UP Bund 2017 arbeitet das BSI mit der Bundesakademie für öffentliche Verwaltung (BAköV) zusammen, um eine inhaltlich aktuell ausgerichtete Fortbildung für IT-Sicherheitsbeauftragte der öffentlichen Verwaltung zu gewährleisten.

2.1.8 IT-Konsolidierung des Bundes

Im Großprojekt IT-Konsolidierung des Bundes führt die Bundesregierung ihre Informationstechnik durch die Handlungsstränge Betriebskonsolidierung, Dienstekonsolidierung und Beschaffungsbündelung bei einem Leistungsverbund von IT-Dienstleistern zusammen. Dadurch verändert sich die IT-Landschaft der Bundesverwaltung in erheblichem Maße, verbunden mit neuen Chancen, aber auch neuen Risiken. Beispielsweise können entstehende Skaleneffekte für eine Professionalisierung der IT-Prozesse genutzt werden. Jedoch ergeben sich bei einer Konzentration von IT-Systemen auf IT-Dienstleister auch potenzielle IT-Risikokonzentrationen bei den IT-Dienstleistern.

Das BSI berät die Gesamtprojektleitung der IT-Konsolidierung des Bundes regelmäßig und intensiv zu strategischen und operativen Fragen der Informationssicherheit in der IT-Konsolidierung. Besonders intensiv wirkt das BSI durch Beratung in mehreren Maßnahmen des Teilprojekts 6 „Gemeinsame IT des Bundes“ mit, beispielsweise bei den Maßnahmen Bundescloud und Bundesclient, und engagiert sich auch im Lenkungsausschuss dieses Teilprojektes.

Darüber hinaus berät das BSI Gremien der IT-Dienstleister des Bundes zu Fragen der Informationssicherheit.

Weiterhin führt das BSI für den Haushaltsausschuss des Deutschen Bundestags die Untersuchung sämtlicher Rechenzentren der Bundesverwaltung auf Basis des „HVBenchmark kompakt“ fort. In Ergänzung zu den Ergebnissen der vorherigen Teilprüfungen konnten neue Erkenntnisse gewonnen werden, was die Wirkung verschiedener Einzelmaßnahmen beim Informationssicherheitsmanagement von Rechenzentren betrifft. Damit zeigte sich die Untersuchung auf Basis des „HVBenchmark kompakt“ als effektives Werkzeug für eine kontinuierliche Verbesserung der Rechenzentrumssicherheit.

2.1.9 Dienstleistungen und Maßnahmen zur Absicherung während der Bundestagswahl 2017

Das BSI hat bei der Bundestagswahl im September 2017 den Bundeswahlleiter in Fragen der Informationssicherheit unterstützt. Hierfür wurden die Gefährdungslage und der bestehende Schutzbedarf erörtert sowie die zentrale Sicherheitskonzeption fachlich analysiert. Ergänzend fanden begleitende Penetrationstests statt. Darüber hinaus hat das BSI punktuell Landeswahlleiter zu Aspekten der Informationssicherheit ihrer IT-bezogenen Aufgaben während der Bundestagswahl beraten.

Das BSI hat zur Absicherung der Bundestagswahl ein auf die Cyber-Sicherheit ausgerichtetes Dienstleistungsangebot geschaffen und mit den entsprechenden personellen Ressourcen hinterlegt. Eckpunkte dieses Dienstleistungsangebots umfassen:

- Beratung von Parteien und parteinahen Stiftungen zum Aufbau von Managementsystemen für Informationssicherheit (ISMS),
- Unterstützung bei der Erstellung verifizierter Accounts bei Twitter und Facebook,
- Digitaler Persönlichkeitsschutz in Form eines Informations- und Beratungsangebots für Spitzenpolitiker,
- Durchführung von Penetrationstests und Webchecks sowie
- Untersuchung von Social Bots.

Während des relevanten Zeitraums vor der Bundestagswahl hat das BSI eine Vielzahl von Aktivitäten durchgeführt, von denen einige hier genannt werden:

- Fokussierte Lagebeobachtung hinsichtlich der Bundestagswahl,
- 24/7-Betrieb des Nationalen IT-Lagezentrums in der kritischen Phase der Wahldurchführung,
- Beratung des Bundeswahlleiter und der Landeswahlleiter in Fragen der Informationssicherheit,
- Beratung nahezu aller im Bundestag vertretenen Parteien,
- Bearbeitung von mehr als 700 Anträgen zur Verifizierung von Social-Media-Accounts.

Zusammenfassend ist festzustellen, dass das BSI eine Reihe relevanter Ereignisse im Zusammenhang mit der Bundestagswahl erfasst und geprüft hat. Im Hinblick auf Cyber-Angriffe auf die Bundestagswahl konnte kein Einfluss auf die Bundestagswahl festgestellt werden.

2.1.10 Mindeststandards

Das BSI erarbeitet nach § 8 BSIG Mindeststandards für die Sicherheit der Informationstechnik des Bundes. Gemäß der Leitlinie für Informationssicherheit in der Bundesverwaltung (Umsetzungsplan Bund 2017) sind diese Mindeststandards innerhalb der Bundesverwaltung zur Gewährleistung der Informationssicherheit zu beachten. Um eine hohe Qualität der Standards sicherzustellen, werden Mindeststandards nach einer standardisierten Vorgehensweise erarbeitet: Jeder Mindeststandard durchläuft mehrere Prüfungszyklen einschließlich eines Konsultationsverfahrens mit der Bundesverwaltung. Über die aktive Beteiligung bei der Erarbeitung von Mindeststandards hinaus kann sich die Bundesverwaltung auch bei der Erschließung fachlicher Themenfelder für neue Mindeststandards einbringen oder im Hinblick auf einen Änderungsbedarf bei bestehenden Mindeststandards Kontakt mit dem BSI aufnehmen. Einhergehend mit der Erarbeitung berät das BSI die Bundesverwaltung auf Ersuchen bei der Umsetzung und Einhaltung der Mindeststandards.

Die bereits veröffentlichten Mindeststandards decken ein breites Spektrum der Informationstechnik ab:

- Einsatz des SSL/TLS-Protokolls,
- sichere Web-Browser,
- externe Cloud-Dienste,
- Mobile Device Management,
- Anwendung des HV-Benchmark kompakt,

- Schnittstellenkontrolle.

Weitere Mindeststandards aus den Themenbereichen ‚Protokollierung und Detektion von Cyber-Angriffen', ‚IT-Grundschutz Bund' und ‚Nutzerpflichten Netze des Bundes' werden derzeit erarbeitet.

Die Mindeststandards helfen konkret, IT sicher zu betreiben. So hatte z. B. der im Dezember 2017 entdeckte ROBOT-Angriff, mit dem Schwachstellen in TLS-Implementierungen ausgenutzt werden sollten, keine Auswirkungen auf Institutionen, die den Mindeststandard ‚Einsatz des SSL/TLS-Protokolls' bereits umgesetzt hatten. Durch die vom Mindeststandard vorgegebene sichere Konfiguration des TLS-Protokolls konnte der Angriff vollständig verhindert werden.

2.1.11 Sichere Mobilkommunikation in der Bundesverwaltung

Die Mobilkommunikation hat in den letzten Jahren eine enorme Entwicklung durchlaufen. Technische Innovationen und die zunehmende Leistungsstärke mobiler Systeme machen es möglich, unabhängig von Zeit und Ort zu kommunizieren und zu arbeiten. Die Nutzung mobiler Geräte stellt die Bundesverwaltung vor diverse Herausforderungen. Ihre Bereitstellung muss den Anforderungen an die Geschäftsprozesse genauso Rechnung tragen wie denen an die Sicherheit der Regierungs- und Behördennetze.

Zur Verarbeitung und Übertragung von Verschlusssachen bis zum Geheimhaltungsgrad VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) hat das BSI zusammen mit Herstellern von Sicherheitsprodukten für die Bundesverwaltung verschiedene sichere mobile Lösungen entwickelt und zugelassen. So bietet der Hersteller Secusmart, der bereits die Lösung SecuSUITE for BlackBerry 10 entwickelt hat, mit SecuSUITE for Samsung Knox sichere Smartphones und Tablets auf Basis moderner Samsung-Geräte mit dem Betriebssystem Android an. Im Apple-iOS-Umfeld steht Behörden seit dem Ende des ersten Quartals 2018 mit dem Produkt SecurePIM Government SDS des Herstellers Virtual Solution eine sichere mobile Lösung zur Datenübertragung für die aktuelle Produktpalette von iPhones und iPads zur Verfügung.

SecurePIM Government SDS

In Zusammenarbeit mit dem BSI wurde die Lösung SecurePIM Government SDS für die sichere Verarbeitung von VS-NfD-eingestuften Daten mit iPhones und iPads entwickelt. SecurePIM Government SDS synchronisiert E-Mail, Adressbuch, Notizen, Aufgaben, Kalender und Dokumente aus dem internen Netzwerk einer Behörde auf dienstlich genutzte iPhones oder iPads und ermöglicht den sicheren mobilen Zugriff auf das Intranet von Behörden. Die Lösung verwendet als Sicherheitsanker eine Chipkarte, die über Smartcard-Reader an iOS-Geräte gekoppelt wird.

Studie zur sicheren Telefonie mit iOS-basierten Endgeräten

Eine zentrale Anforderung an sichere mobile Lösungen ist die sichere Sprachübertragung. Die technischen Möglichkeiten und Aufwände zur Implementierung einer solchen sicheren Telefonie mit dem Schutzniveau VS-NfD auf iOS-Geräten wurde 2017 in der „Studie zur Implementierung sicherer Telefonie unter iOS" untersucht. Es wurde ein Grobkonzept für die Implementierung von SNS erarbeitet, an dessen Umsetzung der Hersteller nun arbeitet.

2.1.12 Sichere Identitäten im E-Government

Im Rahmen der Digitalisierung von Prozessen kommt der Vertrauenswürdigkeit von Identitäten in der digitalen Welt eine besondere Bedeutung zu: Dort, wo Menschen nicht mehr persönlich auftreten, muss ihre Identität auf anderem Wege verlässlich sichergestellt werden können. Das BSI befasst sich daher mit der sicheren Umsetzung von Identifizierungs- und Authentisierungsverfahren, insbesondere auch im E-Government.

Der Koalitionsvertrag sieht vor, ein digitales „Bürgerportal" für Bürgerinnen und Bürger sowie Unternehmen zu schaffen, in dem zentrale und dezentrale Verwaltungsportale miteinander vernetzt werden sollen. Dieses Bürgerportal (im Online-Zugangs-Gesetz auch als Portalverbund von Bund und Ländern beschrieben) soll bis Ende 2022 die Portale des Bundes und aller Länder intelligent verknüpfen und Online-Verwaltungsleistungen leichter auffindbar machen.

Der Portalverbund ist eines von drei Teilprojekten des Vorhabens „Verwaltungsportale aller Ebenen intelligent verknüpft" des IT-Planungsrates.

Die weiteren Teilprojekte sind das Bundesportal und das Bürgerkonto (bzw. heute Service- oder Nutzerkonto).

Bund und Länder stellen im Portalverbund jeweils Nutzerkonten bereit, über die sich Nutzer für die im Portalverbund verfügbaren elektronischen Verwaltungsleistungen von Bund und Ländern einheitlich identifizieren können. Da beide schon zum Teil über Nutzer- bzw. Servicekonten verfügten, hat der IT-Planungsrat beschlossen, kein standardisiertes Bundes-Servicekonto bereitzustellen, sondern stattdessen einen Föderationsverbund „Interoperable Ser-

vicekonten“ einzurichten, damit Bürgerinnen, Bürger und Unternehmen nur über ein einziges Servicekonto verfügen müssen, um sich auch für die Verwaltungsleistungen der übrigen Föderationsteilnehmer identifizieren zu können.

Im Bereich der Interoperablen Servicekonten unterstützt das BSI die vom IT-Planungsrat eingesetzte Projektgruppe “eID-Strategie“ und wird im Ergebnis der Pilotierungsphase eine Technische Richtlinie zu diesem Thema erarbeiten.

Im Kontext des Onlinezugangsgesetzes (OZG) werden für den Pilotbetrieb des Portalverbundes/Online-Gateways derzeit Sicherheitsanforderungen erstellt und mit den am Piloten teilnehmenden Stellen abgestimmt.

2.1.13 Smart Borders und hoheitliches Identitätsmanagement

Ende 2017 ist auf europäischer Ebene die Verordnung über ein einheitliches Europäisches Ein-/Ausreisesystem (entry/exit system, EES) in Kraft getreten. Das Gesamtsystem besteht aus einem zentralen europäischen Register, einem Biometrie-Hintergrundsystem für über 100 Millionen Reisende und der Integration in die nationalen Grenzkontroll- und anderen Sicherheitssysteme der Schengen-Staaten.

Im Rahmen von EES wird jeder Grenzübertritt eines Drittstaatenangehörigen über eine der Schengen-Außengrenzen in einem europäischen Register für drei Jahre, in Ausnahmefällen für bis zu fünf Jahre, gespeichert. Hierbei werden nicht nur die biographischen Daten abgelegt, sondern auch ein biometrisches Lichtbild und vier Fingerabdrücke. Dadurch wird eine deutlich bessere Identifikation der Reisenden ermöglicht, da Mehrfachidentitäten durch den biometrischen Abgleich aufgedeckt werden können. Overstayer, d.h. Reisende, die ihre berechtigte Aufenthaltsdauer überschritten haben, können so leicht ermittelt und bei Kontrollen erkannt werden.

Weiterhin wird derzeit der Rechtsrahmen für das neue „European Travel Information and Authorisation System“ (ETIAS) geschaffen. Es ist als Vorregistrierungssystem für visumsbefreite Reisende ähnlich dem US-amerikanischen ESTA-System gedacht. Die neuen Systeme in Verbindung mit existierenden Systemen wie dem Visa-Informationssystem (VIS) und dem europäischen Asylsystem (EURODAC) ermöglichen eine sichere Identitätsfeststellung von Personen, selbst wenn diese über keine Dokumente mehr verfügen. Das BSI gestaltet damit wichtige Bausteine im europäischen System der Migrationskontrolle entscheidend mit.

Die Digitalisierung der europäischen Grenzkontrollarchitektur rückt die Anforderungen an Funktionalität und IT-Sicherheit der neuen Systeme in den Fokus. In Zukunft werden die meisten Schritte der Grenzkontrolle im Self-Service automatisiert ablaufen. Technische Systeme werden Grenzübertrittsentscheidungen vorbereiten, wobei die Verantwortlichen ein hohes Maß an Zuverlässigkeit von diesen Systemen erwarten.

In der nationalen Umsetzung ist das BSI gemeinsam mit den Partnerbehörden Bundesverwaltungsamt und Bundespolizei mit der nationalen Umsetzung des EES und zukünftig des ETIAS beauftragt. Das BSI sorgt mit seinen technischen Vorgaben dafür, dass sowohl die Dokumentenprüfung der optischen und elektronischen Sicherheitsmerkmale als auch die biometrischen Verfahren stets auf dem aktuellen Stand der Technik sind. In enger Abstimmung mit der Bundespolizei prüft das BSI die Grenzkontrollsysteme auf Schwachstellen und betreibt auch die notwendige Hintergrund-Infrastruktur im Rahmen des Nationalen Public Key Directory.

Das BSI leistet hiermit einen wichtigen Beitrag zum hoheitlichen Identitätsmanagement im Grenzkontrollprozess. Die Sicherstellung eines hohen Sicherheitsniveaus ist ein zentrales Anliegen der Bundesregierung und schreibt das Konzept von Schengen fort: ein einheitliches und verlässliches System der Kontrolle gemeinsamer Außengrenzen.

2.1.14 Abstrahlsicherheit

In Erfüllung der NATO- und EU-Verträge kommt dem BSI die Rolle der „National TEMPEST Authority“ (NTA) zu. TEMPEST ist ein Sammelbegriff für alle elektromagnetischen Effekte, die als Begleiterscheinung jeder elektrischen und elektronischen Datenverarbeitung auftreten. Eine solche kompromittierende Abstrahlung kann unter geeigneten Rahmenbedingungen zur Rekonstruktion der verarbeiteten Informationen missbraucht werden.

In der Rolle als NTA ist das BSI hoheitlich zuständig, um Abwehrmaßnahmen gegen die Ausnutzung kompromittierender Abstrahlung bei der Verarbeitung, Übertragung und Speicherung von Verschlusssachen (VS) zu entwickeln, umzusetzen und zu kontrollieren. Dabei kommen Sicherheitsvorgaben und Messverfahren zum Einsatz, die auf den Schutzbedarf der Information und die Einsatzumgebung

bei ihrer Verarbeitung abgestimmt sind. Die höchste Sicherheitsstufe für Hardware, als „Level A“ bezeichnet, setzt die international abgestimmten TEMPEST-Vorgaben direkt in Form von aufwändigen Analyseverfahren um. Für die VS-Verarbeitung in Einsatzumgebungen, die ein bestimmtes Sicherheitsniveau aufweisen, wurde im BSI das Nationale Zonenmodell entwickelt. Dabei wird ein Teil der Sicherheitsanforderungen an VS-verarbeitende Geräte in die Einsatzumgebung verlagert. Dies ermöglicht den Einsatz von Prüfverfahren, die für die Serienproduktion von VS-verarbeitender Hardware optimiert sind. Das Vorgehen besteht aus Musterzulassungen von Gerätesätzen mit anschließender Produktion baugleicher Hardware, wobei eine Testabdeckung von 100% besteht. Im Berichtszeitraum wurden mit diesen Verfahren zehn TEMPEST-Zulassungen für Level-A-Geräte und 549 TEMPEST-Zulassungen für Geräte gemäß Nationalem Zonenmodell ausgesprochen.

Angriffe auf E-Pässe

Sachverhalt
Ende 2017 wurde von einem Forscherteam der als ROCA (Return of the Coppersmith Attac) bekannt gewordene Angriff publiziert. Der Angriff zielt auf RSA-Schlüssel ab, die auf Smartcards von Infineon generiert wurden. Anhand des öffentlichen Schlüssels kann mit einigem Rechenaufwand der private RSA-Schlüssel rekonstruiert werden.

Das RSA-Verfahren bildet die Grundlage für zahlreiche Anwendungen, jedoch sind die Auswirkungen von ROCA bisher überschaubar. Hauptsächlich sind von ROCA-Signaturkarten eine Reihe ausländischer ID-Karten betroffen. Im Rahmen der möglichen Notifizierung solcher ID-Karten nach der EU-eIDAS Verordnung zur Anerkennung von elektronischen Identitäten wird die Mitigation von ROCA bei den betroffenen Ländern eine wesentliche Rolle spielen. Auch die elektronischen Signaturen von Reisepässen einiger Staaten (Document-Signer-Schlüssel) basieren auf RSA und können betroffen sein. Mithilfe dieser Signatur wird die Unverfälschtheit der auf dem E-Pass gespeicherten Daten garantiert und ist daher wesentlich kritischer zu betrachten. Deutsche Reisedokumente sind von ROCA nicht betroffen, da hier Signaturen auf Basis von elliptischen Kurven eingesetzt werden.

Ursache/Schadenswirkung
Bei einer Überprüfung aller RSA-basierten Document-Signer-Schlüssel anderer Staaten durch das BSI (im Sinne des §3, Abs. (1), Satz 13(a) BSIG) konnten zwei Probleme identifiziert werden:

- Malaysia verwendet seit 2016 von ROCA betroffene Schlüssel.
- Liechtenstein verwendet seit 2016 Schlüssel, die vermutlich durch fehlerhafte Konfiguration mit schwachen Zufallszahlen erzeugt wurden.

Die betroffenen Reisepässe sind unabhängig von der elektronischen Funktion weiterhin gültig und bieten über physikalische Eigenschaften einen gewissen Fälschungsschutz. Bei den betroffenen Document-Signer-Schlüsseln lässt sich jedoch eine elektronische Fälschung eines Reisepasses mit beliebigen Passdaten erzeugen. Insbesondere für ABC-Stationen (Automated-Border-Control) hat dies signifikante Auswirkungen.

Reaktion
Das BSI informierte umgehend die betroffenen Staaten Malaysia und Liechtenstein. Nach der Benachrichtigung hat Liechtenstein zeitnah und vorbildlich reagiert und konnte in Zusammenarbeit mit dem BSI die technische Ursache identifizieren. Die zuständigen Behörden in Liechtenstein haben mit dem kostenlosen Austausch von ca. 5500 betroffenen Pässen begonnen und die entsprechenden fehlerhaften Zertifikate zurückgerufen. Malaysia hat zwar umgehend die von ROCA betroffenen Signaturkarten ausgetauscht, so dass neu produzierte Pässe nicht mehr bedroht sind, jedoch wurden weder die zugehörigen Document-Signer-Schlüssel zurückgerufen, noch fand ein Austausch der im Feld befindlichen Pässe statt. Das BSI hat parallel zu den betroffenen Staaten die Bundespolizei über den Sachverhalt informiert und in Abstimmung mit dieser die betroffenen Schlüssel im Grenzkontrollsystem gesperrt.

Empfehlung
Aufgrund der Sperrung der Document-Signer-Schlüssel von Liechtenstein und Malysia im Grenzkontrollsystem kann es zu Problemen bei der Einreise mit den Reisepässen dieser Staaten kommen. Es wird daher empfohlen, betroffene Reisepässe gegen einen neuen auszutauschen. In Liechtenstein ist der Austausch kostenlos möglich.

2.1.15 Zulassung

Das BSI ist laut BSI-Gesetz (§3 Abs.1 S.2 Nr.1, 14 und 17) 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 geheim gehaltenen 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. Hauptsächlich sind von dem Verfahren IT-Sicherheitsprodukte betroffen, die Funktionen zur Verschlüsselung (Kryptierung) enthalten und daher als Kryptosysteme bezeichnet werden. Der Antrag auf Zulassung eines IT-Sicherheitsproduktes kann grundsätzlich nur von einem behördlichen Anwender (Bedarfsträger) gestellt werden.

Nach § 37 der VSA müssen Produkte zur Herstellung von Schlüsselmitteln, zur Verschlüsselung, zur Sicherung von Übertragungsleitungen und zur Trennung von Netzen mit unterschiedlichen maximalen Einstufungen der zu verarbeiteten Verschlusssachen vom BSI zugelassen 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 190. 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 nach zugelassenen Produkten decken zu können, betreut das BSI aktuell mehr als 60 parallel laufende Verfahren mit dem Ziel einer Zulassung.

