Bundesamt
für Sicherheit in der
Informationstechnik

Die Lage der IT-Sicherheit in Deutschland 2017

Vorwort

Nichts ist so beständig wie der Wandel. Auf wohl kaum etwas Anderes trifft Heraklits Erkenntnis so zu wie auf die Digitalisierung. Ihre Chancen für unseren gesellschaftlichen, wissenschaftlichen und wirtschaftlichen Fortschritt sind immens. Die Risiken sind es ebenso und müssen beherrschbar bleiben.

Ein Blick zurück zeigt: Die vergangenen Jahre waren von IT-Sicherheitsvorfällen geprägt wie nie zuvor. Trotz aller Anstrengungen waren sie an der Tagesordnung, oft schwerwiegend und selten auf Deutschland beschränkt. Es traf Krankenhäuser in Großbritannien, Energieversorger in der Ukraine, einen der weltweit größten Logistiker, Banken, Pharmaunternehmen und Stahlproduzenten – dies sind nur einige der Ziele der jüngsten Cyber-Attacken. Cyber-Kriminalität, Cyber-Spionage gegenüber Staat und Wirtschaft und provozierte Ausfälle Kritischer Infrastrukturen sind eine ernstzunehmende Bedrohung unserer Gesellschaft im 21. Jahrhundert.

Richtig ist aber auch: Nie zuvor haben wir im Bereich der IT- und Cyber-Sicherheit so viel Recht gesetzt und soviel erreicht wie in den letzten Jahren. Nie zuvor waren wir auf internationaler Ebene an so vielen Kontakten und Austauschformaten zur IT- und Cyber-Sicherheit beteiligt. Mit der neuen Cyber-Sicherheitsstrategie wurde ein strategischer Überbau für alle Maßnahmen des Bundes auf dem Gebiet der Cyber-Sicherheit geschaffen. Das BSI wurde zu dem ausgebaut, was es heute ist: eine weltweit einmalige Fachbehörde.

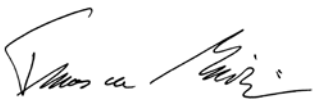
Der Blick in die Zukunft zeigt: Auf dem Erreichten dürfen wir uns nicht ausruhen. Die hohe Dynamik in der Entwicklung der Informationstechnik lässt es auch nicht zu, dass moderne Wirtschaftsnationen auf dem Gebiet der Digitalisierung und IT-Sicherheit stillstehen. Wir müssen auch künftig unsere rechtlichen, technischen und personellen Möglichkeiten zur Gestaltung der Digitalisierung und zur Gewährleistung weitreichender IT-Sicherheit fortentwickeln.

In diesen bewegten Zeiten verdient der Lagebericht des BSI zur IT-Sicherheit in Deutschland 2017 besondere Aufmerksamkeit. Er ist mehr als eine Momentaufnahme, sondern eine fundierte wie verlässliche Dokumentation, welchen Bedrohungen Deutschlands IT ausgesetzt ist und welche Herausforderungen sich uns stellen.

Wer den BSI-Bericht liest, wird auch feststellen: Die Mitarbeiter des BSI leisten Großes auf einem Gebiet, das Millionen Menschen betrifft und dessen ernste Probleme häufig nur von wenigen Experten durchdrungen werden. Sie sind es, die die wichtigen Aufgaben der Prävention und Detektion und beim Schutz vor Cyber-Angriffen erfüllen und passende Antworten auch auf drängendste Herausforderungen finden.

Mit diesen anspruchsvollen Aufgaben ist das BSI eine tragende Säule unseres digitalen Deutschlands.

Berlin, im August 2017



Dr. Thomas de Maizière, MdB
Bundesminister des Innern

Vorwort

Leistungsfähige und sichere Kommunikationssysteme sind das zentrale Nervensystem der Gesellschaft im 21. Jahrhundert. Sie sind essenziell für eine funktionierende Wirtschaft und sorgen auch im privaten Umfeld für Komfort und vielfältige Möglichkeiten. Sie schaffen die Bedingungen für Mobilität und Datenaustausch sowie für Kapital-, Waren- und Dienstleistungstransfer. Sie sind Voraussetzung für die Industrie 4.0, die Energiewende und den Betrieb Kritischer Infrastrukturen.

In den letzten Monaten haben weltweite Angriffskampagnen wie WannaCry und Petya / NotPetya sowie erfolgreiche Cyber-Angriffe auf Unternehmen, auf demokratische Institutionen wie den Deutschen Bundestag oder die Parteien, auf Entscheidungsträger in der Wirtschaft und nicht zuletzt auch auf die Bürgerinnen und Bürger sehr deutlich gemacht, wie gefährdet unsere digitalisierte Wirtschaft und Gesellschaft ist. Die Schäden, die dabei für die Gesellschaft entstehen, gehen in die Millionen. Mit jedem Vorfall wird deutlicher, wie abhängig eine erfolgreiche Digitalisierung von der Cyber-Sicherheit ist. Die Informationssicherheit in der Digitalisierung für Staat, Wirtschaft und Gesellschaft zu gestalten und voranzutreiben, ist Aufgabe und Ziel der nationalen Cyber-Sicherheitsbehörde BSI.