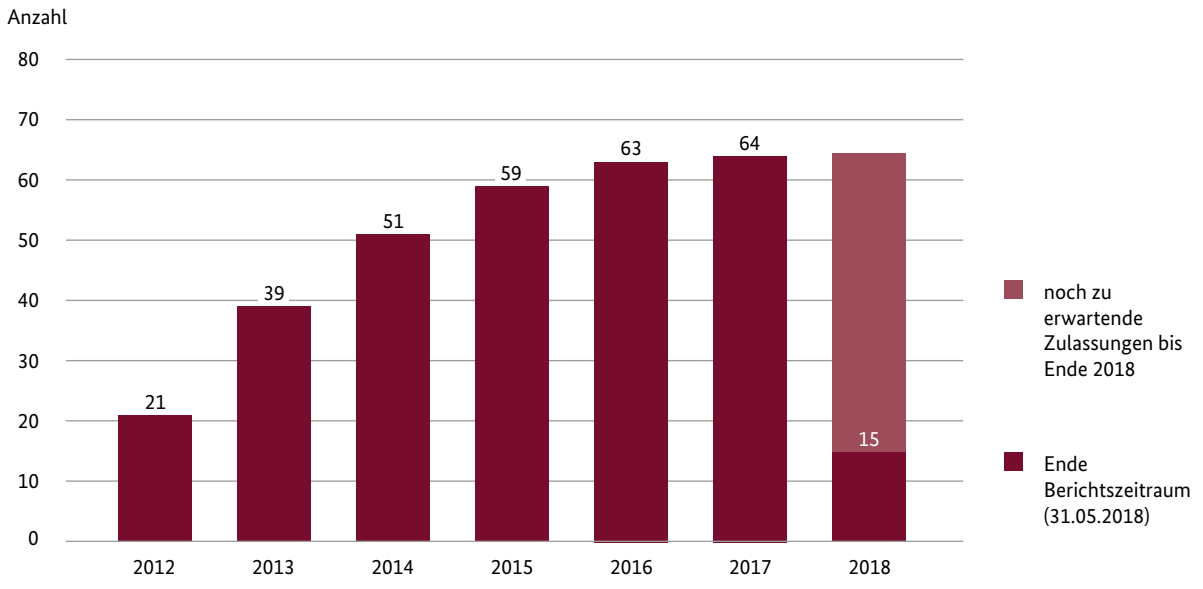


Abbildung 17 Zulassungen der vergangenen Jahre, Stand: 31.05.2018.

2.1.16 VS-Anforderungsprofile

Das BSI möchte den stark wachsenden Bedarf der Bundesverwaltung an sicheren IT-Lösungen durch eine Optimierung des Zulassungsprozesses adäquat begegnen. Im Bereich der Verarbeitung, Übertragung und Speicherung von Verschlusssachen (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, die Produkte beim Umgang mit eingestuften Dokumenten verwenden wollen und hierfür die grundsätzlichen Anforderungen benötigen, denen die geeigneten Produkte genügen müssen. Zum anderen richten sich VS-APs an die Hersteller solcher Produkte, um diesen eine generelle technische Leitlinie zur Umsetzung geltender relevanter IT-Sicherheitsanforderungen zu geben.

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

Die Zielsetzung zur Definition von VS-Anforderungsprofilen soll dabei folgenden maßgeblichen Kriterien genügen:

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 sieben VS-Anforderungsprofile publiziert, weitere vier befinden sich in Bearbeitung. Mit ihnen deckt das BSI bereits die unterschiedlichsten Produktklassen für den Schutz und die Verarbeitung von eingestuften Informationen ab. Parallel dazu befindet sich eine Vielzahl an VS-APs bzw. nPPs für den Einsatz im VS-Bereich in der Vorbereitung für die Standardisierung weiterer IT-Sicherheitsprodukte.

Die Entscheidung des BSI, Produkthersteller, Bedarfsträger und Betreiber schon frühzeitig in die aktive Gestaltung derartiger IT-Sicherheitsanforderungen einzubinden, führt zu einer durchweg positiven Resonanz sowie regen Beteiligung am beschriebenen Vorgehen.

2.1.17 Technische Richtlinien TR-ESOR und TR-RESISCAN

Für die elektronische Aktenführung verlangt der Gesetzgeber die Einhaltung des „Stands der Technik“ (§§ 6 und 7 des Gesetzes zur Förderung der elektronischen Verwaltung (eGovG), §§ 298a Zivilprozessordnung (ZPO) und 32e Strafprozessordnung (StPO)).

Das BSI veröffentlicht Technische Richtlinien (TR), die eine Umsetzung entsprechender E-Government-Lösungen nach dem „Stand der Technik“ ermöglichen. Wenn die TR des BSI befolgt werden, kann regelmäßig der „Stand der Technik“ als eingehalten gelten.

- Für die rechtskonforme elektronische Aktenführung definiert die BSI-TR 03138 „Ersetzendes Scannen“ (kurz: TR-RESISCAN) Anforderungen an die ordnungsgemäße und risikominimierende Gestaltung des Scanprozesses. Das Ziel der TR-RESISCAN ist es, Anwendern in Verwaltung, Justiz, aber auch in der Wirtschaft und im Gesundheitswesen als Handlungsleitfaden und Entscheidungshilfe zu dienen, wenn es darum geht, Papierdokumente nicht nur einzuscannen, sondern nach Erstellung des Scanproduktes auch zu vernichten.

- Mit der Technischen Richtlinie BSI-TR 03125 „Beweiswerterhaltung kryptographisch signierter Dokumente“ (kurz: TR-ESOR) definiert das BSI auf Basis der internationalen Standards RFC 4998 und RFC 6283 und der ETSI-AdES- bzw. -ASiC-Formate sowie der eIDAS-Verordnung und des Vertrauensdienstegesetzes für Anwender in Verwaltung, Justiz, aber auch in der Wirtschaft und im Gesundheitswesen einen Leitfaden zur Beweiswerterhaltung archivierter Daten und Dokumente bis zum Ende der gesetzlich vorgeschriebenen Aufbewahrungspflicht.

Darüber hinaus wurde sowohl mit dem ArchiSig-Modell, das der TR-ESOR zugrunde liegt, als auch mit einem nach TR-RESISCAN erzeugten Digitalisat mittels Simulationsstudien in rechtlicher Hinsicht nachgewiesen, dass bei Einhaltung der TR-Empfehlungen der jeweilige Beweiswert optimiert und die Beweisführung vor Gericht entsprechend vereinfacht werden kann.

2.2 Zielgruppe Wirtschaft

Vernetzung und Austausch sind wichtige Elemente des digitalen Wandels in der Industrie. Sie sind zugleich ein wichtiger Faktor für die Produktivität und das wirtschaftliche Wachstum in Deutschland. Intelligente und miteinander vernetzte Maschinen tauschen Informationen direkt untereinander in Echtzeit aus. In der „Smart Factory" organisieren sich die Produktionsanlagen selbstständig und koordinieren Abläufe und Termine untereinander. Dadurch wird die Produktion flexibler, dynamischer und effizienter. Zudem kommunizieren die Maschinen direkt mit allen IT-Systemen des Unternehmens und damit direkt mit den Mitarbeitern. Damit wird aber auch die Anfälligkeit der Wirtschaft für Hackerattacken und Cyber-Angriffe zusätzlich erhöht. Das BSI hat bereits in vielfältiger Weise in Eigenregie und durch seine Partnernetzwerke Impulse gesetzt, um seinen Auftrag auch gegenüber der Wirtschaft zu erfüllen.

2.2.1 Allianz für Cyber-Sicherheit

Mit der 2012 gegründeten Allianz für Cyber-Sicherheit (ACS) verfolgt das BSI das Ziel, die Cyber-Sicherheit am Standort Deutschland zu erhöhen. Unter dem Motto „Netzwerke schützen Netzwerke" unterstützt die ACS Unternehmen mit praxisnahen Hilfestellungen bei der Analyse von Cyber-Risiken und der Umsetzung geeigneter Schutzmaßnahmen. Inzwischen gehören der Initiative mehr als 2.700 Unternehmen, Behörden, Vereine und Verbände, Forschungsinstitute und andere Institutionen aus ganz Deutschland an. Und täglich kommen neue Teilnehmer hinzu, um von der Expertise des BSI und der Kooperations-Partner der ACS aus Wirtschaft und Forschung sowie dem vertrauensvollen Erfahrungsaustausch mit anderen Unternehmen und Institutionen zu profitieren. Ein weiteres starkes Wachstum strebt die Allianz für die ACS bei kleinen und mittleren Unternehmen (KMU) an. Hierzu werden umfangreiche Maßnahmen ergriffen, die im Folgenden dargestellt werden.

Rund hundert Partner und über fünfzig Multiplikatoren engagieren sich in der ACS und leisten so einen wertvollen Beitrag für mehr Cyber-Sicherheit am Wirtschaftsstandort Deutschland. Die für Teilnehmer der ACS kostenfreien Angebote der Partnerunternehmen sind ein wichtiger Mehrwert der Allianz für Cyber-Sicherheit; insbesondere für kleine und mittlere Unternehmen, die keine eigene Threat-Intelligence betreiben. Dazu gehören Schulungen und Workshops, Analysen und Erstberatungen oder Penetrations-Tests. Im Jahr 2018 konnte die ACS ihren Teilnehmern nahezu wöchentlich ein kostenfreies Angebot eines Partner-Unternehmens bereitstellen.

Darüber hinaus konnten im Berichtszeitraum wichtige strategische Partnerschaften, z. B. mit dem Zentralverband des Deutschen Handwerks (ZDH) und dem Handelsverband Deutschland (HDE), initiiert und durch die Unterzeichnung formaler Absichtserklärungen bekräftigt werden. Allein über den ZDH erreicht die ACS rund eine Million Handwerksbetriebe mit 5,45 Millionen Beschäftigten in ganz Deutschland. Als erste konkrete Maßnahmen im Rahmen dieser Kooperationen werden beispielsweise gemeinsam mit dem ZDH neue IT-Grundschutzprofile für Handwerksorganisationen bzw. -betriebe entwickelt und zielgruppenspezifische Veranstaltungen durchgeführt.

Ein weiteres Erfolgsmodell ist das im Auftrag des BSI durchgeführte „Übungszentrum Netzverteidigung". Das Angebot ist stets in wenigen Stunden ausgebucht. Großen Zuspruch erfahren auch die Cyber-Sicherheits-Tage, die die ACS in Kooperation mit Partnern oder Multiplikatoren ausrichtet. Diese themen- oder zielgruppenspezifischen Veranstaltungen werden aufgrund der großen Nachfrage inzwischen sechsmal im Jahr durchgeführt.

Ein strategisches Ziel der Allianz für Cyber-Sicherheit ist es, den praxisnahen Erfahrungsaustausch in der Wirtschaft zu fördern. Die im Berichtszeitraum neu konzipierten ERFA-Kreise stehen unter dem Motto „miteinander voneinander lernen" und dienen dazu, den fachlichen, thematisch gebundenen oder zielgruppenspezifischen Austausch in einem geschützten und vertraulichen Rahmen zu ermöglichen. Cyber-Sicherheitsexperten des BSI und anderer Institutionen begleiten und bereichern den Austauschprozess mit ihrem Fachwissen.

Austausch der Cybersicherheits-Initiativen in Deutschland

Mitte 2017 startete das BSI einen Dialogprozess der Cyber-Sicherheits-Initiativen in Deutschland. Eingeladen sind Netzwerke und Organisationen wie Verbände, Forschungseinrichtungen sowie Behörden, die sich übergreifend im Bereich Cyber-Sicherheit für Unternehmen und/oder Bürgerinnen und Bürger engagieren. Ziel ist es, Synergien zu nutzen, das Bewusstsein für Cyber-Sicherheit in Deutschland und die Reichweite einzelner Sensibilisierungsaktionen weiter zu erhöhen. Die Organisation und Gestaltung des Austauschs hat die Allianz für Cyber-Sicherheit übernommen.

Der Austausch der Cyber-Sicherheits-Initiativen entwickelt sich sehr positiv. Es entstehen an vielen Stellen produktive und auf Nachhaltigkeit ausgerichtete Kooperationen. Perspektivisch kann dieser Austausch unter Federführung des BSI den Ausgangspunkt für das im Koalitionsvertrag angeregte Cyber-Bündnis bilden.

2.2.2 IT-Grundschutz

Mit dem IT-Grundschutz bietet das BSI Anwendern aus Wirtschaft und Verwaltung ein fundiertes und praktisches Managementsystem für Informationssicherheit (ISMS). Es hilft dabei, den Status der Informationssicherheit in einer Institution zu überprüfen und in der Folge zu verbessern. Im Oktober 2017 wurde auf der Sicherheitsmesse it-sa der modernisierte IT-Grundschutz vorgestellt, der unter anderem um die Themen Detektion und industrielle Steuerungssysteme (ICS) ergänzt worden ist. Die Empfehlungen des IT-Grundschutzes können nun noch schneller bereitgestellt und besser an die Größe und den erforderlichen Sicherheitsbedarf einer Institution angepasst werden. Die neue Struktur und die kompakteren Veröffentlichungen zu unterschiedlichsten Themen der Informationssicherheit tragen dazu bei, dass die Inhalte dem Stand der Technik besser entsprechen.

Praktische Empfehlungen für mehr Informationssicherheit

Die grundlegend überarbeiteten BSI-Standards sind die zentralen Veröffentlichungen des IT-Grundschutzes:

- Im BSI-Standard 200-1 erfahren Sicherheitsverantwortliche alles Wissenswerte zum Aufbau eines Managementsystems zur Informationssicherheit.
- Im BSI-Standard 200-2 wird die Methodik des IT-Grundschutzes erläutert.
- Der BSI-Standard 200-3 behandelt die Risikoanalyse auf der Basis von IT-Grundschutz.

Mit Hilfe der BSI-Standards erfahren die Anwender, wie die relevanten IT-Systeme identifiziert werden können, wie deren Schutzbedarf ermittelt werden kann und wie vorgegangen werden kann, wenn ein höherer Schutzbedarf abgesichert werden soll.

Eine weitere essentielle Veröffentlichung des IT-Grundschutzes ist das IT-Grundschutz-Kompendium mit den zugehörigen Bausteinen. In der aktuellen Edition von Februar 2017 sind die ersten 80 IT-Grundschutz-Bausteine veröffentlicht, die gleichzeitig auch Grundlage für eine Zertifizierung nach ISO27001 auf Basis IT-Grundschutz sind. Anwender können sich anhand der Bausteine detailliert mit jeweils einem Thema auseinandersetzen. In den Anforderungen der Bausteine erfahren Sicherheitsverantwortliche, mit welchen Stellschrauben sie das Sicherheitsniveau anheben können. Detaillierte Hinweise und Maßnahmen sind in den ergänzenden Umsetzungshinweisen zu finden, die zu den meisten IT-Grundschutz-Bausteinen veröffentlicht wurden. Die Aktualisierung aller Inhalte erfolgte mit enger Einbindung der IT-Grundschutz-Community. Dadurch sind die aktuellen Inhalte des IT-Grundschutzes nicht nur fachlich fundiert, sondern auch praxiserprobt und anwendungsnah aufbereitet.

Von Anwendern für Anwender: IT-Grundschutz-Profile

Ein neues Element des IT-Grundschutzes bilden die IT-Grundschutz-Profile. Dabei handelt es sich um Muster-Sicherheitskonzepte, die als Schablone für Institutionen mit vergleichbaren Rahmenbedingungen dienen können. Das BSI unterstützt die Wirtschaft und Verwaltung dabei, erste IT-Grundschutz-Profile für bestimmte Branchen auf den Weg zu bringen. Dazu wurde u. a. eine Anleitung veröffentlicht, die Interessenten durch den Prozess führt. Mit ersten Branchenvertretern fanden erfolgreiche Auftakt-Workshops statt, in deren Folge bereits erste IT-Grundschutz-Profile veröffentlicht wurden. Ein enger Austausch und Zusammenarbeit wird auch bei der Realisierung der IT-Grundschutz-Profile gelebt. Der IT-Grundschutz trägt auch damit nachhaltig zur Erhöhung des Niveaus der Informationssicherheit in Deutschland bei.

2.2.3 UP KRITIS und IT-SiG

Umsetzung des IT-Sicherheitsgesetzes

Um der zunehmenden Bedeutung der Informations- und Kommunikationstechnik Rechnung zu tragen und neue Bedrohungen rechtzeitig zu bekämpfen, wurden dem BSI durch das BSI-Gesetz vom Gesetzgeber Aufgaben und Befugnisse zum Schutz Kritischer Infrastrukturen (KRITIS) eingeräumt. So müssen beispielsweise nach § 8a BSIG Betreiber Kritischer Infrastrukturen IT-Sicherheitsvorkehrungen nach dem Stand der Technik treffen und deren Umsetzung alle zwei Jahre gegenüber dem BSI nachweisen. Weiterhin kann das BSI die Einhaltung der IT-Sicherheit vor Ort überprüfen und darf, sofern Sicherheitsmängel aufgedeckt werden, im Einvernehmen mit den zuständigen Aufsichtsbehörden deren Beseitigung verlangen.

Anschluss der Betreiber Kritischer Infrastrukturen an die Warn- und Meldestrukturen des BSI

Ende Dezember 2017 endete die Frist zur Registrierung und Benennung einer Kontaktstelle für die Betreiber Kritischer Infrastrukturen aus den KRITIS-Sektoren Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr (ÄnderungsV BSI-KritisV vom 30.06.2017, sogenannter zweiter „Korb“). Über alle KRITIS-Sektoren hinweg haben sich nunmehr etwa 300 Betreiber mit 1400 Anlagen beim BSI registriert. Diese wurden an die Warn- und Meldestrukturen des BSI angeschlossen und werden vom BSI-Lagezentrum regelmäßig und anlassbezogen mit Warnungen und (Lage-)Informationen zur Cyber-Sicherheit versorgt.

Status der branchenspezifischen Sicherheitsstandards der verschiedenen Sektoren

Zur Umsetzung des § 8a Abs.1 BSIG müssen KRITIS-Betreiber „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen treffen“. Sie können dafür branchenspezifische Sicherheitsstandards (B3S) erarbeiten, die auf Antrag vom BSI auf Eignung geprüft werden. Die Erstellung und Anwendung eines B3S

- erleichtert insbesondere die Identifikation geeigneter Vorkehrungen und die Methodik zur Umsetzung entsprechender Maßnahmen,
- berücksichtigt branchenspezifische Anforderungen und
- definiert „Best Practices“ für eine Branche oder einen KRITIS-Sektor.

Anwender erhalten außerdem Klarheit bzgl. der Interpretation von im BSIG verwendeten abstrakten Begriffen wie „angemessen“, „geeignet“ oder „Stand der Technik“. B3S werden vorzugsweise in den Branchenarbeitskreisen des UP KRITIS entwickelt. In den folgenden Branchen befinden sich derzeit B3S in der Entwicklung:

- Lebensmittelproduktion und Verarbeitung,
- Verteilung von Fernwärme,
- Anlagen oder Systeme zur Steuerung/Bündelung elektrischer Leistung,
- Luftverkehr.

In den folgenden Branchen wurde die Eignung von B3S durch das BSI bereits erfolgreich festgestellt:

- Trinkwasserversorgung/Abwasserbeseitigung,
- Lebensmittelhandel,
- Informationstechnik, Anlagenkategorie Rechenzentrum/Serverfarmen und Content Delivery Netzwerk (CDN).

Das BSI berät die Verfasser von B3S auf Wunsch bei der Erstellung und unterstützt durch Beratungsgespräche und Workshops bis hin zu einer Vorab-Eignungsprüfung. Diese Angebote werden von den KRITIS-Branchen häufig angefragt und genutzt. Es gibt sogar Branchen, die nicht zur Umsetzung des § 8a BSIG verpflichtet sind und dennoch planen, einen B3S zu entwickeln.

Um KRITIS-Betreiber und deren Verbände allgemein bei der Entwicklung von B3S zu unterstützen, hat das BSI bereits im Dezember 2015 eine Orientierungshilfe für B3S herausgegeben. Diese definiert Kriterien zur geeigneten Festlegung des Geltungsbereichs eines B3S sowie der Definition von KRITIS-Schutzzielen und weist auf die Notwendigkeit der Beachtung besonderer Aspekte in der Gefahrenanalyse, der Risikobewertung und des Risikomanagements hin. Die Orientierungshilfe listet für die zu ergreifenden Sicherheitsvorkehrungen und Maßnahmen relevante Themenfelder auf und bietet Hilfestellung zur Detailtiefe, Angemessenheit und Eignung von Maßnahmen.

Anfang des Jahres 2018 hat das BSI nach einer Zeit der Praxiserprobung und mit der gewonnenen Erfahrung die Orientierungshilfe komplett überarbeitet und die neue Fassung auf seiner Website veröffentlicht. Das BSI hat dazu mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), dem Themenarbeitskreis (TAK) „Audits und Standards“ des UP KRITIS sowie mit den Autoren von B3S zusammengearbeitet. Neben vielen Detailverbesserungen wird nun insbesondere die Einbeziehung von allgemeinen sowie branchenspezifischen Standards (IT-Grundschutz, ISO 27001, C5-Katalog, ISO 62443 etc.) bei der Erstellung eines B3S berücksichtigt. Außerdem sind die Erstellungs-, Einreichungs- und Prüfprozesse sowie die Veröffentlichung eines B3S nun detailliert beschrieben.

Die Orientierungshilfe unterstützt damit Verfasser branchenspezifischer Sicherheitsstandards, bietet aber auch KRITIS-Betreibern eine Unterstützung zur Umsetzung der in § 8a (1) BSIG geforderten Sicherheitsvorkehrungen und -maßnahmen und ist für Prüfer eine mögliche Hilfe, um eine geeignete Prüfgrundlage zu entwickeln.

In diesem Sinne enthält die Orientierungshilfe keine harten Vorgaben, sondern beschreibt einen qualitativen Rahmen, der gleichwertige Alternativen zu der beschriebenen Vorgehensweise und den Kriterien zulässt. Sie erlaubt damit eine Berücksichtigung der Gegebenheiten der verschiedenen KRITIS-Sektoren und ermöglicht es KRITIS-Betreibern, auf ihre Situation angepasste B3S zu erstellen und somit die notwendige IT-Sicherheit mit dem geringstmöglichen Aufwand zu verwirklichen.

Ende der Nachweisfrist gemäß § 8a Abs. 3 BSIG für Betreiber gemäß BSI-KritisV vom 03.05.2016

KRITIS-Betreiber aus dem sogenannten ersten „Korb" der BSI-KRITIS-Verordnung (die Sektoren Wasser, Ernährung, Energie sowie Informationstechnik und Telekommunikation) mussten bis 3. Mai 2018 „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind." (§ 8a Abs. 1 BSIG) und dies gegenüber dem BSI nachweisen.

Zur Unterstützung des Nachweisprozesses hat das BSI eine Orientierungshilfe gemäß § 8a Abs. 3 BSIG herausgegeben, in der sowohl für die Betreiber als auch für die prüfenden Stellen die wichtigsten Rahmenbedingungen erläutert werden: Es wird beschrieben, welche Aufgaben und Zuständigkeiten Betreiber, prüfende Stellen und Prüfteams haben und über welche Qualifikationen die beiden letztgenannten verfügen sollten. Zusätzlich wird erläutert, welche Hilfsmittel zur Wahl der Prüfgrundlage zur Verfügung stehen, woraus sich Prüfthemen ableiten lassen und welche Besonderheiten bei den Themen Prüfmethodik, Prüfplan sowie Dokumentation der Prüfergebnisse zu beachten sind.

Deutsches Umsetzungsgesetz zur europäischen NIS-Richtlinie und Auswirkungen auf digitale Dienste

Im August 2016 ist die europäische Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie) in Kraft getreten, die von den EU-Mitgliedstaaten bis zum 9. Mai 2018 in nationales Recht umgesetzt werden musste.

Viele der in der NIS-Richtlinie enthaltenen Anforderungen, besonders an KRITIS-Betreiber, hatte Deutschland mit dem IT-Sicherheitsgesetz schon im Vorfeld umgesetzt. Mit dem Gesetz zur Umsetzung der NIS-Richtlinie wurden die übrigen noch notwendigen Anpassungen und Erweiterungen in nationales Recht überführt. Der Gesetzgeber hat damit insbesondere die Grundlage für die EU-weit einheitliche Regulierung von Anbietern bestimmter digitaler Dienste geschaffen. Die Vorgaben aus diesem Gesetz müssen seit dem 10. Mai 2018 eingehalten werden.

Neben KRITIS-Betreibern haben somit auch Anbieter digitaler Dienste (Online-Marktplätze, Online-Suchmaschinen und Cloud-Computing-Dienste) Sicherheitsvorfälle mit erheblichen Auswirkungen an das BSI zu melden. Weiterhin sehen die neuen Regelungen ein Mindestniveau an Maßnahmen zur präventiven IT-Sicherheit sowie zur reaktiven Bewältigung von Sicherheitsvorfällen vor. Eine Pflicht zur Registrierung einer Kontaktstelle sowie die Erbringung von Nachweisen über die Umsetzung der Maßnahmen sind für die Anbieter digitaler Dienste nicht vorgesehen.

Das BSI wurde als nationale Cyber-Sicherheitsbehörde mit der Aufsicht über die Anbieter der digitalen Dienste beauftragt. Innerhalb des Berichtszeitraums hat das BSI noch keine Meldungen über Sicherheitsvorfälle von Anbietern digitaler Dienste erhalten.

2.2.4 Mobile Incident Response Team

Mit der Cyber-Sicherheitsstrategie 2016 der Bundesregierung wurde der Fokus des CERT-Einsatzes verstärkt auf die Unterstützung vor Ort gelegt. Das BSIG wurde daher im Juni 2017 dahingehend geändert (§ 5a BSIG), dass das BSI befugt ist, unter bestimmten Voraussetzungen Maßnahmen – auch vor Ort – zu treffen, die zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit eines betroffenen informationstechnischen Systems erforderlich sind. Das BSI hat daraufhin mobile Einsatzteams – Mobile Incident Response Teams (MIRT) – aufgebaut, die bei IT-Sicherheitsvorfällen Betroffene vor Ort unterstützen können. Der Schwerpunkt liegt dabei auf Einrichtungen der Bundesverwaltung und Betreibern Kritischer Infrastrukturen. In Einzelfällen können MIRTs auch bei anderen Unternehmen zum Einsatz kommen. Dies geschieht ausschließlich auf Wunsch der betroffenen Stelle, die ein entsprechendes Ersuchen an das BSI richten muss.

Sowohl das Prozedere als auch die Unterstützungsmöglichkeiten entwickelten sich und wuchsen mit den Erfahrungen, die in diesen Notfalleinsätzen gesammelt wurden.

Zu den bekanntesten, öffentlich gewordenen MIRT-Einsätzen zählen der IT-Vorfall im Deutschen Bundestag 2015, die Unterstützung von Krankenhäusern während der Ransomware-Welle 2016 und der 2018 bekannt gewordene IT-Angriff auf das Auswärtige Amt.

Das entsandte MIRT setzt sich üblicherweise aus einem Incident Handler (IH) und zusätzlichen Experten aus verschiedenen Bereichen zusammen. In enger Abstimmung mit dem Betriebs- und IT-Sicherheitspersonal der betroffenen Stelle unterstützt das MIRT organisatorisch und koordinierend, aber insbesondere fachlich das Vorgehen, um den detektierten IT-Sicherheitsvorfall zu beheben. Dazu versuchen die Experten des MIRT, das Problem zunächst einzugrenzen und die Schadensursache zu isolieren. Im Falle eines konkreten IT-Angriffs werden Signaturen, auch Indicators of Compromise (IoCs) genannt, gesucht. Es wird den Fragen nachgegangen, wie weit und tief sich der Angreifer im Netz vorgearbeitet hat und ob zentrale Komponenten befallen sind.

Kurzfristiges Ziel eines MIRT-Einsatzes ist es, erste Maßnahmen zur Schadensbegrenzung und Sicherstellung des Notbetriebes vor Ort zu ergreifen. Oft versetzt erst die unmittelbare Zusammenarbeit sowie der Informations- und Erfahrungsaustausch vor Ort mit denjenigen, die die betroffenen IT-Systeme tagtäglich betreuen, das BSI in die Lage, dieses Ziel zu erreichen.

Eventuell notwendige, langfristige Bereinigung, Neuplanung, Erweiterung oder Aktualisierung der IT-Systeme, muss die betroffene Stelle in eigener Verantwortung durchführen. Aber auch hier kann das BSI im Rahmen seiner Beratungsaufgaben unterstützen, dann allerdings nicht mit einem Vor-Ort-Team.

2.2.5 Trends in der IT-Sicherheitszertifizierung von Produkten

Die Zertifizierung der IT-Sicherheit eines Produktes durch das BSI bedeutet: Es wurde auf Basis öffentlicher Prüfkriterien und in einem transparenten Prozess von einer unabhängigen Partei geprüft (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 im internationalen Abkommen Common Criteria Recognition Agreement (CCRA, https://www.commoncriteriaportal.org) vertretenen 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 es, 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 bereits in zahlreichen Gesetzen und Verordnungen verankert. So wird auch im Koalitionsvertrag gefordert, Hersteller und Anbieter von IT-Produkten, die neben den Kritischen Infrastrukturen von besonderem nationalem Interesse sind, stärker in die Pflicht zu nehmen. Vielfach betrifft dies die Digitalisierungsprojekte der Bundesregierung z. B. in den Bereichen eHealth, Hoheitliche Dokumente und Smart Metering sowie 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 (eIDAS-Verordnung). 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 15 Nationen aktiv unterstützt: Kroatien, Estland, Luxemburg, Polen und Dänemark sind dazugekommen (https://www.sogis.org). Die in der Senior Official Group Information Systems Security (SOGIS) organisierten Mitgliedsstaaten 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, in dem auch ein EU-weites Zertifizierungsmodell verankert werden soll, befindet sich zum Ende des Berichtszeitraums (31. Mai 2018) in der Abstimmung. Der Europäische Rat und das Europäische Parlament haben das Paket

bereits beraten. Im Anschluss wird zusammen mit der EU-Kommission das finale Gesetzeswerk verhandelt. Die EU-Mitgliedstaaten haben mit SOGIS-MRA bereits ein starkes, eingespieltes Zertifizierungskonzept in Betrieb, das dann voraussichtlich 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 einen FIDO-Token,
- PPs für Digitale Tachographen gemäß aktueller EU-Verordnung,
- PP für Datenbank Management Systeme.

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.

Konformitätsprüfungen und Zertifizierung von IT-Sicherheitskomponenten und -dienstleistungen

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 TRs durch die Deutsche Akkreditierungsstelle (DAkkS) akkreditiert. Im Rahmen der Zertifizierung nach Technischen Richtlinien wurden im Zeitraum 01. Juli 2017 bis 31. Mai 2018 60 Zertifikate aus 13 Prüfbereichen erteilt, wobei 27 Erst- und Re-Zertifizierungen und 24 Maintenance-Verfahren durchgeführt wurden.

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 vom BSI entwickelten IT-Grundschutzes durchgeführt wird. Die IT-Grundschutz-Vorgehensweise und die im IT-Grundschutz enthaltenen Empfehlungen von Standard-Sicherheitsmaßnahmen stellen inzwischen einen De-Facto-Standard für IT-Sicherheit dar.

Hier wurden im Berichtszeitraum insgesamt 38 „ISO 27001 Zertifikate auf Basis von IT-Grundschutz“ erteilt und darüber hinaus 73 Überwachungsaudits durchgeführt.

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-Claimsoft 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 Mitgliedsländern 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). Von Mai 2017 bis Mai 2018 wurden folgende Bescheinigungen erteilt:

- BSI-EBI-0008-2017 „Stop Extremism“
- BSI-EBI-0009-2018 „We are a welcoming Europe, let us help!“

Das BSI ist nationale Aufsichtsstelle für Vertrauensdienste im Bereich der „Erstellung, Überprüfung und Validierung von Zertifikaten für die Website-Authentifizierung“ gemäß eIDAS-VO bzw. Vertrauens-Dienste-Gesetz (VDG) und zuständig für die Qualifizierung von Vertrauensdienste-Anbietern in diesem Bereich. Hier wurde von Juli 2017 bis Mai 2018 ein qualifizierter Vertrauensdienste-Anbieter zertifiziert.

2.2.6 Investitionskontrolle

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 §§ 4 ff. des Außenwirtschaftsgesetzes (AWG) bzw. §§ 55 ff. und §§ 60 ff. 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 des Erwerbers und der Zielgesellschaft analysiert und bewertet das BSI mögliche Gefährdungssituationen hinsichtlich der IT-Sicherheit. Die Gefährdungsbewertung fließt ein in das sicherheitspolitische Votum des BMI.

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

- Seit Jahren steigen Anzahl und Volumen unionsfremder Investitionen in deutsche Zielgesellschaften.
- Außenwirtschaftliche Investitionskontrollen gerieten verstärkt in den politischen Fokus, zum Beispiel durch die Übernahme des schwäbischen Roboterherstellers KUKA AG durch das chinesische Unternehmen Midea Group Co Ltd.
- Durch die Änderung der AWV wurden 2017 wichtige Verfahrensregeln geändert und auch eine Meldepflicht für Erwerbsvorhaben im KRITIS-Sektor eingeführt, so dass Erwerbsparteien nun generell mehr Verfahren anzeigen bzw. beantragen müssen, um Rechtssicherheit für die geplante Investition zu erlangen.

Die Anzahl der durch das BSI begleiteten Einzelprüfungen im Zusammenhang mit Investitionskontrollverfahren stieg von vier Verfahren im Jahr 2015 auf 15 im folgenden Jahr. 2017 waren es bereits 23 und 2018 wurden bis Juli schon 31 Verfahren durch das BSI geprüft.

2.2.7 Ausfuhrkontrolle

Das BSI unterstützt das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) bei Anträgen auf Ausfuhr-/Verbringungsgenehmigung auf Basis des Erlasses für die Vorlage von Ausfuhrgenehmigungsanträgen für Güter mit Eigenschaften oder Funktionen der Informationssicherheit beim BSI. Gesetzliche Grundlage für diese Unterstützung sind das Außenwirtschaftsgesetz (AWG), die Außenwirtschaftsverordnung (AWV) und die EU-Verordnung (EG) Nr. 428/2009 des Rates vom 5. Mai 2009 (EG-Dual-Use-VO). Der Schwerpunkt liegt auf dem Gebiet der Krypto-Exportkontrolle und gliedert sich wie folgt:

1. Unterstützung aber auch (Selbst-)Schutz der deutschen Kryptoindustrie,

2. Schutz zugelassener IT-Sicherheitsprodukte, Komponenten wie Smartcards und spezifischer Technologien vor Re-Engineering, Manipulation usw.

Die Bearbeitung dieser Anträge ist eine Querschnittsaufgabe, die eine enge Zusammenarbeit mit externen Behörden, den Antragstellern und Herstellern sowie zwischen den verschiedenen Fachabteilungen des BSI erfordert.

Für die aktuelle bilaterale Zusammenarbeit des BSI mit dem BAFA wurde ein neues Vorgehen erarbeitet, das eine umfassendere, schnellere und qualitätsorientiertere Bearbeitung der Anträge gegenüber den vergangenen Jahren ermöglicht. Dies beinhaltet u. a. den Fokus der Exportkontrolle auf zugelassene IT-Sicherheitsprodukte, dessen Auswirkung auf die BAFA-Anträge in Abb. 1 deutlich wird.

Das BSI hat im Jahr 2017 102 Anträge bearbeitet.

Zudem wurde das BSI im Jahr 2017 zu folgende Themen mit BAFA-Bezug aktiv:

- Mitarbeit bei der Überarbeitung der EG Dual-Use-Verordnung
- Bewertung von Voranfragen (Anträgen) für schutzbedürftige Information im o. g. Kontext, wie z. B. Prüfberichte aus dem Common-Criteria-Umfeld
- Beteiligung bei Verkäufen/Übernahmen von Unternehmen im Bereich der Informationssicherheit
- Bearbeitung von Exportanfragen im Zusammenhang mit der BSI-Verschlüsselungssoftware Chiasmus

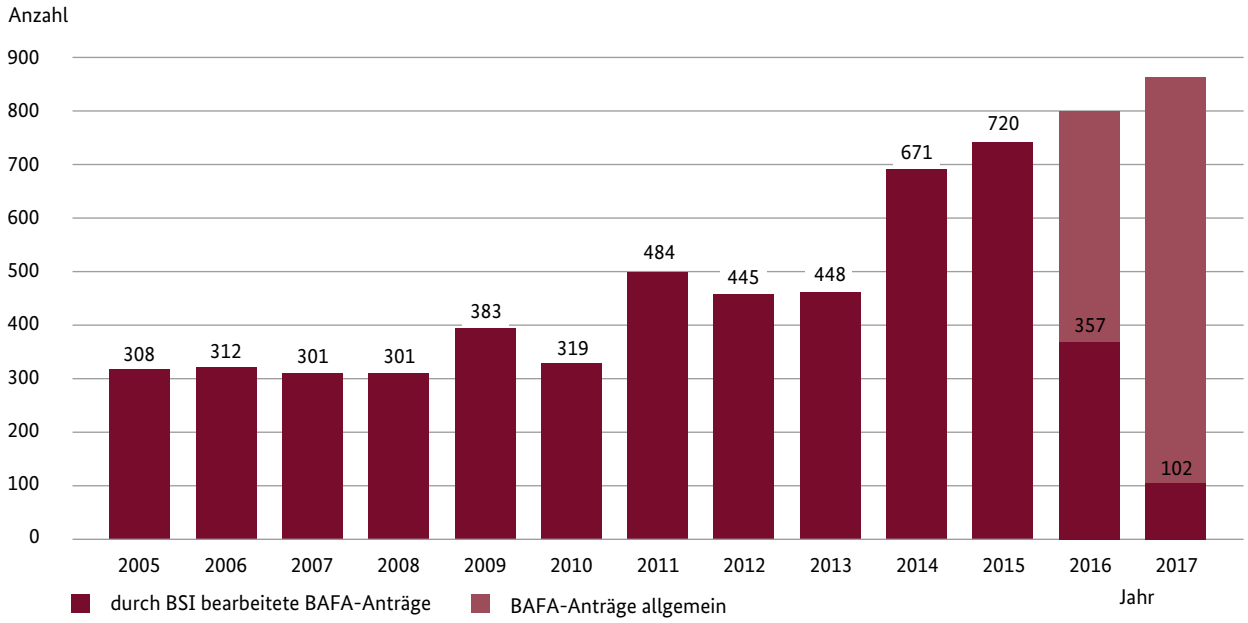


Abbildung 18 Darstellung der Anzahl der im BSI bearbeiteten BAFA-Anträge von 01.01.2005 bis 31.12.2017

- Unterstützung des BAFA bei der Auskunft zur Güterliste (AzG) zur Feststellung der Exportpflicht eines Produktes im o. g. Kontext

- Sicherstellung abgeschlossener Memorandum of Agreement (MoA) für den Export von zugelassenen IT-Sicherheitsprodukten (ab der Einstufung VS-VERTRAULICH)

- Abstimmungen mit dem BAFA hinsichtlich der Optimierung der Zusammenarbeit, insbesondere der Überarbeitung nationaler und EU-Allgemeingenehmigungen (AGG16, AGG24, EU001, EU004 und EU009)

2.2.8 Sonstige Lösungen und Angebote für die Wirtschaft

Absicherung von Ad-Servern

Zur Refinanzierung von kostenfreien Inhalten auf Webseiten (z. B. von Nachrichten-Portalen) setzen Webseiten-Betreiber bevorzugt Online-Werbung ein. Ein typisches Werbemittel dabei sind sogenannte Werbebanner, die beispielsweise im oberen Bereich oder im Seitenbereich einer Webseite eingeblendet werden. Aus technischer Sicht wird das Ausliefern von Werbemitteln von sogenannten Ad-Servern realisiert: Beim Besuch einer werbefinanzierten Webseite durch den Nutzer stellt die Webseite zunächst eine Verbindung zu den hinterlegten Ad-Servern her. Der Ad-Server wählt anschließend, basierend auf einem komplexen Prozess (real-time bidding) auf den Nutzer zugeschnittene Werbemittel aus und sendet diese unmittelbar an den Besucher der Webseite zurück.

In der Vergangenheit gab es wiederholt Vorfälle, bei denen Schadprogramme in Werbebannern versteckt und verteilt wurden (Malvertising). Dazu haben Angreifer beispielsweise bestehende, schlecht abgesicherte Ad-Server kompromittiert oder mittels gestohlener Kreditkarten Werbeplätze bei Vermarktern eingekauft, um schadhafte Werbemittel zu verbreiten. Für Angreifer ist Online-Werbung ein aussichtsreicher Angriffsvektor, da durch die Verknüpfung eines Ad-Servers mit vielen Webseiten eine potenziell hohe Reichweite für die Verteilung von Schadprogrammen erzielt wird. Insbesondere besteht hier für Angreifer die Möglichkeit, Schadprogramme selbst auf seriösen Webseiten zu platzieren, sofern es gelingt, die vom Webseiten-Betreiber verlinkten Ad-Server zu kompromittieren.

Um das Bereitstellen von Online-Werbung sicher zu gestalten, hat das BSI ein Diskussionspapier zur Absicherung von Ad-Servern erstellt. Es richtet sich an die Adressaten der Online-Werbebranche, insbesondere an Betreiber von Ad-Servern und Vermarkter. Das Dokument enthält Empfehlungen, welche Maßnahmen nach dem Stand der Technik zu berücksichtigen sind, um IT-Systeme der Online-Werbebranche technisch abzusichern. Dazu gehört ein als sicher anerkanntes Verschlüsselungsverfahren,

damit u. a. die Auslieferung von Werbemitteln zwischen Web-Server und Client verschlüsselt erfolgt.

Da es sich bei Ad-Servern um geschäftsmäßig angebotene Telemedien handelt, müssen deren Betreiber neben anderen gesetzlichen Vorgaben wie dem Artikel 32 Datenschutz-Grundverordnung (DSGVO) die Sicherheitsmaßnahmen nach § 13 Abs. 7 Telemediengesetz (TMG) umsetzen, die im Rahmen des IT-Sicherheitsgesetzes eingeführt wurden. Die Empfehlungen des Diskussionspapiers sollen die Online-Werbebranche bei der Umsetzung dieser Sicherheitsmaßnahmen unterstützen.

Das Diskussionspapier wurde von Mitgliedern des Bundesverbandes Digitale Wirtschaft (BVDW) und des Bitkom kommentiert und befindet sich aktuell in einer finalen Abstimmung. Mit einer Veröffentlichung ist im Laufe des Jahres 2018 zu rechnen.

Cloud: Anforderungskatalog C5/Testate nach C5

Das BSI hat mit dem Anforderungskatalog zur Bewertung der Informationssicherheit von Cloud-Diensten (Cloud Computing Compliance Controls Catalogue; kurz: C5) einen Prüfstandard veröffentlicht, der ein Mindestsicherheitsniveau für Cloud-Dienste definiert (s. https://www.bsi.bund.de/C5). Mit dem Mindeststandard nach BSIG §8 „Nutzung externer Cloud-Dienste“ (https://www.bsi.bund.de/DE/Themen/StandardsKriterien/Mindeststandards/Nutzung_externer_Cloud-Dienste/Nutzung_externer_Cloud-Dienste_node.html) wurden dieses Niveau und der entsprechende Nachweis über ein Testat eines Wirtschaftsprüfers für die externe Cloudnutzung bei allen Stellen des Bundes vorgegeben.

Der Cloud-Markt hat diese Vorgabe für Stellen des Bundes aufgegriffen und so werden inzwischen C5-Testate auch von Unternehmen bei einer Cloud-Nutzung angewendet. Die große Spannbreite von ergangenen Testaten im Berichtszeitraum macht dies deutlich:

- August 2017: Testat für Microsoft Azure Dienste aus Deutschland
- November 2017: Testat für die Dropbox Dienste Business und Education
- Dezember 2017: Testat für die Dienste der Alibaba Cloud aus den Regionen Frankfurt und Singapur
- März 2018: Testat für Microsoft Office 365 aus Deutschland
- April 2018: Erneuerung des C5 Testats für die Dienste von Amazon Webservices aus Frankfurt
- Mai 2018: Testat für die Infrastructure-as-a-Service Dienste von IBM weltweit

2.3 Zielgruppe Gesellschaft

Eine wichtige Aufgabe des BSI ist die Information und Sensibilisierung von Bürgerinnen und Bürgern für einen sicheren Umgang mit Informationstechnologie, mobilen Kommunikationsmitteln und dem Internet. Dazu hat das BSI ein umfangreiches Informationsangebot unter „BSI für Bürger“ (https://www.bsi-fuer-buerger) entwickelt. Darüber hinaus ist das BSI in zahlreiche Digitalisierungsprojekte von der eID-Ausweisfunktion bis zum autonomen Fahren involviert und bringt dort seinen Sachverstand ein. Es kooperiert mit relevanten gesellschaftlichen Gruppen und der Wissenschaft. Durch den Koalitionsvertrag der Bundesregierung aus CDU, CSU und SPD vom Februar 2018 ist zudem festgelegt, dass Verbraucherschutz als zusätzliche Aufgabe des BSI etabliert werden soll.

2.3.1 Koalitionsvertrag: Neue Aufgabe Verbraucherschutz

Mit der Etablierung des Verbraucherschutzes als weitere Aufgabe des BSI wird das Profil des BSI als bürgerorientierte Cyber-Sicherheitsbehörde gestärkt. Das BSI möchte Verbraucherinnen und Verbraucher unterstützen, um so die Resilienz gegen Cybergefahren jeglicher Art zu steigern. Dadurch leistet das BSI einen wichtigen Beitrag zur Gestaltung von Informationssicherheit und trägt zum Gelingen der Digitalisierung bei.

Bereits heute unterstützt das BSI als herstellerunabhängige und kompetente technische Stelle die Verbraucherinnen und Verbraucher in der Risikobewertung von Technologien, Produkten, Dienstleistungen und Medienangeboten. Zur Steigerung des Risikobewusstseins, der Beurteilungsfähigkeit und Handlungskompetenz im Bereich der Informationssicherheit, sollen im BSI bestehende Aktivitäten gebündelt und neue Maßnahmen eingeführt werden.

Um dieses Ziel zu erreichen, ist die Zusammenarbeit mit starken Partnern notwendig. Sie bildet den Ausgangspunkt für die geplante Intensivierung und den Aufbau der Aktivitäten zur Unterstützung der Verbraucherinnen und Verbraucher in Deutschland.

Bereits jetzt gibt es Ansätze im BSI, mit etablierten und anerkannten Akteuren im Bereich des Verbraucherschutzes zusammenzuarbeiten. So wurde etwa im März 2017 ein Memorandum of Understanding zwischen dem BSI und der Verbraucherzentrale Nordrhein-Westfalen (VZ NRW) e.V. abgeschlossen. Ein Beispiel der Kooperation stellt das gemeinsame Vorgehen hinsichtlich der fehlenden Update-Fähigkeit von Smartphones dar, die mit einem veralteten Betriebssystem im Handel als neu angeboten werden. Hierdurch bestehen bei der Nutzung teils gravierende Sicherheitslücken. Mit Unterstützung des BSI hat die Verbraucherzentrale NRW ein gerichtliches Unterlassungsverfahren gegen den Verkäufer eines solchen Geräts wegen unzureichender Verbraucherinformation eingeleitet. Das Verfahren ist zum Ende des Berichtszeitraums noch nicht abgeschlossen.

2.3.2 Bürger-Services des BSI

Seit über 15 Jahren betreibt das BSI die Webseite www.bsi-fuer-buerger.de, auf der Nutzerinnen und Nutzer neben Beiträgen und Informationen zu aktuellen Themen auch Checklisten und zuletzt vermehrt anschauliche Erklärvideos und Infografiken zu Risiken im Internet und zur sicheren Nutzung von IT finden. Im Berichtszeitraum wurde insbesondere das Informationsangebot zum Themenbereich Internet der Dinge aufgebaut: Es stehen nun Informationen auf der Webseite zur Verfügung, darunter Empfehlungen für Smart-Home-Anwendungen. Im Oktober 2017 wurde das Informationsangebot als Broschüre „Internet der Dinge – aber sicher!“ veröffentlicht. Zudem stehen Informationen und Empfehlungen zum Thema Wearables bereit.

Der kostenlose Warn- und Informationsdienst „Bürger-CERT“ ist ebenfalls Teil des Informationsangebots auf www.bsi-fuer-buerger.de. Mit diesem informiert das BSI auf der Webseite und per E-Mail-Abonnement entweder in Form von „Technischen Warnungen“ oder mit dem vierzehntägigen Newsletter „Sicher ° Informiert“ schnell und kompetent über Schwachstellen, Sicherheitslücken und andere Risiken und gibt entsprechende Hilfestellungen. Derzeit nutzen rund 105.000 Abonnenten dieses Angebot.

Mit der Facebook-Seite www.facebook.com/bsi.fuer.buerger und dem Twitter-Kanal www.twitter.com/BSI_Presse ist das BSI auch in den sozialen Netzwerken vertreten, informiert dort Nutzer und bietet eine Dialogmöglichkeit. Zum Stichtag 31. Mai 2018 folgten dem BSI auf Facebook 34.160 Personen, bei Twitter 11.715.

An das Service-Center des BSI können Privatanwender telefonisch unter 0800 2741000 oder per E-Mail unter mail@bsi-fuer-buerger.de ihre Fragen zu Themen der IT- und Internetsicherheit stellen. Monatlich erreichen im Durchschnitt 600 Anfragen von Privatanwendern auf diesem Weg das BSI. Zudem können Privatanwender und Organisationen kostenfrei Exemplare der Bürgerbroschüren des BSI beziehen.

Europäischer Monat der Cyber-Sicherheit (ECSM)

Im Oktober 2017 fand zum inzwischen fünften Mal europaweit unter der Federführung der European Network and Information Security Agency (ENISA) der Europäische Monat der Cyber-Sicherheit (European Cyber Security Month ECSM) statt. Wie in den Vorjahren übernahm das BSI in Deutschland die Rolle der nationalen Koordinierungsstelle. Es konnten 104 Partner für den Aktionsmonat gewonnen werden, die sich mit 216 Aktionen einbrachten. Eine Übersicht zu diesen Aktionen – von Informationsveranstaltungen und Live-Hackings über Webinare und Onlinekampagnen – findet sich auf www.bsi.bund.de/ecsm.

Zu den wöchentlichen Schwerpunktthemen „Cyber-Sicherheit am Arbeitsplatz“, „Sicherheit und Schutz persönlicher Daten“, „Cyber-Sicherheit zuhause“ sowie „Cyber-Sicherheit vermitteln - an Profis und Anwender“ beteiligte sich das BSI mit eigenen Aktionen in Form von jeweils einer Pressemitteilung, themenbezogenen Facebook-Postings und einem Statementvideo, in dem ein Experte aus dem BSI eine zentrale Frage aus dem Themenbereich erläuterte.

Darüber hinaus wurde anlässlich des ECSM auf www.bsi-fuer-buerger.de das Thema sicheres Smart Home in den Fokus gestellt: Neben zwei aktuellen Informationstexten wurde ein animiertes Erklärvideo veröffentlicht, mit dem Online-Quiz „Smart Home – aber sicher“ konnten Webseitennutzer ihr Wissen zu dem Thema testen. Zusätzlich wurde ein kurzes Expertengespräch aufgezeichnet und als Radio-Materndienst über einen Dienstleister Radiosendern zur Verfügung gestellt.

An seinem Standort Bonn brachte sich das BSI bei den Bonner Tagen der Cyber-Sicherheit vom 23.–27. Oktober 2017 mit ein. Unter anderem beteiligte es sich an dem Aktionstag „Dark Cyber Monday“ mit einem Informationsstand mit Roboter-Live-Hacking und einem Fachvortrag.

Kooperation mit ProPK

Im Berichtszeitraum wurde die zwischen dem BSI und dem Programm Polizeiliche Kriminalprävention (ProPK) der Länder und des Bundes geschlossene Kooperation weiter fortgesetzt. Gemeinsam kommunizierten die beiden Partner unter anderem zum sicheren vernetzten Zuhause und zum regelmäßigen Anlegen von Back-ups. Anlässlich des Safer Internet Days am 6. Februar 2018 veröffentlichten BSI und ProPK die Ergebnisse einer gemeinsam durchgeführten, repräsentativen Onlinebefragung unter Bürgerinnen und Bürgern zu den Themenschwerpunkten Sicherheit im Internet und Erfahrungen mit Internet-Kriminalität (siehe separates Kapitel zu Umfrageergebnissen).

2.3.3 Institutionalisierung des gesellschaftlichen Dialogs

Bereits im Jahr 2016 hat das BSI daran mitgewirkt, den gesellschaftlichen Dialog zum Themenfeld Informations- und Cyber-Sicherheit zu intensivieren. Das Veranstaltungsformat der „Denkwerkstatt sichere Informationsgesellschaft“ hat sich etabliert und dient dem offenen und vertrauensvollen Austausch zu Fragen der Cyber-Sicherheit zwischen Staat, Wirtschaft, Wissenschaft und Zivilgesellschaft. Im Projekt „Digitale Gesellschaft: smart & sicher“ wurde hierauf aufgebaut und die Aktivitäten verstärkt. Unter anderem wurden gemeinschaftlich „Impulse für eine smarte und sichere digitale Gesellschaft“ erarbeitet und im September 2017 der Öffentlichkeit vorgestellt. Dieser fruchtbare Diskurs hat das BSI motiviert, den eingeschlagenen Weg weiterzugehen. Im Nachfolgeprojekt „Institutionalisierung des gesellschaftlichen Dialogs“ wird der vertrauensvolle Dialog aktuell ausgebaut und vertieft. Hierfür werden derzeit in einem partizipativen Vorgehen Möglichkeiten der Institutionalisierung entwickelt und erprobt.

BSI im Dialog

BSI im Dialog ist eine Mitte 2016 gestartete Veranstaltungsreihe für die Zielgruppen Politik, Wirtschaft, Verbände und Gesellschaft. Ziel der Veranstaltungsreihe ist, Dialoge rund um strategische Themen der Cyber-Sicherheit anzuregen. Damit soll das BSI bei den Zielgruppen sichtbarer, die Aufgaben des BSI transparenter und die Aufmerksamkeit der Öffentlichkeit für das Themenfeld Informations- und Cyber-Sicherheit erhöht werden. Auch für die Zukunft ist geplant, weitere BSI-im-Dialog-Veranstaltungen zu verschiedenen Schwerpunkten mit unterschiedlichen Zielgruppen durchzuführen.

Durch das Format der Veranstaltung wird ein persönlicher Austausch auf Augenhöhe weiter gefördert. Damit einhergehend werden Synergieeffekte für das Cyber-Sicherheitslagebild in Deutschland geschaffen.

Besonderes elektronisches Anwaltspostfach (beA)

Sachverhalt
Ende Dezember 2017 wurden Sicherheitsprobleme rund um das besondere elektronische Anwaltspostfach (beA) bekannt. Ein Mitglied des Chaos Computer Clubs hatte die zum Postfach-Zugriff sowie zum Ver- und Entschlüsseln der Nachrichten benötigte Software „beA Client-Security“ analysiert und war dabei neben veralteten Softwarebibliotheken mit Sicherheitslücken auch auf den privaten Schlüssel eines TLS-Zertifikats gestoßen, der mit der Software ausgeliefert wurde.

Der Chaos Computer Club meldete die Probleme zunächst an die für das beA zuständige Bundesrechtsanwaltskammer (BRAK) sowie an das CERT Bund des BSI. Zeitgleich informierte er die Zertifizierungsstelle, die das TLS-Zertifikat ausgestellt hatte, über die offensichtliche Kompromittierung des privaten Schlüssels. Diese zog entsprechend ihrer Zertifizierungsrichtlinien das zugehörige Zertifikat zurück.

Ursache/Schadenswirkung
Die Auslieferung eines privaten TLS-Schlüssels in der Clientsoftware war bei der vorgesehenen Architektur des beA-Postfachs prinzipbedingt notwendig: Die beA Client-Security betreibt auf einem lokalen Port einen HTTPS-Server und kommuniziert über diesen mit dem Webmail-Interface des beA-Postfachs im Webbrowser des Anwenders.

Um die Nutzbarkeit des beA-Postfachs zur passiven Nutzungspflicht ab 1. Januar 2018 nicht zu gefährden, informierte die BRAK über die Ungültigkeit des Zertifikats und stellte im Austausch ein selbst-signiertes TLS-Zertifikat (prinzipbedingt

erneut inkl. des zugehörigen privaten Schlüssels) zur Verfügung. Dieses Zertifikat sollten Anwälte nun auf ihren Systemen manuell installieren.

Bei diesem Zertifikat handelte es sich jedoch um ein Root-Zertifikat, mit dem Zertifikate für beliebige Web-Domains ausgestellt werden könnten. Auf betroffenen Anwaltsrechnern wäre es somit möglich gewesen, den Kommunikationsverkehr in verschlüsselten Internetverbindungen mitzulesen oder zu manipulieren.

Nach Hinweisen aus dem IT-Sicherheitsumfeld stoppte die BRAK die Verteilung des Zertifikats und der entsprechenden Installationsanleitung umgehend und forderte dazu auf, das Zertifikat wieder zu deinstallieren.

Reaktion
Die BRAK schaltete das beA-Postfach nach Bekanntwerden der Sicherheitslücken serverseitig bis auf Weiteres ab und veranstaltete im Januar 2018 einen sogenannten „beAthon", um die Sicherheitsprobleme mit dem ursprünglichen Entdecker und weiteren Experten zu diskutieren. Darüber hinaus beauftragte die BRAK ein unabhängiges Expertengutachten bei einem IT-Sicherheitsdienstleister.

Parallel dazu arbeitete die von der BRAK mit der Entwicklung beauftragte Dienstleisterin an der Behebung der Sicherheitsprobleme. Zum 4. Juli 2018 stellte die BRAK den Rechtsanwältinnen und Rechtsanwälten eine neue Version der beA Client-Security zum Download zur Verfügung, bei der die durch den IT-Sicherheitsdienstleister bekannt gewordenen Schwachstellen als behoben verifiziert wurden; das beA-Postfach soll nach derzeitiger Planung am 4. September 2018 wieder in Betrieb genommen werden.

Das BSI stand bereits früh mit der BRAK und dem für die beA Client-Security verantwortlichen Auftragnehmer unterstützend in Kontakt.

Aus Sicht des BSI ist das Zurückziehen der anfälligen Software die richtige Reaktion des Anbieters gewesen, auch wenn eine gesetzliche Vorgabe hierdurch nicht eingehalten werden konnte. Datensicherheit hatte in diesem Fall richtigerweise Vorrang vor Funktionalität.

Empfehlung
Falls nicht bereits geschehen, sollte das durch die BRAK am 22. Dezember 2017 bereitgestellte, selbst-signierte TLS-Zertifikat umgehend von betroffenen Rechnern entfernt werden.

Die BRAK empfiehlt außerdem, die alte Version der beA Client-Security komplett zu deinstallieren und wird am 4. Juli 2018 eine neue Version der beA Client-Security bereitstellen bei der laut BRAK die Sicherheitsprobleme behoben seien. Das am 22. Dezember 2017 bereitgestellte Zertifikat werde in dieser Version automatisch gelöscht.

2.3.4 Digitalisierungsprojekte in Deutschland

Energiewende/Smart Meter

Eine erfolgreiche digitale Transformation in der Energiewirtschaft kann nur mit der frühzeitigen nationalen Entwicklung und Bereitstellung von allgemeinverbindlichen Sicherheitsstandards sowie Maßnahmen zur Sicherung der Vertrauenswürdigkeit digitaler Infrastrukturen gelingen („privacy & security by design"). Folglich ist zunächst ein nationaler Referenzmarkt mit sicheren Produktkomponenten, Systemen und Kommunikationsinfrastrukturen entscheidend, um eine führende Gestaltungsrolle bei der Digitalisierung des Energiebereichs einzunehmen und darauf aufbauend die europäische sowie internationale Standardisierung zu gestalten.

Das BSI entwickelt im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi) Schutzprofile und Technische Richtlinien sowie Prüfverfahren für das Smart-Meter-Gateway als zentrale Kommunikationsplattform intelligenter Messsysteme. Im Zusammenhang mit den technischen Standards des BSI schafft das Gesetz zur Digitalisierung der Energiewende nun verbindliche Rahmenbedingungen für den sicheren und datenschutzkonformen Einsatz und zeigt bereits perspektivisch die Ausgestaltung von Mindestanforderungen zur sicheren Integration der Ladesäuleninfrastruktur von Elektromobilen in das intelligente Stromnetz auf.

Die Nutzung der Batterien von Elektromobilen als Stromspeicher und die Erzeugung von Regelenergie, die zum Ausgleich der schwankenden Einspeisung aus Windparks und Solaranlagen gebraucht wird, werden eine immer wichtigere Rolle spielen. Die zukünftige Integration des Smart-Meter-Gateways in die Ladesäule ermöglicht damit ein sicheres und datenschutzkonformes Laden und Abrechnen, das eine Grundvoraussetzung für eine zunehmende Verbreitung der Elektromobilität darstellt. Für die Weiterentwicklung der Standards wird es nach der BMWi-BSI-Roadmap („Standardisierungsstrategie zur sektorübergreifenden Digitalisierung nach dem Gesetz zur Digitalisierung der Energiewende“) die drei Schwerpunkt-Cluster Smart- & Sub-Metering, Smart Grid & Smart-Mobility und Smart Home & Building & Services geben.

Autonomes Fahren, Strategiepapier BMVI

In der Strategie automatisiertes und vernetztes Fahren der Bundesregierung wurde die IT-Sicherheit als wesentliches Handlungsfeld definiert. Angesichts zunehmend komplexer Informationstechnologie und zahlreicher Kommunikationsschnittstellen in modernen Fahrzeugen sind geeignete Maßnahmen zu identifizieren, die z. B. Hacker-Angriffe verhindern. In der gemeinsamen Arbeitsgruppe IT-Sicherheit und Datenschutz und der angeschlossenen Unterarbeitsgruppe IT-Sicherheit haben das Bundesministerium für Verkehr und digitale Infrastruktur (BMVI), das BSI und weitere Beteiligte aus Behörden und Wirtschaft eine Reihe entsprechender Handlungsempfehlungen in diesem Kontext entwickelt. Unter anderem wurden folgende Aspekte betrachtet:

- Typgenehmigung:
  Angesichts der möglichen Auswirkungen von IT-basierten Angriffen auf die Fahrzeuginsassen und weitere Verkehrsteilnehmer müssen IT-Sicherheitsmechanismen frühzeitig in der Entwicklung von (vernetzten und/oder automatisierten) Kraftfahrzeugen konzipiert und umgesetzt werden. Diese sollten dann im Rahmen der Typgenehmigung, die Voraussetzung für die Zulassung im Straßenverkehr ist, überprüft werden. Dafür sind geeignete Anforderungen und Prüfkriterien festzulegen. Zurzeit werden Grundlagen solcher Anforderungen bei der United Nations Economic Commission for Europe (UNECE) diskutiert, die die internationale Harmonisierung von Typgenehmigungsregeln vornimmt.

- Zertifizierung:
  Im Bereich klassischer IT-Sicherheitsprodukte sind seit vielen Jahren die Common Criteria als Grundlage für international anerkannte Zertifizierungen etabliert. Auch für IT-Komponenten in Fahrzeugen mit dedizierter Sicherheitsfunktionalität und hohem Schutzbedarf (z. B. zentrale Kommunikationsschnittstellen oder Komponenten für die Fahrzeug-zu-Fahrzeug-Kommunikation) wird empfohlen, eine solche Zertifizierung, z. B. als Bestandteil des Typgenehmigungsprozesses, zu prüfen.

- IT-Sicherheit im Feld:
  Angesichts der Komplexität der für die neuen Funktionen notwendigen Software in Fahrzeugen und den Erfahrungen aus der klassischen IT ist davon auszugehen, dass manche Schwachstellen und Sicherheitslücken erst entdeckt werden, wenn das Fahrzeugmodell schon auf dem Markt ist. Es sind Verfahren zu etablieren, die die dadurch entstehenden Gefährdungen minimieren. Es ist zu diskutieren, wie geeignete Meldewege für IT-Sicherheitsvorfälle aussehen können und ein Update-Management durch die jeweiligen Hersteller sichergestellt wird. Ferner sollten Behörden in die Lage versetzt werden, die IT-Sicherheit auch nach der Zulassung, etwa durch Penetrationstests, stichprobenartig zu überwachen.

eID: Europaweite Anerkennung der Online-Ausweisfunktion

Für die Umsetzung der Digitalisierung ist die sichere Identifizierung von Personen und Dingen von entscheidender Bedeutung. Nur so kann das Vertrauen in elektronische Dienstleistungen und Prozesse sichergestellt werden. Die Entwicklung sicherer eID-Technologien und ihrer Standardisierung ist daher eine der Kernkompetenzen des BSI.

Im Hinblick auf die Digitalisierung des europäischen Binnenmarkts wurden auf EU-Ebene mit der eIDAS-Verordnung (EU) 910/2014 erstmals einheitliche, europaweit geltende Rahmenbedingungen für die gegenseitige Anerkennung von elektronischen Identifizierungsmitteln und Vertrauensdiensten festgelegt. Das BSI beteiligt sich mit seiner Fachkenntnis an der weiteren Ausgestaltung sowie der technischen Umsetzung in allen Bereichen.

Im September 2017 hat Deutschland als erster EU-Mitgliedsstaat die Notifizierung der Online-Ausweisfunktion des Personalausweises und des elektronischen Aufenthaltstitels auf dem höchsten Vertrauensniveau gemäß eIDAS-Verordnung erfolgreich abgeschlossen. Im Rahmen

der Notifizierung wurde in einem „peer review"-Verfahren das deutsche eID-System durch die anderen Mitgliedstaaten der EU beziehungsweise des Europäischen Wirtschaftsraums (EWR) begutachtet. Im Beschluss durch das Kooperationsnetzwerk – das für die Koordination der eID-Themen zuständigen EU-Gremium – wurde dem deutschen System auf Basis des Abschlussberichts des Peer-Reviews bescheinigt, dass es die Anforderungen an das eIDAS-Vertrauensniveau „hoch" einhält. Das BSI hat die technischen Vorarbeiten für die Notifizierung der Online-Ausweisfunktion geleistet und den gesamten Notifizierungsprozess aus technischer Sicht begleitet.

Damit sind alle EU/EWR-Mitgliedstaaten ab September 2018 verpflichtet, die Online-Ausweisfunktion für Anwendungen des öffentlichen Sektors, d.h. insbesondere im *eGovernment*, anzuerkennen. Auch Unternehmen im EU-Ausland können den elektronischen Identitätsnachweis auf freiwilliger Basis anerkennen.

Auch bei der Anerkennung elektronischer Identitäten anderer Mitgliedstaaten im deutschen eGovernment laufen die Vorbereitungen mit Unterstützung des BSI auf Hochtouren. Im EU-Förderprojekt TREATS wurde die Infrastruktur für die technische Integration in das deutsche eID-System geschaffen. Zurzeit wird diese Infrastruktur in die eGovernment-Anwendungen integriert, so dass Deutschland für die Anerkennungsverpflichtung nach eIDAS zum September 2018 vorbereitet sein wird.

Im ersten Quartal 2018 haben mit Estland, Spanien, Kroatien, Italien und Luxemburg fünf weitere Länder die Notifizierung ihrer eID-Systeme eingeleitet, mit weiteren Notifizierungen ist im Laufe des Jahres zu rechnen.

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.

Eine sichere Zwei-Faktor-Authentisierung schafft hier Abhilfe. Dabei werden statt einem Faktor zwei Faktoren für die Authentisierung verwendet. Diese beiden Faktoren müssen unterschiedlichen Kategorien (Besitz, Wissen, Biometrie) angehören, damit sich die Stärken der Faktoren gegenseitig ergänzen, und miteinander verknüpft sind, so dass die beiden Faktoren nicht unabhängig voneinander angegriffen werden können. Die Instanziierung einer solchen sicheren Zwei-Faktor-Authentisierung ist ein Sicherheitselement. Hier wird der Faktor Wissen (in Form eines Passworts oder einer PIN) mit dem Faktor Besitz (das Sicherheitselement in Form z. B. einer Smartcard) sicher kombiniert – die PIN dient etwa zum Freischalten der Karte, auf der dann das Sicherheitselement durch kryptografische Methoden den Besitz gegenüber dem Authentisierungsserver nachweist.

Sichere Zwei-Faktor-Authentisierungslösungen sind bisher wenig verbreitet. Die Fast-IDentity-Online-Allianz (FIDO) wurde 2012 mit vielen verschiedenen Stakeholdern gegründet, um offene und lizenzfreie Industriestandards für die weltweite Authentisierung im Internet zu entwickeln. Nach FIDO sind bisher zwei Standards entwickelt worden:

- Der Universal Second Factor (U2F) passt sich in Form eines USB-Tokens nahtlos in existierende Web-Infrastrukturen ein.
- Der FIDO-UAF-Standard (Universal Authentication Framework) erlaubt darüber hinaus auch den Faktor Besitz durch biometrische Verfahren zu ersetzen und so eine sichere Zwei-Faktor-Authentisierung mit gleichzeitigem Verzicht auf jegliche Passwörter durchzuführen.

Ein Nachweis über die Sicherheit des verwendeten U2F-Tokens bzw. der Implementierung des UAF-Standards ist jedoch notwendig, um eine sichere Umsetzung der Protokolle in Produkte zu gewährleisten.

Als Mitglied der FIDO-Allianz ist das BSI an der Definition nachweisbar sicherer Authentisierungstoken beteiligt. Der Nachweis eines hohen Sicherheitsniveaus kann durch eine Zertifizierung nach Common Criteria erbracht werden. Das BSI hat hierzu ein solches Schutzprofil mit hoher Prüftiefe (EAL4+, AVA_VAN.5) für sichere FIDO-U2F-Token veröffentlicht (BSI-CC-PP-0096-2017), nach dem ein durch das BSI entwickelte FIDO-U2F-Token derzeit zertifiziert wird. Nach Abschluss der Zertifizierung werden die notwendigen Hersteller-Dokumente veröffentlicht, um anderen Herstellern von FIDO-Token einen erleichterten Zugang zur Zertifizierung eigener Produkte zu ermöglichen.

Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme

Im Zuge der Digitalisierung kommen beim Verkauf von Waren und Dienstleistungen heutzutage in der Regel elektronische Kassensysteme oder Registrierkassen (elektronische Aufzeichnungssysteme) zum Einsatz. Hierdurch hat sich das technische Umfeld des Besteuerungsverfahrens stark verändert. So sind nachträgliche Manipulationen an Aufzeichnungen elektronischer Kassensysteme (digitale Grundaufzeichnungen) ohne entsprechende Schutzmaßnahmen nur mit sehr hohem Aufwand feststellbar.

Das Gesetz zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen hat daher zum Ziel, Manipulationen an solchen Aufzeichnungen deutlich zu erschweren. Der zentrale technische Baustein zur Umsetzung des Gesetzesentwurfs ist die Einführung einer technischen Sicherheitseinrichtung.

Ab dem Jahr 2020 müssen elektronische Aufzeichnungssysteme über eine zertifizierte technische Sicherheitseinrichtung verfügen, die aus drei Bestandteilen besteht:

- Sicherheitsmodul:
  Es gewährleistet, dass Kasseneingaben mit Beginn des Aufzeichnungsvorgangs protokolliert und später nicht mehr unerkannt verändert werden können.

- Speichermedium:
  Dort werden die Einzelaufzeichnungen für die Dauer der gesetzlichen Aufbewahrungsfrist gespeichert.

- Einheitliche digitale Schnittstelle:
  Sie soll eine reibungslose Datenübertragung für Prüfungszwecke gewährleisten.

Durch die einheitliche digitale Schnittstelle der technischen Sicherheitseinrichtung soll auch die Integration in existierende und zukünftige Kassensysteme vereinfacht werden. Insbesondere sind für die digitale Schnittstelle keine besonderen Anforderungen an die physikalische Schnittstelle geplant, sodass übliche Standardschnittstellen wie z. B. USB, Ethernet, SD-Karten, etc. zum Einsatz kommen können.

Nachdem der gesetzliche Rahmen durch die Verabschiedung des Gesetzes festliegt, werden die technischen Anforderungen an das Sicherheitsmodul, das Speichermedium und die digitale Schnittstelle vom BSI über Technische Richtlinien und Schutzprofile festgelegt.

Die Technischen Richtlinien wurden mit dem Bundesministerium der Finanzen und einschlägigen Fachverbänden abgestimmt und werden im Juni 2018 final veröffentlicht. Somit bleibt ausreichend Zeit, um Technische Sicherheitseinrichtungen zu entwickeln und in den Verkehr zu bringen.

2.3.5 Elektronischer Reisepass

Am 1. November 2005 wurde in Deutschland die erste Generation des elektronischen Reisepasses eingeführt, zwei Jahre später mit der Integration von Fingerabdruckbildern die zweite Generation. Am 1. März 2017 folgte nun die dritte Generation. Neu sind dabei insbesondere ein völlig überarbeitetes äußeres Erscheinungsbild und neue physikalische Sicherheitsmerkmale. Augenfälligste Änderung ist die Einführung eines „Flexcovers“, welches das bekannte Hardcover-Passbuch ablöst, und die Einführung einer Polycarbonat-Datenseite analog zum Personalausweis und elektronischem Aufenthaltstitel. Dies führt dazu, dass auch der Chip aus dem vorderen Passdeckel in die Datenseite gewandert ist.

Auch für den elektronischen Bestandteil, den Chip, steht eine grundlegende Überarbeitung an. Unter Federführung des BSI werden die zurzeit getrennt gepflegten Chips für Reisepass, Personalausweis und Aufenthaltstitel auf eine gemeinsame Plattform überführt („Familienkonzept“). Dadurch werden die logistischen Aufwände reduziert. Zum anderen wird sichergestellt, dass in allen Dokumenten jeweils die neueste Chipgeneration eingesetzt werden kann.

Aktuelle Vorfälle (z. B. ROCA, siehe Infokasten Seite 35) zeigen, dass auch im Bereich von Chipkarten – insbesondere bei zehnjähriger Gültigkeit wie bei deutschen hoheitlichen Dokumenten – auf Sicherheitsvorfälle reagiert werden muss, auch wenn deutsche Dokumente von ROCA selbst nicht betroffen sind. Daher bereitet das BSI in Zusammenarbeit mit den Herstellern die Möglichkeit eines Chip-Updates nach Ausgabe vor. Die Updatemöglichkeit soll ebenfalls im Rahmen der neuen Chip-Plattform eingeführt werden. Für ein Update ist neben der Einführung einer entsprechenden chipseitigen Möglichkeit natürlich auch die entsprechende Infrastruktur notwendig, die ebenfalls vorbereitet wird.

Auch auf europäischer Ebene werden die Vorgaben für Pässe und Aufenthaltstitel zurzeit unter intensiver Mitarbeit des BSI aktualisiert. Neben der technischen Aktualisierung macht es dies möglich, den in die Jahre gekommenen Zugriffsschutz Basic Access Control (BAC) endgültig durch das im BSI entwickelte Password Authenticated Connection Establishment (PACE) abzulösen.

2.3.6 Gütesiegel/IT-Sicherheits-kennzeichen

Bereits in der 2016 veröffentlichten Cyber-Sicherheits-strategie für Deutschland hat das BMI die Einführung eines „Gütesiegels für IT-Sicherheit“ angekündigt. Dieses IT-Sicherheitskennzeichen soll es dem Verbraucher ermöglichen, IT-Sicherheit aktiv zum Bestandteil seiner Kaufentscheidung zu machen. Das Vorhaben wurde im Koalitionsvertrag 2018 bestätigt. Gleichzeitig ist dort vorgesehen, das Portfolio des BSI um das Thema Verbrau-cherschutz zu erweitern. Das IT-Sicherheitskennzeichen bettet sich in diese erweiterte Verbraucherschutzaufgabe des BSI ein.

Bereits heute gehört die Zertifizierung von IT-Sicherheits-produkten zu den etablierten Verfahren des BSI. Hersteller können ihre Produkte beim BSI zertifizieren lassen und mit diesem Zertifikat nachweisen, dass ihre Produkte in Bezug auf IT-Sicherheit - je nach Prüftiefe - einem spezifi-schen IT-Sicherheitsniveau entsprechen. Bislang richten sich Zertifikate an professionelle Anwender und durch das BSI zertifizierte Produkte finden meist im Rahmen von Digitalisierungsprojekten des Bundes ihre Anwendung.

Eine Lösung für den breiten Markt der Verbraucherpro-dukte mit Wirkungen für den Verbraucher unterscheidet sich von diesen etablierten Zertifizierungsverfahren.

Da die Kaufentscheidung des Verbrauchers im Mittel-punkt steht, muss das IT-Sicherheitskennzeichen leicht verständlich und transparent gestaltet sein. Das IT Sicher-heitskennzeichen muss dem Verbraucher bereits optisch auf dem Produkt (oder in einem Webshop) mit begleiten-den Sicherheitsinformationen präsent gemacht werden. Das IT-Sicherheitskennzeichen muss ferner dynamisch gestaltet werden, d.h. die Aktualität und Gültigkeit der Sicherheitsaussagen müssen transportiert werden können. Der Anreiz zur freiwilligen Verwendung auf Seiten der Hersteller wird in der Abgrenzung der eigenen Produkte gegenüber den Wettbewerbern liegen. Die IT-Sicherheit der Produkte muss Verkaufsargument werden.

Voraussetzung für ein freiwilliges IT-Sicherheitskennzei-chen sind transparente technische Kriterien, auf deren Basis das IT-Sicherheitskennzeichen verwendet werden kann. Diese Kriterien werden bisher in Form von Protec-tion Profiles oder Technischen Richtlinien durch das BSI veröffentlicht und werden zukünftig durch Anforderun-gen für IT-Produkte des Verbrauchermarktes erweitert. Auf diese Weise kann der Stand der Technik durch das BSI abgebildet werden.

Zur Nutzung des IT-Sicherheitskennzeichens ist die Etablierung eines Rechtsrahmens erforderlich, der es ermöglicht, die Bedürfnisse der Hersteller nach einer transparenten und schnellen Nutzung des IT-Sicherheits-kennzeichens zu bedienen (Herstellererklärung). Auf der anderen Seite muss der Rechtsrahmen auch Gewähr für die ausreichende Aussagekraft bzgl. der Einhaltung der IT-Sicherheitseigenschaften gegenüber den Verbrauchern bieten. Da je nach Produktkategorie unterschiedliche IT-Sicherheitsanforderungen gelten werden, wird das IT-Sicherheitskennzeichen nach und nach für die rele-vanten Produkte auf dem Verbrauchermarkt angeboten werden.

2.3.7 Biometrie-Evaluations-Zentrum

Biometrische Systeme sind einfach zu bedienen und zuverlässig. Deswegen haben sie mittlerweile einen festen Platz unter den IT-Sicherheitssystemen zur Benutzer-Authentisierung eingenommen. Sie gehören seit vielen Jahren im Consumer-Bereich zum Alltag und bekommen auch bei Hoheitlichen Anwendungen eine immer größere Bedeutung.

Die tatsächliche Qualität eines biometrischen Systems lässt sich aber nach wie vor nur mit großem Aufwand ermitteln. Ausschließlich durch umfangreiche Tests mit vielen Testpersonen und durch tiefgreifende Überwin-dungsversuche lassen sich belastbare Aussagen über Funktionalität und Schwachstellen eines biometrischen Systems treffen.

Auch bei biometrischen Verfahren ist das BSI bestrebt, seine Kompetenz in der ganzen Bandbreite von technolo-gischen Grundlagen über die Entwicklung neuer Technolo-gien und die Beratung von Herstellern bis hin zur Unter-stützung und Begleitung von biometrischen Verfahren im Wirkbetrieb einzubringen – mit effizienten und unab-hängigen Evaluationsmethodologien als Grundlage jedes Projektes. Je höher dabei die Anforderungen an IT-Sicher-heit und Zuverlässigkeit sind, desto umfangreicher muss auch evaluiert werden – und zwar mit jeder Änderung an Soft- und Hardware.

So nehmen z. B. auch im Europäischen Ein-/Ausreisesys-tem (EES) biometrische Authentifizierungs-Technologien zur Personenidentifikation in Verbindung mit elektroni-schen Ausweisen eine zentrale Rolle ein. Die eingesetzten Systeme müssen in hohem Maße verlässlich und über-windungssicher sein. Das ist für die praktische Umsetzung der EES-Ziele von besonderer Bedeutung.

In Kooperation mit der Bundespolizei hat das BSI u. a. die Aufgabe übernommen, die Performanz und die Überwindungssicherheit der eingesetzten biometrischen EES-Systeme kontinuierlich zu überprüfen und die Entwicklung neuer, sicherer Technologien sowie von entsprechenden Test- und Zertifizierungsverfahren voranzutreiben. Dazu sind insbesondere geeignete Labore notwendig, in denen die Testsysteme mit größeren Gruppen an Testpersonen unter kontrollierten Bedingungen geprüft werden können.

Diese Tests werden im neuen Biometrie-Evaluations-Zentrum (BEZ) durchgeführt, das zurzeit auf dem Campus der Hochschule Bonn-Rhein-Sieg (HBRS) in St. Augustin aufgebaut wird. Im BEZ wird die geeignete Test- und Analyse-Infrastruktur bereitgestellt, um regelmäßige „Performanz-“, „Überwindungssicherheit-“ und „Usability-Untersuchungen an biometrischen Systemen mit großen Nutzergruppen“ durchzuführen. Das BEZ ist ein mit öffentlichen Mitteln gefördertes Institut an der HBRS, für dessen Betrieb BSI und HBRS eine enge Kooperation eingegangen sind. So kann das BSI alle notwendigen Untersuchungen im Rahmen des EU-EES-Projektes im BEZ durchführen. In Zukunft wird diese Kooperation konsequent weiter ausgebaut.

Eine wichtige Aufgabe, um die Harmonisierung von EES-Systemen in Europa zu fördern, werden Schulungsmaßnahmen für Polizei (Bundespolizei bzw. FRONTEX), Prüflabore und Hersteller sein.

Durch die Zentralisierung dieser Testkompetenzen im BEZ wird die Evaluation biometrischer Systeme deutlich effizienter und belastbarer umgesetzt als es bisher möglich war. Mit dem BEZ unterstützt das BSI Hersteller, Entwickler und Anwender gleichermaßen und erzeugt eine größtmögliche Synergie für den gesamten Bund.

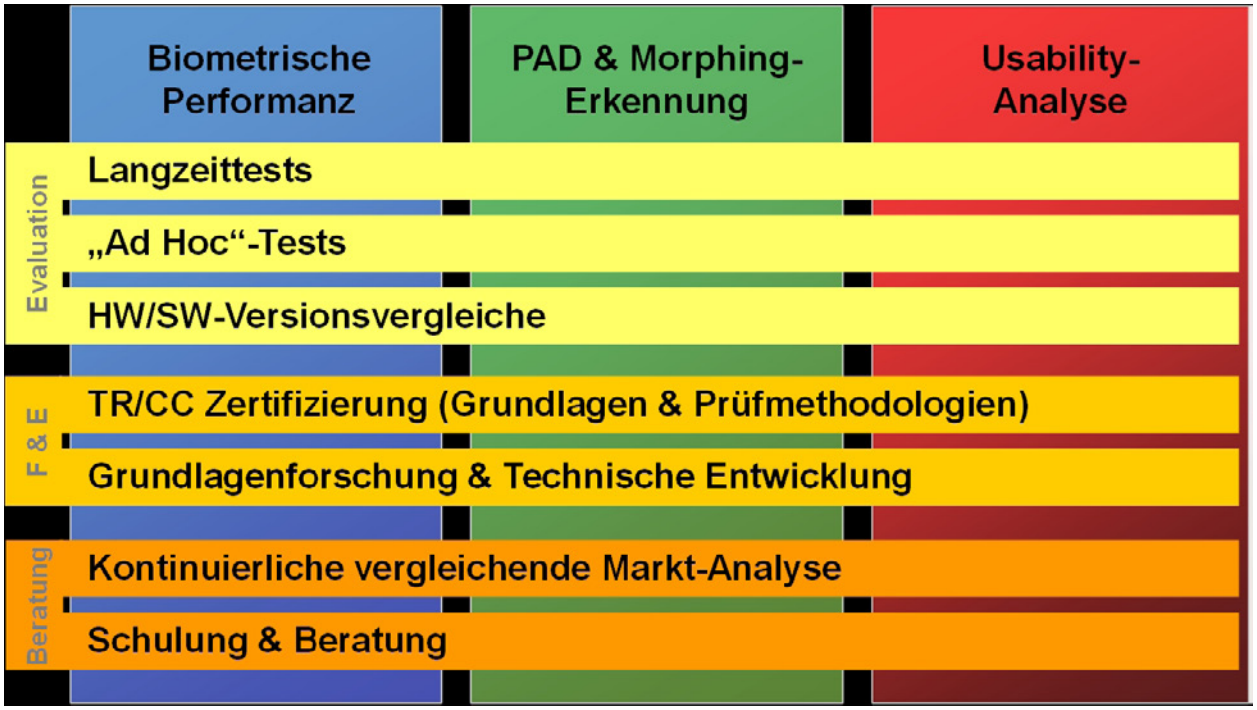


Abbildung 19 Handlungsfelder und Aktivitäten des BEZs

2.3.8 Eckpunktepapier Blockchain

Mit Blockchain entwickelt sich seit einiger Zeit eine neue Technologie für die dezentrale, manipulationssichere und konsensuale Datenhaltung in verteilten Netzwerken. Der Blockchain-Technologie wird momentan für einen Einsatz nicht nur im Finanzsektor (mit Kryptowährungen wie Bitcoin als dem klassischen Anwendungsfall für Blockchain), sondern auch im Gesundheitswesen, im Energiemarkt, im öffentlichen Sektor und in vielen anderen Branchen großes Potenzial zugeschrieben. Gleichzeitig werden immer wieder spektakuläre Fehler und Krisen in Bitcoin und anderen Blockchain-Anwendungen bekannt, die das Vertrauen in die neue Technologie auf die Probe stellen.

Beim Einsatz von Blockchains sind zurzeit noch viele sicherheitstechnische, regulatorische, rechtliche und soziotechnische Fragen offen. Insbesondere die Herstellung

von IT-Sicherheit ist aber essentiell für einen langfristigen Erfolg der Blockchain-Technologie in den verschiedenen Anwendungsbereichen.

Viele der klassischen Herausforderungen der IT-Sicherheit wie Netzwerk-, Endpunkt- oder Implementierungssicherheit sind auch beim Einsatz von Blockchains relevant. Für alle Anwendungen ist außerdem die Verwendung starker Kryptografie und sicherer Protokolle von großer Bedeutung, insbesondere dann, wenn eine Blockchain staatliche oder andere kritische Angebote absichern soll. Gerade in Anwendungen, die sicherheitsrelevante (etwa personenbezogene) Daten in einer Blockchain ablegen, ist die Vertraulichkeit und Integrität der Daten langfristig kryptografisch sicherzustellen.

Zum Thema Blockchain und IT-Sicherheit hat das BSI im Februar 2018 fünf zentrale Eckpunkte veröffentlicht, die den Dialog zwischen Staat, Wirtschaft und Gesellschaft anregen und kontinuierlich weiterentwickelt werden sollen. Das Eckpunktepapier ist unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Eckpunktepapier.pdf verfügbar.

2.3.9 Sicherer E-Mail-Transport

Ein Großteil der digitalen Kommunikation findet auch heute noch schnell und komfortabel per E-Mail statt. Vernachlässigt wird in der Praxis jedoch häufig die konsequente Anwendung von IT-Sicherheit. Um dem entgegenzuwirken, hat das BSI mit der Technischen Richtlinie „Secure E-Mail Transport (BSI TR-03108)“ einen einheitlichen Standard definiert, der den E-Mail-Dienste-Anbietern als Blaupause für den sicheren Betrieb ihrer E-Mail-Dienste dient. Dabei zielen die Anforderungen der Technischen Richtlinie insbesondere auf die funktional und kryptografisch sichere Konfiguration der Kommunikationsschnittstellen, um eine hochwertige Transportsicherheit zu gewährleisten. Hierbei wird auf zeitgemäße Standards wie DANE gesetzt, die bereits in der Praxis erprobt sind. Die Umsetzung der Anforderungen erfolgt allein durch die E-Mail-Dienste-Anbieter. Die Nutzer der E-Mail-Dienste profitieren somit von einem hohen Maß an IT-Sicherheit, ohne dass für sie ein zusätzlicher Aufwand entsteht.

Bereits der 2015 veröffentlichte Entwurf der TR wurde im Dialog mit am Markt tätigen E-Mail-Dienste-Anbietern erstellt. Das dem Entwurf zugrunde liegende Konzept wurde dabei stetig weiterentwickelt, wobei die IT-Sicherheit, Praxistauglichkeit und Nutzerakzeptanz im Vordergrund standen. Kern des Konzepts ist, dass durch die Technische Richtlinie kein neues in sich geschlossenes System entsteht, sondern die IT-Sicherheit der bereits existierenden E-Mail-Infrastruktur angehoben wird. Neben der Verwendung hochwertiger Kryptoverfahren zeichnen signierte DNS-Abfragen, obligatorische Verschlüsselung und vertrauenswürdige Zertifikate die Anforderungen der TR aus. Sie sind dabei so gewählt, dass immer eine sichere Verbindung mit dem E-Mail-Dienste-Anbieter aufgebaut wird, wenn die Gegenstelle dies ebenfalls unterstützt.

Ein Großteil der in Deutschland aktiven E-Mail-Dienste-Anbieter hat die Anforderungen der Technischen Richtlinie bereits umgesetzt. International stößt sie ebenfalls auf ein großes Interesse und findet viele Befürworter. So gibt es mittlerweile einen engen Kontakt zum niederländischen Nationaal Cyber Security Centrum (NCSC) und die gemeinsame Bestrebung, den Einsatz von modernen E-Mail-Sicherheitsstandards in Europa und darüber hinaus zu fördern. Mit jedem E-Mail-Dienste-Anbieter, der die Anforderungen der Technischen Richtlinie erfüllt, wächst das Netz des sicheren E-Mail-Transports weltweit.

2.3.10 Sicherheitsstandard für Breitband-Router

In vielen Haushalten werden Breitbandrouter (im Folgenden auch Router) genutzt, um damit auf das Internet zuzugreifen. Sie ermöglichen nicht nur den Zugriff auf das Internet, sondern man kann mit ihnen auch das private Heimnetzwerk verwalten. Sie können aber auch von beiden Seiten–lokal per Kabel bzw. on-the-air über Funkschnittstellen oder über das Internet – angegriffen werden. Es ist ihnen daher ein besonderes Gefahrenpotenzial zuzuschreiben.

Breitbandrouter sind verhältnismäßig leistungsstarke integrierte Systeme. Hieraus ergibt sich auch das Potenzial, sich erfolgreich gegen digitale Angriffe zur Wehr zu setzen. Mit einer Kontrollübernahme des Routers können von diesem selbst Angriffe initiiert werden, z. B. DDoS-Angriffe. So wurde im Jahre 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. Häufig bleiben Infektionen mit Schadsoftware allerdings unbemerkt. Daher ist es wichtig, für einen Basisschutz zu sorgen. Im besten Falle kann die Infektion des Routers so schon im Vorfeld verhindert werden.

Mit der Erstellung der Technischen Richtlinie für Breitbandrouter durch das BSI wurde eine Grundlage geschaffen, um Breitbandrouter gegen Angriffe zu schützen bzw. widerstandsfähig zu machen.

Folgende Angriffsszenarien und Bedrohungsarten können dabei unterschieden werden:

- Der Router wird angegriffen, um die Kontrolle darüber zu erlangen.
- Der Router wird angegriffen, um auf das private Netzwerk des Inhabers zugreifen zu können.
- Weiterhin könnte der Router angegriffen werden, um darüber unerlaubt Internetzugriff zu erlangen.

Die Technische Richtlinie für Breitbandrouter stellt wirksame Sicherheitsanforderungen an die Schnittstellen und Funktionalitäten eines Routers. So wird zum Beispiel zwingend die Fähigkeit gefordert, dass Updates eingespielt werden können. Zur besseren Transparenz soll der Hersteller der Breitbandrouter z. B. im Konfigurationsinterface angeben, bis zu welchem Zeitpunkt Updates bereitgestellt werden. Ebenso soll der Router immer nur die Ports öffnen, die für die Funktionalitäten, die er gerade anbietet, absolut essentiell sind. Fernwartungsports sollen nur dann geöffnet sein, wenn der Router im Vorhinein so konfiguriert wurde. Ebenso fordert die Technische Richtlinie, dass die Konfigurationsoberfläche nur mit ausreichend starker Authentifizierung erreicht werden kann und empfiehlt hierfür z. B. eine Multi-Faktor-Authentifizierung zu nutzen.

Die Anforderungen wurden in Zusammenarbeit mit Herstellern, Verbänden und anderen Vertretern aus Wirtschaft und Gesellschaft entwickelt. Die Technische Richtlinie ist inhaltlich fertiggestellt und kann als Grundlage für eine nationale sowie internationale Verwendung dienen.

2.3.11 Zusammenarbeit mit der Wissenschaft

Das BSI steht im regen Austausch mit der deutschen Cyber- und IT-Sicherheitsforschung. So diskutierten im vom BSI veranstalteten „BSI im Dialog mit der Wissenschaft“ Vertreter der folgenden führenden IT-Sicherheits-Forschungsstandorte mit Vertretern des BSI über Herausforderungen im Bereich IT- und Cyber-Sicherheit und mögliche Lösungsansätze: Center for IT-Security, Privacy and Accountability (CISPA, Saarbrücken), Center for Research in Security and Privacy (CRISP, Darmstadt), Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (AISEC, München), Kompetenzzentrum für angewandte Sicherheitstechnologie (KASTEL, Karlsruhe), Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE), Forschungsinstitut Cyber Defence (CODE, Neubiberg), Horst Görtz Institut für IT-Sicherheit (HGI, Bochum). Das BSI ist bzw. war in fachlichen Beiräten (Advisory Boards) von verschiedenen Forschungsprojekten vertreten, etwa im EU-Horizon2020-Projekt Hardware Enabled Krypto And Randomness (HECTOR). Es adressiert das Spannungsfeld zwischen mathematischer Sicherheit, Implementierungssicherheit und der Effizienz von kryptografischen Systemen unter einem ganzheitlichen Ansatz. Weiterhin ist das BSI im Advisory Board des EU-Horizon2020-Projekts Robust and Efficient Approaches to Evaluating Side Channel and Fault Attack Resilience (REASSURE) vertreten, das die Effizienz, Qualität und Vergleichbarkeit von Seitenkanaluntersuchungen im Kontext von Sicherheitsbewertungen weiterentwickelt. Durch diese Mitwirkung nimmt das BSI seine Position in der EU als nationale Cyber-Sicherheitsbehörde wahr. Darüber hinaus fördert das BSI gezielt vielversprechende Ansätze zur Weiterentwicklung der IT-/Cyber-Sicherheit durch Unterstützungsschreiben (Letter-Of-Support).

Weiterhin unterstützt das BSI personell den Aufbau und die Ausgestaltung der in Planung befindlichen „Agentur für Innovation in der Cybersicherheit“, die der US-amerikanischen DARPA vergleichbare Aufgaben wahrnehmen und sicherheitsrelevante innovative Projekte fördern soll.

Im Auftrag des BMI unterstützt das BSI das Bundesministerium für Bildung und Forschung (BMBF) zudem bei der Erstellung von sogenannten Forschungs-Calls. Das BSI war z. B. an der inhaltlichen Ausgestaltung des Forschungsprogramms der EU-Kommission „Horizon2020 – Secure societies“ für die Jahre 2018 bis 2020 und des Forschungsrahmenprogramms der Bundesregierung zur IT-Sicherheit „Selbstbestimmt und sicher in der digitalen Welt 2015-2020“ beteiligt.

Vertreter des BSI führen regelmäßig Fachgespräche mit den Forschungsstandorten der Cyber- und IT-Sicherheit in Deutschland, um sich zu neuesten Forschungsergebnissen auszutauschen. So wurden im letzten Jahr u. a. das CISPA und das Fraunhofer Institut für Nachrichtentechnik (Heinrich-Hertz-Institut, HHI, Berlin) besucht.

eFail-Schwachstellen in den Implementierungen von OpenPGP und S/MIME

Sachverhalt
Sicherheitsforscher der Fachhochschule Münster, der Ruhr-Universität Bochum sowie der Universität Leuven (Belgien) haben schwerwiegende Schwachstellen in den Implementierungen der weit verbreiteten E-Mail-Verschlüsselungsstandards OpenPGP und S/MIME gefunden und am 14. Mai 2018 unter https://efail.de/ veröffentlicht. Angreifer können demnach verschlüsselte E-Mails so manipulieren, dass der Inhalt der Nachricht nach der Entschlüsselung durch den Empfänger im Klartext an sie ausgeleitet wird. Der Titel der Forschungsarbeit ist allerdings irreführend, da die gefundenen Schwachstellen weniger die Standards als vielmehr deren Implementierung in den jeweiligen Mail-Clients betreffen. Dies führte im Anschluss an die Veröffentlichung zu Missverständnissen.

Ursache/Schadenswirkung
Zur Ausnutzung der Schwachstellen muss ein Angreifer Zugriff auf den Transportweg, den Mailserver oder das E-Mail-Postfach des Empfängers haben. Zusätzlich müssen auf Empfängerseite aktive Inhalte erlaubt sein, also etwa die Ausführung von HTML-Code und insbesondere das Nachladen externer Inhalte. Dies ist derzeit, insbesondere bei mobilen Geräten, in der Regel standardmäßig voreingestellt.

Reaktion
Das BSI war seit November 2017 durch das Forscherteam in den Prozess der sogenannten Coordinated Vulnerability Disclosure eingebunden. Koordiniert mit der Veröffentlichung der eFail-Schwachstellen hat das BSI daher seine nationalen und internationalen Partner, die Bundesverwaltung, die Bundesländer und zahlreiche KRITIS-Unternehmen über geeignete Maßnahmen zum sicheren Einsatz der E-Mail-Verschlüsselung informiert und Empfehlungen veröffentlicht.

Empfehlung
Die genannten E-Mail-Verschlüsselungsstandards können nach Einschätzung des BSI weiterhin sicher eingesetzt werden, wenn sie korrekt implementiert und sicher konfiguriert werden. Zur Zeit werden die Standards angepasst und mittelfristig von den jeweiligen Anwendungen implementiert. Die meisten Hersteller von E-Mail-Clients haben schon jetzt Maßnahmen gegen eFail auch gegen das direkte Ausleiten der Daten, also ohne Verschlüsselung, in ihren Produkten implementiert.

Das BSI empfiehlt grundsätzlich für mehr Sicherheit bei der E-Mail-Kommunikation auf die Darstellung und Erzeugung von E-Mails im HTML-Format zu verzichten. Insbesondere sollte die Ausführung aktiver Inhalte, also das Anzeigen von E-Mails im HTML-Format sowie das Nachladen externer Inhalte ausgeschaltet werden. So können Nutzer ein Ausspähen des E-Mail-Klartexts über die efail-Schwachstellen verhindern. Sofern ein E-Mail-Provider über die Einstellungen seiner Webmail-Anwendung dazu die Möglichkeit bietet, sollten auch hier entsprechende Maßnahmen umgesetzt werden. Unabhängig von speziellen Sicherheits-Updates schützt auch die sichere Konfiguration.

Die jeweiligen Hersteller erklären auf den folgenden Webseiten zudem, wie Nutzer bei gängigen E-Mail-Programmen das Nachladen externer Inhalte unterbinden können:

- Microsoft Outlook - Deaktivieren des automatischen Herunterladens von Bildern in E-Mail-Nachrichten https://support.office.com/de-de/article/Aktivieren-bzw-Deaktivieren-des-automatischen-Herunterladens-von-Bildern-in-E-Mail-Nachrichten-15e08854-6808-49b1-9a0a-50b81f2d617a
- Mozilla Thunderbird - Externe Inhalte in Nachrichten unterbinden https://support.mozilla.org/de/kb/externe-inhalte-nachrichten
- Apple Mail - Ein- oder Ausblenden nicht lokal verfügbarer Bilder https://support.apple.com/kb/PH4873?locale=de_DE

Unabhängig von den gefundenen Schwachstellen ist bei der Kommunikation mit dem E-Mail-Serviceprovider auf die Art der Verbindung und die ausgetauschten Daten zu achten. Wird z. B. Internet Message Access Protocol (IMAP) benutzt, werden Daten zwischen Server und Client auf dem Endgerät synchronisiert. Abhängig vom Mailclient und dessen Konfiguration kann nach der lokalen Entschlüsselung einer Mail eine dechiffrierte Kopie wieder an den Server hochgeladen und dort im Klartext gespeichert werden.

2.3.12 Soziale Netzwerke

Im März 2018 verschickten Kriminelle massenweise Nachrichten im Facebook-Messenger, die getarnt als Nachrichten von Facebook-Freunden einen Link zu einem angeblichen YouTube-Video enthielten. Folgte man einem solchen Link, landete man auf einer gefälschten Facebook-Anmeldeseite. Sobald ein Nutzer dort seine Anmeldedaten eingab, konnten die Kriminellen die Zugangsdaten abgreifen und somit den vollen Zugriff auf das Facebook-Konto des Opfers erhalten. Dazu gehörten u. U. auch die Facebook-Seiten, bei denen der eigentliche Inhaber des Facebook-Kontos Administrator-Rechte hatte.

Dieser Vorfall ist leider keine Ausnahme. Immer wieder nutzen Kriminelle die sozialen Netzwerke aus, um Nutzer auf bösartige Webseiten zu locken. Dort versuchen sie u. a. an die Zugangsdaten von Konten zu gelangen oder den Rechner mit Schadprogrammen zu infizieren.

Doch nicht nur Kriminelle sind an sensiblen Daten interessiert, auch dubiose Firmen versuchen personenbezogene Daten wie Adressen, Telefonnummern und Hobbys aus den sozialen Netzwerken abzugreifen, um beispielsweise gezielt Werbung zu schalten. Dabei nutzen sie die Möglichkeit, als App getarnt und mittels der Programmierschnittstelle des sozialen Netzwerks systematisch Daten aus dem persönlichen Profil zu analysieren.

Viele der aktuellen Gefährdungen in den sozialen Netzwerken basieren auf dem mangelnden Sicherheitsbewusstsein der Nutzer. Diese müssen die Gefährdungen besser kennen, um sich und die eigenen Daten zu schützen.

Um einen Schutz vor gestohlenen Passwörtern zu etablieren, sollten Nutzer von sozialen Netzwerken eine Zwei-Faktor-Authentisierung einsetzen. Dadurch erhalten Kriminelle trotz abgefangenem Passwort keinen Zugriff auf das Konto. Des Weiteren sollten Nutzer bei der Verwendung von Apps in sozialen Netzwerken hinterfragen, welche Zugriffsrechte man Apps einrichten möchte, um das Erheben von personenbezogenen Daten zu erschweren.

Im Allgemeinen sollten Links oder Kurz-Links in Facebook, Twitter oder anderen Diensten nur dann geöffnet werden, wenn sicher ist, dass sie aus einer vertrauenswürdigen Quelle stammen. Erscheinen solche Inhalte verdächtig, sollten Nutzer sich beim Absender rückversichern, ob z. B. die Nachricht wirklich von ihr bzw. ihm stammt.

2.4 Internationale Zusammenarbeit

Als nationale IT- und Cyber-Sicherheitsbehörde vertritt das BSI die nationalen Interessen in den Cyber-Sicherheitsgremien der EU und NATO und gestaltet Cyber-Sicherheit auch auf internationaler Ebene. Daneben galt es 2018, den Gestaltungs- und Wirkungskreis des BSI mittels besserer Vernetzung und Zusammenarbeit mit Akteuren aus Wirtschaft, Politik und Zivilgesellschaft auch international zu erweitern.

Europäische Union

Das Hauptaugenmerk des BSI-Engagements in der EU lag in den letzten beiden Jahren auf der Umsetzung der 2016 verabschiedeten NIS-Richtlinie. Diese ist seit Mai 2018 in allen Mitgliedsstaaten der EU rechtswirksam. Deutschland hatte auf Basis des 2015 verabschiedeten IT-Sicherheitsgesetzes bereits frühzeitig die Anforderungen der NIS-Richtlinie ins deutsche Recht überführt. Mit dieser Erfahrung unterstützt das BSI andere Mitgliedsstaaten bei der Umsetzung der NIS-Richtlinie in nationales Recht.

Bei der weiteren Ausgestaltung der NIS-Richtlinie hat das BSI aktiv mitgewirkt, insbesondere durch die themenübergreifende Mitarbeit in den beiden durch die Richtlinie neu geschaffenen Gremien auf europäischer Ebene:

- der NIS-Kooperationsgruppe und
- dem Cyber Security Incident Response Team (CSIRT)-Netzwerk.

Im CSIRT-Netzwerk wurden in einer Arbeitsgruppe unter Federführung des BSI die grundlegenden Standardverfahrensweisen bei signifikanten Cyber-Sicherheitsvorfällen entwickelt, die zukünftig als Basis für die Kommunikation und Kooperation zwischen den Mitgliedsstaaten dienen. Sie sind im Rahmen der Übung „Cyber Europe 2018“ erstmalig in einer europaweiten Übung zum Einsatz gekommen.

Im Rahmen der Kooperationsgruppe brachte das BSI in diversen Unterarbeitsgruppen seine Erfahrungen aus der Umsetzung des IT-Sicherheitsgesetzes ein, z. B. im Bereich der Identifizierung von Kritischen Infrastrukturen, bei der Ausgestaltung der Mindestanforderungen und Vorfallsmeldepflichten für Betreiber wesentlicher Dienste (Operators of essential services) und Anbieter digitaler Dienste (Digital service providers). Aktuell engagiert sich das BSI zudem in einer Arbeitsgruppe mit der Zielrichtung, die technische Sicherheit der Europawahlen 2019 zu gewährleisten und bringt dabei wesentliche Erfahrungen aus der Bundestagswahl 2017 ein.

Cisco Smart Install

Sachverhalt
Cisco Smart Install (SMI) ist eine Funktion zur automatischen Konfiguration von Cisco Netzwerk-Switches, die auf neuen Geräten standardmäßig aktiviert ist. SMI sieht keinen Zugriffschutz vor, eine Authentifizierung ist nicht erforderlich. Der Zugriff auf SMI sollte daher nur von vertrauenswürdigen Netzen aus und keinesfalls offen aus dem Internet erlaubt werden.

Ursache/Schadenswirkung
Das CERT-Bund des BSI warnte bereits im Februar 2017, dass Angreifer mit Zugriff auf die Smart-Install-Funktion eines Cisco-Switches diese Bund 2017 missbrauchen können, um sensible Informationen auszuspähen und ggf. die vollständige Kontrolle über das Gerät zu erlangen https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k17-0274.htm.

Im August 2017 wurde bekannt, dass Cyberkriminelle die offen aus dem Internet erreichbare SMI-Funktion auf Cisco-Geräten bei verschiedenen australischen Organisationen ausnutzten, um Konfigurationsdateien der Geräte auszulesen https://acsc.gov.au/news/routers-targeted.html.

Im November wurden hunderte weiterer Konfigurationsdateien entdeckt, die nach Presseberichten zuvor von Cyberkriminellen auf betroffenen Geräten in aller Welt ausgespäht wurden.

Anfang April 2018 nutzten Cyberkriminelle den offenen Zugriff auf SMI-Funktionen, um tausende Cisco-Switche in verschiedenen Ländern zu kompromittieren. In Russland und dem Iran wurden betroffene Geräte von den Angreifern gezielt außer Betrieb gesetzt. Als Folge dieser Angriffe waren viele größere Netzbereiche in diesen Ländern für mehrere Stunden vom Internet abgeschnitten.

Reaktion
CERT-Bund informiert seit Anfang November 2017 deutsche Netzbetreiber/Provider regelmäßig zu Cisco-Geräten mit aktiver Smart-Install-Funktion in ihren Netzen, welche offen aus dem Internet erreichbar sind. Die Anzahl betroffener Geräte ist seitdem drastisch zurückgegangen, von über 6000 am 1. November 2017 auf gut 400 am 30. April 2018.

Abbildung 20 Anzahl von Cisco-Geräten mit offen aus dem Internet erreichbarer Smart-Install-Funktion in Deutschland

Empfehlung
Der Zugriff auf die Smart-Install-Funktion (Port 4786/tcp) sollte grundsätzlich auf vertrauenswürdige Quell-IP-Adressen (z. B. das interne Administrationsnetz) eingeschränkt werden. Nach der Konfiguration eines neuen Gerätes sollte die SMI-Funktion deaktiviert werden, wenn diese nicht weiter benötigt wird. Weiterhin sollte die Konfigurationsanleitung des Herstellers zu SMI https://www.cisco.com/c/en/us/td/docs/switches/lan/smart_install/configuration/guide/smart_install/concepts.html beachtet werden.

Einen weiteren zentralen Baustein des BSI-Engagements in der EU bildet die Zusammenarbeit mit der European Union Agency for Network and Information Security (ENISA), dessen neues Mandat aktuell zwischen den Mitgliedsstaaten, dem Europäischen Parlament und der Kommission als Teil des „Cybersecurity Acts" verhandelt wird. Der BSI-Präsident ist der deutsche Vertreter im Management Board, daneben stellt das BSI den deutschen ENISA-Verbindungsbeamten (National Liaison Officer). Zudem arbeiten BSI-Fachexperten kontinuierlich in diversen Expertengruppen der ENISA mit.

Mit der Neuregelung der gesetzlichen Grundlage der ENISA soll der langjährigen Forderung des BSI nach einem permanenten Mandat gefolgt werden. Sie bildet die Basis für eine weitere Intensivierung der Zusammenarbeit mit den Cyber-Sicherheitsbehörden der Mitgliedsstaaten. Dabei gilt, dass Cyber-Sicherheit in nationaler Verantwortung liegt und ENISA die EU-Institutionen und Mitgliedsstaaten beraten und unterstützen kann. Ein Beispiel sind die neu zu definierenden Aufgaben der ENISA im Rahmen des geplanten europäischen Zertifizierungs-Frameworks für die IKT-Sicherheitszertifizierung als weiterer Bestandteil des „Cybersecurity Acts". Das BSI verfügt im Bereich der Zertifizierung über eine maßgebliche Expertise in der EU und wurde 2017 und 2018 durch den BSI-Vizepräsidenten bei den Sitzungen des für den „Cybersecurity Act" federführenden Ausschusses für Industrie, Forschung und Energie (ITRE) des Europäischen Parlaments als einziger Vertreter einer nationalen Behörde angehört.

Mit Fokus auf das geplante europäische Zertifizierungs-Framework ist es für das BSI zentral, die Reichweite des europäischen Anerkennungsabkommens SOGIS-MRA als europäisches Zertifizierungsinstrument insbesondere für den Bereich der Hochsicherheit auszubauen, um Cyber-Sicherheit national und international gestalten zu können.

NATO

Die Aktivitäten des BSI als nationale Cyber-Sicherheitsbehörde sind ein entscheidender Beitrag des deutschen Engagements in der NATO. Als nationale Kommunikationssicherheitsbehörde, Cyber-Sicherheitsbehörde sowie Zulassungsstelle für Kryptoprodukte ist das BSI für die NATO ein zentraler Ansprechpartner in Sachen Information Assurance und Cyber Defence. Es vertritt Deutschland durch aktive sowie beratende Mitarbeit in den wichtigsten technischen und politischen NATO-Gremien in den Bereichen Informations- und Cyber-Sicherheit.

Das Thema Cyber Defence ist in den vergangenen Jahren in der NATO zunehmend wichtiger geworden. Auf dem NATO-Gipfel von Warschau 2016 beschlossen die Staats- und Regierungschefs der Mitgliedstaaten den sog. „Cyber Defence Pledge". Damit hat sich auch Deutschland verpflichtet, seine nationalen Widerstandsfähigkeiten im Cyber-Bereich beständig zu erhöhen, um somit seinen Teil zur Verteidigungsfähigkeit des Bündnisses zu leisten. Dieser Beschluss wird nun in konkrete Maßnahmen umgesetzt.

Das Jahr 2017 war geprägt durch die Operationalisierung von Cyber als NATO-Operationsraum, um die Allianz und ihre Mitgliedstaaten im Cyber-Raum voll handlungsfähig zu machen. Das BSI übt seit Unterzeichnung des Memorandums of Understanding (MoU) mit der NATO im Jahr 2011 und der Bestätigung des MoUs im Jahr 2016 für Deutschland die Funktion als „National Cyber Defence Authority" (NCDA) bei der NATO aus. Es ist in enger Zusammenarbeit mit den zuständigen Ministerien BMI, Bundesministerium für Verteidigung (BMVg) und Auswärtiges Amt (AA) in diesen Prozess eingebunden und leistet damit einen entscheidenden Beitrag zur Sicherheit und Verteidigung Deutschlands.

Im März 2018 wurde Thomas Caspers, Fachbereichsleiter für Evaluierung und Betrieb von Kryptosystemen im BSI, zum nationalen Co-Chair des NATO Cyber Defence und Information Assurance Capability Panels gewählt. In dieser Funktion wird er sich auf die Weiterentwicklung der Kommunikations- und Managementprozesse in der Allianz, auf das Vorantreiben der dringend erforderlichen Kryptomodernisierung der NATO-Streitkräfte sowie auf die Vertiefung der Kooperation von NATO und EU konzentrieren. Dass sich die überwiegende Mehrheit der NATO-Nationen für einen BSI-Mitarbeiter ausgesprochen hat, zeigt das große Vertrauen der Alliierten in die Arbeit des BSI und spiegelt gleichzeitig die große Verantwortung des BSI gegenüber der NATO wider.

Facebook-Löschaktion

Sachverhalt
Facebook hat am 3. April 2018 zahlreiche Konten und Seiten auf seinen Social-Media-Plattformen Facebook, WhatsApp und Instagram gelöscht, die der Russian Internet Research Agency (IRA) zugeordnet wurden. Die Russian IRA ist eine russische, vermutlich staatlich geförderte sogenannte Trollfabrik, die massenweise nicht-authentische Inhalte in sozialen Netzwerken verbreitet sowie Fake-Accounts einsetzt. Die betroffenen Seiten, insbesondere eine Seite namens IRA Open, sind größtenteils russischsprachig und verbreiten Falschinformationen bzw. Inhalte, die die öffentliche Meinung im Sinne der russischen Regierung beeinflussen sollen. In Deutschland wurde diese Seite von 8.580 Personen geliked. Davon haben etwa 1.300 Personen diese Seite auch aktiv gelesen. Zählt man alle betroffenen Konten, Seiten und Werbebanner zusammen, die solche Inhalte verbreitet haben, sollen laut Facebook rund eine Million Seitenaufrufe zusammengekommen sein.

Ursache/Schadenswirkung
Die großen US-amerikanischen Betreiber sozialer Netzwerke, u. a. Facebook, Twitter und Tumblr, hatten in der jüngeren Vergangenheit öfter über russische Aktivitäten berichtet, die eine Beeinflussung der US-Präsidentschaftswahl zum Ziel gehabt hätten.

Im September 2017 teilte Facebook mit, mutmaßlich russische Akteure hätten zwischen Juni 2015 und Mai 2017 annähernd 100.000 US-Dollar für Werbung zur Verbreitung von Falschinformationen auf Facebook ausgegeben.

Anfang 2018 gab Twitter bekannt, fast 4.000 Nutzerkonten mit Verbindungen zur Russian IRA zehn Wochen vor der US-Präsidentschaftswahl identifiziert zu haben. Von diesen seien ca. 180.000 Tweets gepostet worden, davon 8,4 Prozent mit Bezug zur US-Wahl. Man habe 13.500 automatisierte Konten (sogenannte Social Bots) mit Verbindungen zu Russland identifiziert werden, die automatisiert Tweets mit Bezug zur US-Wahl abgesetzt hätten.

Der Blogging-Anbieter Tumblr gab im März 2018 bekannt, ebenfalls 84 Konten mit Verbindungen zur Russian IRA identifiziert zu haben. Die Akteure hätten hier nicht auf Bots oder Werbung gesetzt, sondern diffamierten über reguläre Posts offenbar insbesondere US-Präsident Trumps damalige Gegenkandidatin Hillary Clinton.

Einen Bezug oder eine Beeinflussung der Bundestagswahl 2017 durch die betroffenen Konten wurde nicht beobachtet.

Reaktion
Das BSI steht mit den Anbietern sozialer Netzwerke in Kontakt, um regelmäßig Informationen über die Sicherheit von Accounts auszutauschen. Dazu wurde beispielsweise ein direkter Kommunikationskanal zu Facebook eingerichtet, um potenzielle Sicherheitsvorfälle (z. B. Unregelmäßigkeiten bei Accounts von politischen Entscheidungsträgern) an das Sicherheits-Team von Facebook eskalieren zu können. Des Weiteren hat Facebook zugesagt, das BSI zukünftig über Aktionen (z. B. Löschung von Accounts, die nicht-authentische Inhalte verbreiten) vorab zu informieren.

Empfehlung
In den sozialen Netzwerken existieren neben herkömmlichen Accounts auch sogenannte verifizierte Accounts. Solche verifizierte Accounts sind mit einem weißen Haken auf blauem Grund („blue badge“) gekennzeichnet und bestätigen die Echtheit eines Kontos. Nutzer von sozialen Netzwerken können so erkennen, ob ein entsprechender Account tatsächlich der angegebenen Person (z. B. einem Politiker, einer Partei oder einer Fraktion) gehört. Darüber hinaus sind Nutzer angehalten, Inhalte aus den sozialen Netzwerken stets kritisch zu hinterfragen.

2.4.1 Kryptografie: internationale Standardisierung

Aufgrund der Bedrohung der Public-Key-Kryptografie durch mögliche künftige Quantencomputer ist eine Standardisierung neuer kryptografischer Verfahren, die gegen diese Bedrohung sicher sind (sogenannter Post-Quanten-Kryptografie), dringend erforderlich. Das amerikanische National Institut for Standards and Technology (NIST) hat im November 2016 einen Standardisierungsprozess gestartet, an dessen Ende eine Auswahl von Verfahren zur Schlüsseleinigung, Verschlüsselung und Signatur zur Verfügung stehen soll. Bis Ende November 2017 konnten beim NIST Vorschläge für solche Verfahren eingereicht werden. Inzwischen sind noch 64 Kandidaten im Rennen, 19 Signaturverfahren und 45 Schlüsseltransport- bzw. Verschlüsselungsverfahren. Einen guten Überblick liefert die Seite www.safecrypto.eu/pqclounge/.

Aber auch andere Organisationen wie die Internet Engineering Task Force (IETF) und die Internationale Organisation für Normung (ISO) haben mit der Standardisierung von Post-Quanten-Kryptografie begonnen. Die IETF beschäftigt sich zudem mit der Anpassung kryptografischer Protokolle wie TLS und IKE an die neuen Verfahren, z. B. mit der Möglichkeit, einen „hybriden" Schlüsselaustausch (Kombination eines klassischen Verfahrens mit einem Post-Quanten-Verfahren) durchzuführen. Besonders aktiv ist auch das Europäische Institut für Telekommunikationsnormen (ETSI), sowohl in Richtung von Quantenkommunikation (Quantum Key Distribution, QKD) als auch in Richtung Post-Quanten-Kryptografie (dort Quantum-Safe Cryptography genannt). Die Arbeitsgruppe zu Quantum-Safe Cryptography des ETSI Technical Committees Cyber hat bereits einige Übersichtspapiere (beispielsweise zu Verfahren zur Schlüsseleinigung) veröffentlicht. An den Treffen dieser Gruppe nehmen auch Vertreter des BSI teil.

Ein wichtiger Faktor zur Erhöhung der IT-Sicherheit ist es, ein einheitliches Sicherheitsniveaus auf internationaler Ebene abzustimmen sowie gemeinsame Standards und Prüfkriterien festzulegen. Auch Hersteller profitieren davon, wenn ihre Produkte durch Einhaltung von Standards und vergleichbaren Vorgaben auf einem breiten Markt angeboten werden können. Das BSI befindet sich zu diesem Zweck beim Thema Kryptografie im Austausch mit internationalen Partnern und beteiligt sich an der Entwicklung von Standards wie bspw. ISO-20543 „Test and analysis methods for random bit generators", um für diese neuen Verfahren einheitliche Sicherheitsniveaus und Prüfkriterien international zu etablieren. Erwähnenswert ist in diesem Zusammenhang zudem die vom NIST begleitete Standardisierung von Post-Quanten-Kryptografie sowie die Standardisierung von TLS 1.3.

Nationale Empfehlungen bzw. Vorgaben zu Verschlüsselungsalgorithmen und Protokollen, wie beispielsweise die Technische Richtlinie TR-02102 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen" des BSI, sowie beauftragte Studien, wie die Daueruntersuchung des Linux-Zufallszahlengenerators, werden vom BSI auf der Webseite veröffentlicht und auch in englischer Sprache angeboten, um sie einer internationaler Leserschaft zugänglich zu machen.

2.5 Cyber-Sicherheit braucht IT-Fachkräfte

Die Bemühungen um eine zuverlässige Cyber-Abwehr können nur gelingen, wenn genügend Expertinnen und Experten sowie talentierte Nachwuchskräfte rekrutiert werden, die Cyber-Sicherheit aktiv gestalten und in den Köpfen verankern. Deswegen wurde dem BSI für die Erfüllung seiner Aufgaben im Jahr 2017 180 neue Stellen zugesprochen. Diese in Zeiten des Fachkräftemangels zu besetzen, stellte eine besondere Herausforderung dar, die jedoch erfolgreich bewältigt werden konnte. Zum Ende des Berichtszeitraums waren fast alle Stellen besetzt. Zwei Herausforderungen wurden im Kern deutlich:

- einerseits die Gewinnung der stark umworbenen IT-Fachkräfte,
- andererseits die Einarbeitung und Integration der gewonnenen Kollegen und Kolleginnen.

Dem Aufwuchs von 180 Stellen stand eine Mitarbeiterzahl von circa 650 Personen gegenüber, folglich war auch ein spürbarer Einfluss auf die Struktur und Kultur des Hauses unvermeidbar.

Der öffentliche Dienst macht MINT: Gewinnung von Fachkräften

Nachdem bereits zu Anfang des Jahres das Karriereportal sowie die Kampagnenlinie „Was wir wollen: Deine digitale Seite“ neu entwickelt wurden, fanden im Berichtszeitraum vor allen Dingen Maßnahmen statt, um die Kampagne mit Leben zu füllen. Dabei sollte unterstrichen werden, dass das BSI für seine Mitarbeiterinnen und Mitarbeiter und ihre herausfordernde und gesellschaftlich bedeutsame Tätigkeit ideale und verlässliche Rahmenbedingungen schafft. Dazu gehören auch die vielfältigen Möglichkeiten, die Arbeit familienfreundlich und flexibel zu gestalten. Darüber hinaus sollte gezeigt werden, dass die Behörde ein sehr attraktiver Arbeitgeber ist, der bundesweit und international einen exzellenten Ruf genießt und bei dem zukunftsweisende Sicherheitsprojekte zum Arbeitsalltag gehören. Neben einem spannenden Arbeitsumfeld bietet das BSI seinen Mitarbeiterinnen und Mitarbeitern auch ein umfassendes Trainings- und Weiterbildungsprogramm. Dazu kommen internationale Projektarbeit und Konferenzen sowie der regelmäßige Austausch mit führenden deutschen und internationalen Sicherheitsexperten. Außerdem eröffnen sich den Mitarbeiterinnen und Mitarbeitern erstklassige Vernetzungsmöglichkeiten in Politik, Wirtschaft und Verwaltung.

Um die Kampagne zu bewerben, setzte das BSI auf seine Beschäftigten, die in Wort, Bild und Ton die Arbeitgebermarke präsentieren. Über Online-Kanäle, Printanzeigen, redaktionelle Beiträge online und in Zeitschriften, Videos und Broschüren konnten diese Botschaften transportiert werden. Weiterhin wurde über Hochschulmessen, Exkursionen ins BSI, Praktika und die Betreuung von Abschlussarbeiten der direkte Kontakt zu Studierenden der MINT-Fächer gesucht, so dass sich die nationale Cyber-Sicherheitsbehörde als der ideale Arbeitgeber für den Berufseinstieg empfehlen konnte.

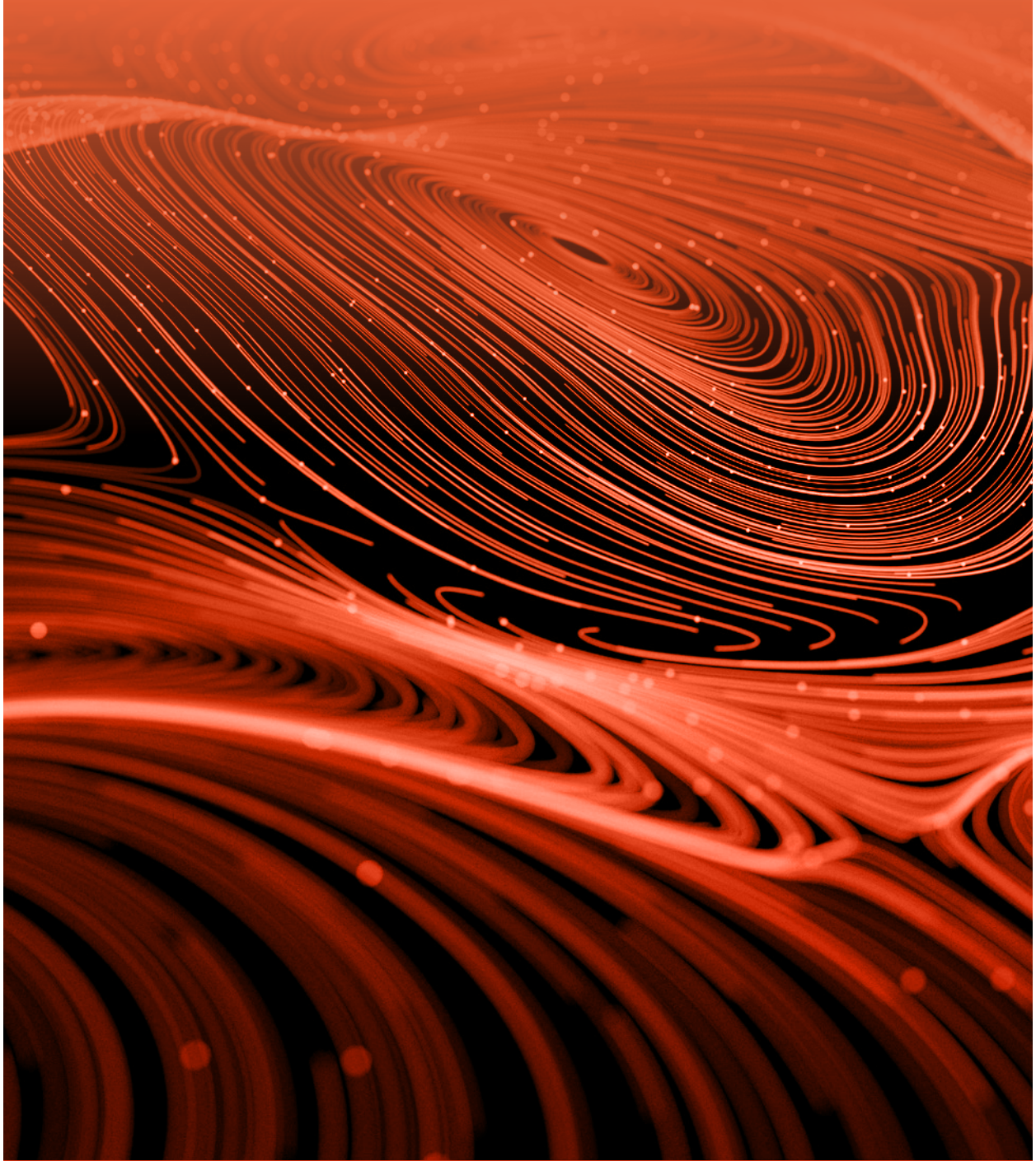
Die umfangreichen Maßnahmen sowie der vollständig digitalisierte Bewerbungsprozess führten im Jahr 2017 zu einer Erhöhung der Bewerberzahlen um ca. 47 Prozent sowie zu der sehr guten Stellenbesetzung. Es wurde bewiesen, dass trotz häufig betonter Probleme bei der Gewinnung von IT-Fachkräften auch der öffentliche Dienst in der Lage ist, sich als attraktiver Arbeitgeber gegenüber Wirtschaft und Forschung zu behaupten.

Mit seiner Personalarbeit setzt das BSI im öffentlichen Bereich Maßstäbe: Auf dem diesjährigen Zukunftskongress Staat & Verwaltung in Berlin gewann das BSI für das Projekt „Gewinnung, Einarbeitung und Bindung von mehr als 260 neuen Mitarbeitern seit 2016“ im eGovernment-Wettbewerb zum Thema Digitalisierung und Modernisierung der öffentlichen Verwaltung den zweiten Platz.

Viele neue Gesichter: Einarbeitung und Integration

Um die neuen Mitarbeiterinnen und Mitarbeiter in das BSI zu integrieren, wurden verpflichtende Einführungsveranstaltungen mit verschiedenen Modulen initiiert. Diese sollen sowohl die Fachaufgaben in den unterschiedlichen Bereichen allen Mitarbeitenden näher bringen und somit einen Blick für das große Ganze erzeugen, als auch Verwaltungsgrundlagen für die MINT-Fachkräfte vermitteln, die oftmals noch keine Berührungspunkte mit diesen Anforderungen hatten. Weiterhin wurden Inhouse-Schulungen zu grundsätzlichen Themen wie Projektmanagement, Präsentation, Resilienz, Konfliktmanagement, Zeitmanagement, Kommunikation und Kooperation, Verhandlungsführung und Stressmanagement angeboten. Hierin spiegeln sich unterschiedliche überfachliche Anforderungen an neue und erfahrenere Mitarbeiterinnen und Mitarbeiter wider. Somit wird vor allem die bereichsübergreifende Kooperation und Zusammenarbeit forciert, aber auch die BSI-spezifische Vorgehensweise vermittelt (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.

3 Gesamtbewertung und Fazit



3 Gesamtbewertung und Fazit

Gefährdungslage weiterhin hoch

Die Gefährdungen sind im Berichtszeitraum im Vergleich zum vorangegangenen Berichtszeitraum vielfältiger geworden. Ein Beispiel dafür sind die Hardware-Sicherheitslücken wie *Spectre*/*Meltdown* und *Spectre* NG, die zu Beginn dieses Jahres bekannt geworden sind.

Im Jahr 2018 sind neue große Ransomware-Wellen ausgeblieben. Trotzdem muss Ransomware weiterhin als massive Gefährdung eingestuft werden. Dies zeigen die Angriffe in der zweiten Jahreshälfte 2017 mit der Ransomware *Petya*/*NotPetya*: Sie verursachten allein in der deutschen Wirtschaft Schäden in Millionenhöhe. Auch werden immer neue Ransomware-Familien bekannt wie z. B. Bad Rabbit im Oktober 2017. Im Bereich der Ransomware besteht kein Anlass für eine Entwarnung.

Insgesamt ist die Anzahl an Schadprogrammen weiter gestiegen: Es gibt über 800 Millionen bekannte Schadprogramme. Pro Tag kommen rund 390.000 neue Varianten hinzu. Im Mobil-Umfeld gibt es bereits mehr als 27 Millionen Schadprogramme allein für Google Android.

Auch die Wege zur massenhaften Verteilung von Schadsoftware wurden weiterentwickelt. So wurde 2017 in mehreren Vorfällen (z. B. bei *NotPetya*) Schadsoftware durch die Kompromittierung von Updates, Update-Dateien oder Update-Servern verteilt (Installations- oder Update-Hijacking).

Bekannte Schadsoftware-Familien werden fortlaufend verändert, weiterentwickelt und mit zusätzlichen Schadfunktionen ausgestattet. Seit September 2017 fällt die Malware Emotet durch häufige Attacken in Deutschland auf. Emotet begann 2015 als Banking-Trojaner und wurde inzwischen zu einer vielgestaltigen Malware mit beliebig nachladbaren Modulen für Spam, DDoS, Datenausspähung, Identitätsdiebstahl, Sandbox-Detektion sowie anderen Malware-Komponenten weiterentwickelt.

Auch die Evolution von IoT-Botnetzen geht weiter; neue Botnetze wie Hajime und IoT_reaper/IoTroop haben nicht die Bedeutung des *Mirai*-Botnetzes erlangt. Wegen des schnellen Zuwachses an verwundbaren IoT-Geräten und Mobilgeräten sind allerdings neue große Botnetze für wirkungsvolle Angriffe (Spam, DDoS usw.) zu erwarten. Als Erfolg konnte im Dezember 2017 verzeichnet werden, dass unter Mitwirkung des BSI das globale Andromeda-Botnetz vom Netz genommen wurde. Es hatte zuvor Schadsoftware wie Banking-Trojaner auf Millionen von Rechnern verteilt.

Bei der Anzahl der offenen kritischen Software-Schwachstellen gab es im Vergleich zum vorangegangenen Berichtszeitraum nur geringe Veränderungen.

Aufgrund des Umfangs der Credential-Leaks und der Gefährdungen durch fehlkonfigurierte Cloud-Dienste gibt es auch bei Spam und Phishing keine Entspannung der Sicherheitslage. Die Masse der verfügbaren Credentials erlaubt gezieltere und personalisierte IT-Angriffe.

Die bekannt gewordenen Identitätsdiebstähle erreichen quantitativ immer neue Größenordnungen. Auf dem IT-Schwarzmarkt werden zunehmend Datenkollektionen gehandelt, es handelt sich um Milliarden erbeuteter digitaler Identitäten.

Obgleich es wirkungsvolle Techniken am Markt gibt, DDoS-Angriffe abzuwehren, ist die Bedrohungslage aufgrund der hohen Mitigationskosten und neuen Angriffstechniken („memcached Amplification“) nach wie vor hoch. Im zweiten Halbjahr 2017 gab es zunächst jedoch keine signifikante Erhöhung der eingesetzten Angriffskapazitäten, typisch waren Spitzenwerte von 50 bis 60 Gbit/s. Im ersten Quartal 2018 wurden jedoch DDoS-Angriffe mit bis zu 190 Gbit/s in Deutschland detektiert. Ein Zusammenhang mit dem Missbrauch der Server-Software memcached als DDoS-Reflection-Vektor ist sehr wahrscheinlich.

Anfang Januar 2018 wurden schwerwiegende und grundlegende Sicherheitslücken in der Hardware-Architektur bei fast allen Prozessoren von Intel, ARM, AMD entdeckt. Es handelt sich hier um eine neue Klasse von Schwachstellen (*Meltdown*/*Spectre*) aufgrund von Design-Fehlern in der Prozessor-Architektur. Die Sicherheitslücken können durch Updates nicht vollständig geschlossen werden. Ein Austausch aller betroffenen Prozessoren ist ebenfalls nicht realistisch. Für einen nicht einzugrenzenden Zeitraum verbleibt deshalb ein Restrisiko, dass die Schwachstellen ausgenutzt werden. Es handelt sich hierbei um eine neue Gefährdung für virtuelle Strukturen, z. B. bei Cloud-Angeboten.

Auch illegales Krypto-Mining ist neu hinzugekommen. Aufgrund der hohen finanziellen Attraktivität und der Unauffälligkeit der Infektionen ist es als signifikant zunehmendes Cyber-Risiko zu bewerten. Die registrierten Vorfälle haben ab dem zweiten Halbjahr 2017 sowohl an Zahl als auch an Intensität zugenommen. In mehreren Fällen ist zu beobachten, dass die Verwendung von derzeit bekannten Infrastrukturen (z. B. Botnetze und Exploit-Kits) auf die Distribution von Krypto-Currency-Mining-Malware erweitert wird.

Der zusammenfassende Überblick zeigt, dass die Gefährdung im Vergleich zum vorangegangenen Berichtszeitraum keinesfalls zurückgegangen ist, sondern sogar etwas zugenommen hat. Sie ist vielschichtiger geworden, was den Aufwand für den Schutz erhöht. Es gibt nach wie vor eine hohe Dynamik der Angreifer bei der Weiterentwicklung von Schadprogrammen und Angriffswegen, was hohe Aufmerksamkeit und Flexibilität zur Gewährleistung der Informationssicherheit erfordert. Und es gibt eine neue Qualität von Schwachstellen in Hardware, die ohne einen Austausch der Hardware nicht vollständig geschlossen werden können.

Digitalisierung erst am Anfang

Gleichzeitig befinden wir uns erst am Anfang einer Ära der Digitalisierung, die unseren Alltag und unsere Gesellschaft umfassend beeinflussen wird. Angriffe und Gefährdungen, die Staat, Wirtschaft und Gesellschaft schon heute vor extreme Herausforderungen stellen, werden in einer digitalisierten und vernetzten Welt weiter zunehmen. Ohne entsprechende Anstrengungen, das notwendige Maß an Informationssicherheit durch Prävention, Detektion und Reaktion zu gewährleisten, werden Staat, Wirtschaft und Gesellschaft in Deutschland zunehmend gefährdet.

Das Problem liegt in der Kombination von wachsender Gefährdung mit zunehmender Abhängigkeit von Informationstechnik. Die Wahrscheinlichkeit für den Erfolg von Angriffen auf digitalisierte Infrastrukturen steigt, da sich die Anzahl der Angriffspunkte erhöht, die Kommunikationsinfrastrukturen immer komplexer werden und die zu verarbeitenden Datenmengen sich vervielfachen. Relevante Sicherheitsvorfälle aus dem Berichtszeitraum zeigen dies in aller Deutlichkeit:

- Trotz aller Maßnahmen, die dazu führen, dass die IT-Netze und -Systeme der Bundesregierung als besonders gesichert gelten, kam es 2017 zu einem erfolgreichen Hackerangriff. Der Angriff erfolgte über einen Webserver der Bundesakademie für öffentliche Verwaltung. Betroffen waren das Auswärtige Amt und die Hochschule des Bundes. Das BSI konnte den Cyber-Angriff auf das Auswärtige Amt durch den Einsatz eines Mobile Incident Response Teams (MIRT) über längere Zeit beobachten und so tiefere Einsichten in Absicht und Vorgehensweise der Täter erlangen. Größerer Schaden oder eine weitere Ausbreitung konnten dank bestehender Schutzmaßnahmen verhindert werden.

- Im Mai 2017 drangen Hacker in das Netz eines Tochterunternehmens eines deutschen Energieversorgers ein. Sie hatten für einen Zeitraum von wenigen Minuten Zugriff auf einen geringen Teil des Internetverkehrs. Der Vorfall wurde vom BSI im Rahmen des Nationalen Cyber-Abwehrzentrums in Zusammenarbeit mit dem betroffenen Unternehmen analysiert und bearbeitet. Dem BSI liegen Informationen vor, die belegen, dass deutsche KRITIS-Betreiber verstärkt im Fokus ausländischer Cyber-Angriffe stehen und so mit einer veränderten Bedrohungslage rechnen müssen.

- Hardware-Sicherheitslücken wie *Spectre/Meltdown* und *Spectre* NG haben das Potenzial, aktuelle Geschäftsmodelle und grundlegende IT-Sicherheitskonzepte obsolet zu machen. Die betroffenen Chips sind millionenfach verbaut und bilden eine Grundlage moderner Computers. Da es sich um Schwachstellen in der Hardware handelt, können Softwareupdates nur unzulänglich bzw. unzureichend Abhilfe schaffen. Um die betroffenen Chips auszutauschen, müssen zunächst vergleichbare Produkte, die nicht von Schwachstellen betroffen sind, neu entwickelt werden. Bis dahin bleibt die Schwachstelle akut bestehen, auch wenn ihre Ausnutzung sehr aufwändig ist und somit ein Einsatz als Angriffsmethode nur in besonderen Fällen zu erwarten ist.

Diese Vorfälle – als Beispiele für das Gefährdungspotenzial und die Angriffsvarianz – machen deutlich, dass die Cyber-Sicherheit in der Digitalisierung noch stärker betrachtet und beachtet werden muss. Die Sicherheitsarchitektur von computergestützten Arbeitsplätzen und Unternehmensabläufen muss ebenso grundlegend neu gedacht werden wie die IT-Sicherheit von Produkten und Dienstleistungen. Dabei muss die Sicherheit der eingesetzten Systeme in der staatlichen Verwaltung, in der Wirtschaft und beim Endanwender durch „security by design“ und „security by default“ von vornherein gewährleistet sein. Deutschland muss in dieser Frage eine Vorreiterrolle einnehmen.

Wenn es auch in Zukunft einen starken und sicheren Standort Deutschland geben soll, muss mehr in Informations- und Cyber-Sicherheit investiert werden.

Abwehr-Anstrengungen verstärken

Das BSI verfügt schon heute auf der Basis seiner technisch tiefgehenden Expertise über eine integrierte Wertschöpfungskette von der Beratung über die Entwicklung sicherheitstechnischer Lösungen, die Abwehr von Angriffen auf die Cyber-Sicherheit bis zur Standardisierung und Zertifizierung. Als die nationale Cyber-Sicherheitsbehörde gestaltet es für alle Akteure in allen Bereichen die Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion.

In dieser Funktion ist das BSI gefordert, sowohl auf Schwachstellen hinzuweisen als auch neue Lösungen zu konzipieren und umzusetzen.

- Das Internet der Dinge entwickelt sich immer mehr zu einer neuen Gefahrenquelle für die IT-Sicherheit. Dazu trägt entscheidend bei, dass IoT-Geräte einfach angreifbar sind und deren Sicherheit weder bei der Herstellung noch bei der Kaufentscheidung des Kunden eine ausreichende Rolle spielt. In Umsetzung der Cyber-Sicherheitsstrategie der Bundesregierung und des Koalitionsvertrags der 19. Legislaturperiode arbeitet das BSI an der Einführung eines IT-Sicherheitskennzeichens, um zukünftig Verbrauchern die Einschätzung zur IT-Sicherheit von IT-Produkten und -Services zu erleichtern. Ein wichtiger Schritt hierbei ist die Technische Richtlinie für Router, die das BSI derzeit gemeinsam mit der Wirtschaft erarbeitet hat.

- eFail-Schwachstellen ermöglichen Angreifern das Auslesen verschlüsselter E-Mails. Dadurch hat das Vertrauen in verschlüsselte Kommunikation abgenommen. Deutschland muss verschlüsselte Kommunikation für die Bürger und zum Schutz von Unternehmensgeheimnissen endlich massentauglich machen. Dazu braucht es eine Initiative von zentraler Stelle, die diesen Prozess vorantreibt und begleitet. Das BSI mit der Allianz für Cybersicherheit wird diese Aufgabe übernehmen.

- Vorfälle und Schwachstellen wie *WannaCry*, NotPetya, eFail und *Spectre* erschüttern die Grundfesten der weltweiten IT-Sicherheitsarchitekturen und heben die Gefährdungslage im Cyber-Raum auf eine neue Ebene. Deshalb ist es erforderlich, dass die notwendigen Sicherheitsmaßnahmen durch unabhängige Stellen überprüft werden und dass für Hersteller und Anbieter Melde- und Transparenzpflichten gegenüber dem BSI geschaffen werden.

- Betreiber Kritischer Infrastrukturen sind verstärkt im Fokus von Cyber-Angriffen. Das BSI arbeitet intensiv mit der KRITIS-Wirtschaft zusammen, um Schutzmaßnahmen zu verbessern und Cyber-Angriffe abzuwehren. Aus der Umsetzung des IT-Sicherheitsgesetzes und vor dem Hintergrund der aktuellen Bedrohungslage wird aber deutlich, dass für es dringend einer Fortschreibung bedarf, um weitere Teile der Wirtschaft weiterhin effektiv zu schützen und das Sicherheitsniveau deutlich erhöhen zu geschaffen werden.

Prävention weiter denken

So wichtig die Abwehr konkreter Angriffe gleich welcher Herkunft aus dem Cyber-Raum auch ist, so darf sie doch nicht das grundsätzliche Anliegen in den Hintergrund drängen: durch präventive Maßnahmen potenzielle Angreifer bereits von einem Angriffsversuch abzuhalten bzw. Angriffe ins Leere laufen zu lassen.

Dafür bedarf es sowohl der Weiterentwicklung des Rechtsrahmens als auch der zwischen Bund und Ländern und mit der Wirtschaft abgestimmten Entwicklung von Sicherheitsstandards für die IT-Strukturen und den Schutz der Kritischen Infrastrukturen. Dazu zählt auch die IT-Sicherheitsforschung, indem sie einerseits die Sicherheit der IT-Systeme von morgen behandelt, sich aber in mindestens gleichem Maße um die Sicherheit der bereits vorhandenen Informationstechnologien kümmert. Neben den bestehenden Kompetenzzentren für IT-Sicherheitsforschung trägt auch das BSI schon heute zur digitalen Souveränität Deutschlands bei.

Prävention meint immer, einerseits die Hürden für einen Angriff zu erhöhen, zum anderen aber die Akteure in Staat, Wirtschaft und Gesellschaft zu befähigen, Gefahren besser zu erkennen und sich abwehrbewusster zu verhalten. Eine gewichtige Rolle in der Prävention spielt deshalb der Digitale Verbraucherschutz. Nach dem Koalitionsvertrag soll er als zusätzliche Aufgabe des BSI etabliert werden. Das BSI bietet bereits seit vielen Jahren mit dem Konzept „BSI für Bürger“ Informations- und Unterstützungsangebote für die Bevölkerung an. Nun wird das BSI gemeinsam mit etablierten Akteuren aus dem Verbraucherschutz (u. a. Verbraucherzentrale NRW, Verbraucherzentrale Bundesverband) und Akteuren aus der Schwesterdisziplin Datenschutz sein Angebot in diesem Bereich deutlich erweitern. Als herstellerunabhängige und kompetente technische Stelle wird das BSI die Verbraucherinnen und Verbraucher in der Risikobewertung von Technologien, Produkten, Dienstleistungen und Medienangeboten unterstützen. Damit kann die gesellschaftliche Widerstandsfähigkeit gegen Cyber-Gefahren jeglicher Art erhöht werden.

Digitale Zukunft sichern

Der Koalitionsvertrag enthält zahlreiche Punkte, um den künftigen Herausforderungen in der Prävention, Detektion und Abwehr von Cyber-Gefahren gerecht zu werden. Dazu gehören zahlreiche Punkte, die zum Teil über den Aufgabenkreis des BSI hinausgehen:

- Umsetzung eines Rahmenprogramms für die zivile Sicherheitsforschung und Weiterentwicklung der Kompetenzzentren der IT-Sicherheitsforschung zu international sichtbaren Forschungs- und Beratungszentren.

- Einrichtung einer „Agentur für Innovationen in der Cybersicherheit“ sowie eines IT-Sicherheitsfonds zum Schutz sicherheitsrelevanter Schlüsseltechnologien.

- Ausbau einfacher und sicherer Lösungen für die elektronische Identifizierung und Ende-zu-Ende-Verschlüsselung, die es den Bürgerinnen und Bürgern ermöglichen, verschlüsselt mit der Verwaltung über gängige Standards zu kommunizieren (PGP/SMIME).

- Förderung der Verbreitung sicherer Produkte und des Entwicklungsprinzips „security by design“ sowie Entwicklung von IT-Sicherheitsstandards für internetfähige Produkte.

- Entwicklung und Umsetzung eines über die gesetzlichen Mindeststandards hinausgehenden IT-Sicherheitsstandards in Form eines Gütesiegels für IT-Sicherheit.

- Aufstellung klarer Regelungen für die Produkthaftung in der digitalen Welt bei ausgewogener Abgrenzung von Risiko- und Verantwortungssphären für Verbraucher, Hersteller und Provider.

- Stärkung der Fähigkeiten der Finanzaufsicht im Bereich Digitalisierung und IT-Sicherheit und Intensivierung der Zusammenarbeit mit allen zuständigen Aufsichts- und Sicherheitsbehörden.

- Einbindung aller gesellschaftlich relevanten Gruppen, Hersteller, Anbieter und Anwender sowie der öffentliche Verwaltung in einen Nationalen Pakt für Cyber-Sicherheit.

- Fortschreibung des IT-Sicherheitsgesetzes zu einem IT-Sicherheitsgesetz 2.0 und Erweiterung des Ordnungsrahmens, um den neuen Gefährdungen angemessen zu begegnen.

- Etablierung des Digitalen Verbraucherschutzes als zusätzliche Aufgabe des BSI.

Darüber hinaus ist das für das BSI zentrale Vorhaben im Koalitionsvertrag der geplante Ausbau des BSI als nationale Cybersicherheitsbehörde und die Stärkung seiner Rolle als unabhängige und neutrale Beratungsstelle für Fragen der IT-Sicherheit sowie als zentrale Zertifizierungs- und Standardisierungsstelle für IT- und Cyber-Sicherheit.

Diese Maßgaben und Vorhaben müssen jetzt konsequent umgesetzt werden. Das BSI wird dazu in seinen klassischen wie in den neuen Aufgabenbereichen seinen fachlichen Beitrag leisten:

- Es sichert die Informationstechnik des Bundes vor Cyber-Angriffen und Cyber-Gefahren. Das BSI wird dieses bewährte Konzept weiterentwickeln und auf dieser Grundlage Angebote für Länder und Kommunen sowie für die Digitalisierung der Verwaltung und Justiz schaffen.

- Das BSI begleitet die Konsolidierung der IT des Bundes, berät regelmäßig und intensiv die Gesamtprojektleitung zu strategischen und operativen Fragen der Informationssicherheit in der IT-Konsolidierung und sorgt für die notwendige zentralisierte Betrachtung der Themen und des Projektprozesses. Aus einer Konzentration von IT-Systemen bei den IT-Dienstleistern ergeben sich jedoch dort auch potenzielle IT-Risikokonzentrationen.

- Es ist auch in Krisenfällen erster fachlicher Ansprechpartner für Betroffene, nationale und internationale Partner sowie Multiplikatoren. Im Rahmen der jeweiligen Möglichkeiten informiert das BSI aktiv und transparent und unterstützt mit mobilen Einsatzteams - Mobile Incident Response Teams (MIRT) - direkt vor Ort. Der Schwerpunkt liegt dabei auf Einrichtungen der Bundesverwaltung und von Betreibern Kritischer Infrastrukturen.

- Das BSI steht im Austausch mit nationalen und internationalen Anbietern von IT-Produkten und IT-Services und vertritt die Interessen der Nutzer gegenüber diesen Anbietern.

- Es ist Kompetenzträger im Bereich Kryptografie, der Empfehlungen und technische Richtlinien zu kryptografischen Verfahren erstellt und sich an der Entwicklung internationaler Krypto-Standards beteiligt.

- Im Dezember 2017 erfolgte der Startschuss für ein BSI-internes Kompetenzzentrum Künstliche Intelligenz/Maschinelles Lernen, in dem die Themen zukünftig aus IT-Sicherheitssicht intensiv begleitet und vorangetrieben werden.

- International positioniert sich das BSI als Thought Leader und als Kompetenzstelle für alle Fragen der Informationssicherheit in der multi- und bilateralen Zusammenarbeit. Einen besonderen Schwerpunkt bildet dabei die Zusammenarbeit in EU und NATO.

Wirtschaft und Standort schützen

Cyber-Sicherheit ist die Voraussetzung für eine erfolgreiche Digitalisierung. Das Potenzial der Digitalisierung ist nahezu unbegrenzt. Eine vom BDI in Auftrag gegebene Studie zeigt: Bis zum Jahr 2025 kann Europa bis zu 1,25 Billionen Euro zusätzliche industrielle Wertschöpfung erzielen. Bereits heute laufen viele Prozessschritte in der Industrie vollständig automatisiert ab. Neu ist dabei die digitale Vernetzung der Maschinen. Maschinen und Produkte kommunizieren miteinander und die Flexibilität der Produktion nimmt erheblich zu. Diese digitale Vernetzung ist ein wichtiger Faktor für die Produktivität und das wirtschaftliche Wachstum in Deutschland.

Die steigende Anzahl von „smart factories“ und vernetzter Objekte wird jedoch die Anfälligkeit der Wirtschaft für Hackerattacken und Cyber-Angriffe weiter erhöhen. Industrieunternehmen sind zudem häufig Opfer von komplexeren Cyber-Vorfällen. Die Gefahr durch Angriffe aus dem Cyberspace muss langfristig als wichtigstes Risiko für Unternehmen erachtet werden.

Das BSI hat bereits wichtige Schritte unternommen und Impulse gesetzt, um in der Wirtschaft sowohl das Bewusstsein für die Gefährdungen zu erhöhen als auch die Unternehmen konkret bei der Gefahrenabwehr zu unterstützen:

- Mit der „Allianz für Cybersicherheit“ (ACS) führt es das größte Selbsthilfe-Netzwerk der deutschen Wirtschaft mit praxisnahen Hilfestellungen für die Analyse von Cyber-Risiken und die Umsetzung geeigneter Schutzmaßnahmen. Dabei arbeitet die ACS eng mit Partnern aus Wirtschaft und Forschung sowie Multiplikatoren zusammen.

- Mit dem Zentralverband des Deutschen Handwerks (ZDH) und dem Handelsverband Deutschland (HDE) konnten wichtige strategische Partnerschaften initiiert und durch die Unterzeichnung formaler Absichtserklärungen bekräftigt werden.

- Mit der Modernisierung des IT-Grundschutzes bietet das BSI den Anwendern aus Wirtschaft und Verwaltung ein fundiertes und praktisches Managementsystem für Informationssicherheit (ISMS). Es hilft dabei, den Status der Informationssicherheit in einer Institution zu überprüfen und perspektivisch zu verbessern.

Das BSI als zentrale Stelle für Cyber-Sicherheit in Deutschland

Mit dem Nationalen IT-Lagezentrum, CERT-Bund und dem Nationalen Cyber-Abwehrzentrum sind drei wesentliche Bausteine der nationalen Cyber-Sicherheitsarchitektur beim BSI angesiedelt. Das Nationale IT-Lagezentrum wächst im Fall einer IT-Krise zum Nationalen IT-Krisenreaktionszentrum auf. Das BSI ist zudem das neutrale Kompetenzzentrum für Cyber-Sicherheit und der IT-Sicherheitsdienstleister für alle Bundesressorts. Das BSI unterstützt die Ressorts bei der Gestaltung der Informationssicherheit in den großen Digitalisierungsprojekten, um die Funktionsfähigkeit und Wertschöpfung der künftig stark digitalisierten Gesellschaft zu gewährleisten. Beispiele dafür sind:

- die Telematik-Infrastruktur im Gesundheitsbereich/„eHealth“ (BMG),

- die Digitalisierung der Energiewende (BMWi),

- intelligente Verkehrssysteme (BMVI).

- Smart Home / intelligente Baustellen (BMWi, BMJV, BMUB),

- das Internet der Dinge / IoT (BMI, BMWi, BMJV),

- neue Technologien / Blockchain (BMBF),

- digitale Schifffahrt (BMVI) sowie

- Digitalisierung der ressortübergreifenden VS-Kommunikation (BMI, BMVg, AA, BKAmt)

Deutlich wird die ausgeprägte Querschnittsfunktion des BSI auf Bundesebene.

Hinzu kommt der Ausbau der Zusammenarbeit mit den Bundesländern und dem kommunalen Sektor. Mit einer Reihe von Bundesländern konnten bereits Vereinbarungen zur Zusammenarbeit erzielt werden, um den Aufbau von Parallelstrukturen zu vermeiden und im gesamtstaatlichen Interesse ein einheitliches Sicherheitsniveau zu gewährleisten. Damit entwickelt sich das BSI zur „Zentralen Stelle für Cybersicherheit in Deutschland“.

Das BSI geht bereits gestärkt und zuversichtlich in diese Entwicklung. Der Lagebericht 2018 zeigt aber auch, welche Herausforderung noch vor uns liegt. Denn uns allen ist klar: Informationssicherheit ist die Voraussetzung für eine erfolgreiche Digitalisierung. Daher muss das BSI auch in den kommenden Jahren konsequent fortentwickelt werden.

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.

Adware
Als Adware werden Programme bezeichnet, die sich über Werbung finanzieren. Auch Schadprogramme, die Werbung für den Autor des Schadprogramms generieren, gehören zu dieser Kategorie.

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.

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

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

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 unter anderem Infrastrukturen (Rechenleistung, Speicherplatz), Plattformen und Software.

DANE
DNS-based Authentication of Named Entities (DANE) ist ein Protokoll, das es erlaubt Zertifikate an DNS-Namen zu binden. Ein typischer Fall ist die Hinterlegung eines TLS-Zertifikats. Hierzu wird ein DNS-Eintrag mit dem Namen TLSA erzeugt. Um diese Einträge vor Manipulation zu schützen, ist DNSSEC erforderlich.

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.

DNSSEC
DNSSEC ist eine Sicherheitserweiterung für das Domain Name System (DNS). Mit DNSSEC lassen sich Einträge im DNS kryptografisch signieren. Damit werden Manipulationen dieser Einträge erkennbar.

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, z. B. durch Botnetze.

DRDoS/DRDoS-Angriffe
Viele Arten von Distributed-Denial-of-Service (DDoS)-Angriffen basieren auf Reflektion und Verstärkung (reflection and amplification). Reflektionsbasierte DDoS-Angriffe werden oft als Distributed Reflection Denial of Service (kurz DRDoS) bezeichnet.

Das grundlegende Prinzip von DRDoS-Angriffen ist, dass ein Angreifer ein kleines Datenpaket mit einer gefälschten Absenderadresse an einen Server sendet. Dieser Server antwortet dann an die gefälschte Adresse, die dem Opfer des Angriffs gehört. Der Angreifer nutzt also einen Server als Reflektor. Da die Antwortpakete des Servers in der Regel sehr viel größer sind als die Anfragen, wird der Angriff dadurch verstärkt. Das Größenverhältnis von Antwort zu Anfrage bezeichnet man als Verstärkungsfaktor (amplification factor). Alle DRDoS-Angriffe nutzen UDP-basierte Protokolle, da UDP verbindungslos arbeitet und sich die Absenderadresse fälschen lässt.

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 (Plugins) oder im Betriebssystem ausgenutzt, um Schadsoftware unbemerkt auf dem PC zu installieren.

Embedded-Systeme
Ein eingebettetes System (auch englisch embedded system) ist ein elektronischer Rechner oder auch Computer, der in einen technischen Kontext eingebunden (eingebettet) ist. Dabei übernimmt der Rechner entweder Überwachungs-, Steuerungs- oder Regelfunktionen oder ist für eine Form der Daten- bzw. Signalverarbeitung zuständig, beispielsweise beim Ver- bzw. Entschlüsseln, Codieren bzw. Decodieren oder Filtern.

Exploit
Exploits sind Schadprogramme, die Schwachstellen ausnutzen.

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.

Kritische Infrastrukturen KRITIS
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.

Krypto-Mining
Beim Krypto-Mining wird Rechenleistung dafür eingesetzt, am „Proof-of-Work"-Konsensverfahren einer Kryptowährung teilzunehmen und entsprechende Währungstoken wie zum Beispiel Bitcoins zu schürfen.

Nonce
Nonce steht für engl. „number used only once" und steht in der Kryptografie für eine Einmalzahl, d.h. eine Zahl, die in einem Kontext nur einmal benutzt wird. Häufig werden Nonces mit einem Zufallszahlengenerator erzeugt, dann z. B. für die Erstellung einer elektronischen Signatur benutzt und danach wieder gelöscht, damit die gleiche Zahl nicht erneut für eine andere elektronische Signatur verwendet wird. Beim Aufbau der TLS-Verbindung werden ebenfalls Nonces benötigt.

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 Software-Modul, 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 vorgeben, diese Ressourcen nur gegen Zahlung eines Lösegeldes (engl. „ransom") wieder freizugeben. 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 (Malspam), Links zu verseuchten Webseiten oder wird für Phishing-Angriffe genutzt.

Spearphishing-Mails
Phishing-Mails mit maliziösen Links oder Anhängen, die gezielt an Adressaten geschickt werden.

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).

TLSA
Siehe DANE.

Troll
Als Trolle werden Internetnutzer bezeichnet, die durch ihre Äußerungen mit dem Ziel der gezielten Einflussnahme Diskussionen stören, anheizen oder Falschinformationen verbreiten.

UP Bund
Der Umsetzungsplan Bund 2017 ist die Leitlinie für Informationssicherheit in der Bundesverwaltung (UP Bund 2017) und soll die Informationssicherheit in der Bundesverwaltung gewährleisten. Mit dem UP Bund 2017 wurde der ursprünglich aus dem Jahr 2007 stammenden Umsetzungsplan neu gefasst und vom Bundeskabinett in seiner Sitzung am 19. Juli 2017 beschlossen. Der UP Bund 2017 trat am 1. September 2017 in Kraft und setzt Ziele aus der Cyber-Sicherheitsstrategie 2016 aus verschiedenen Handlungsfeldern um. Er gilt für alle Ressorts und Bundesbehörden.

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.

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

Impressum

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik (BSI)

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

E-Mail
bsi@bsi.bund.de

Telefon
+49 (0) 22899 9582-0

Telefax
+49 (0) 22899 9582-5400

Stand
September 2018

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.de/shulz

Grafiken
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Artikelnummer
BSI-LB18/507

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

www.bsi.bund.de