Das BSI genießt als Kompetenzzentrum für Fragen der Cyber-Sicherheit hohes Ansehen in allen Teilen der Gesellschaft. Im BSI sind alle Themen der Cyber-Sicherheit vereint: vom Schutz der Regierungsnetze und der Kritischen Infrastrukturen über die Kryptographie, die Zertifizierung und Standardsetzung, die Beratung von Bund, Ländern, Wirtschaft und Bürgern bis hin zur Gestaltung der Digitalisierung in hochkomplexen Projekten wie der Energiewende oder dem autonomen Fahren. Diese Bündelung und Vernetzung von Cyber-Sicherheits-Expertise in einer Behörde gibt dem BSI seine in Deutschland einzigartige Schlagkraft.

Der Bericht zur Lage der IT-Sicherheit in Deutschland beschreibt und analysiert die aktuelle IT-Sicherheitslage, auch anhand konkreter Beispiele und Vorfälle. Daraus abgeleitet stellen wir die Angebote und Lösungsansätze des BSI zur Verbesserung der IT-Sicherheit in Deutschland vor.

Das erste Kapitel geht gleichermaßen auf die Gefährdungslage für die Bundesverwaltung, die Wirtschaft – insbesondere die Kritischen Infrastrukturen – und die Gesellschaft ein. Wir beschreiben die Ursachen von Cyber-Angriffen und analysieren die verwendeten Angriffsmittel und -methoden.

Dabei zeigen wir auf, wie mit der zunehmenden Vernetzung über Informations- und Kommunikationstechnologie auch der Grad der Abhängigkeit steigt. Wir alle sind immer stärker auf sichere Informationswege angewiesen, doch gleichzeitig steigt die Zahl der Angriffe auf das Netz. Cyber-Kriminalität, Cyber-Spionage und Cyber-Sabotage Kritischer Infrastrukturen stellen ernstzunehmende Bedrohungen dar.

Daraus abgeleitet thematisiert der Lagebericht im zweiten Kapitel Lösungsansätze zur Verbesserung der IT-Sicherheit in Deutschland und stellt dabei auch die Angebote und Maßnahmen des BSI vor. Anhand vieler Beispiele wird deutlich, wie das BSI mit verschiedenen Akteuren aus Staat, Wirtschaft und Gesellschaft gemeinsam daran arbeitet, den Risiken wirksame und umsetzbare Sicherheitsmaßnahmen entgegenzusetzen. Das dritte Kapitel schließlich bewertet die Sicherheitslage, leitet daraus Empfehlungen ab und gibt einen Ausblick auf die weitere Entwicklung.

Die Erfahrung zeigt, dass angesichts der aufgezeigten Bedrohungslage die Fortschritte zur Erhöhung der Cyber-Sicherheit meist Schritt für Schritt erfolgen. Aber je breiter das Bewusstsein für die Bedeutung der Informationssicherheit in der Digitalisierung für alle Bereiche der Gesellschaft wird, desto größer können diese Schritte werden. Daran arbeiten wir.

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

Inhaltsverzeichnis

1 Die Gefährdungslage

1 Die Gefährdungslage

Im folgenden Kapitel wird die Gefährdungslage der IT-Sicherheit in Deutschland 2016/17 beschrieben, gegliedert in die drei Bereiche Bundesverwaltung, Kritische Infrastrukturen/Wirtschaft und Gesellschaft. Außerdem wird auf die Angriffsmethoden und -mittel eingegangen und es wird anhand zahlreicher Beispiele erläutert, wie diese Angriffe das öffentliche Leben in einer digitalisierten Gesellschaft beeinträchtigen oder gefährden können.

1.1 Die Gefährdungslage in der Bundesverwaltung

Die Ausübung der verfassungsrechtlich garantierten Aufgaben der judikativen, legislativen und exekutiven Staatsgewalten setzt einen sicheren und zuverlässigen Betrieb der Informationssysteme des Staates voraus. Nur auf diese Weise sind eine lückenlose und gegen Manipulationen jeglicher Art geschützte Kommunikation und eine fälschungssichere Dokumentation des Verwaltungshandelns garantiert. Das Vertrauen der Bürger und Unternehmen in die Integrität des digitalen Staates wird erschüttert, wenn dieser seinen Aufgaben wegen funktionsunfähiger Informationssysteme nicht mehr nachkommen kann. Die Informationssysteme in den Staatsgewalten sind dadurch zu kritischen Infrastrukturen für das Gemeinwesen geworden.

Erkenntnisse aus dem Schutz der Regierungsnetze

Die Abwehr von Gefahren für die IT des Bundes ist eine der Kernaufgaben des BSI. Insbesondere erfüllt das BSI bereits seit seiner Gründung die Aufgabe, die Netze der Bundesverwaltung zu schützen und trägt heute die Gesamtverantwortung für das IT-Sicherheitskonzept des Regierungsnetzes.

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.

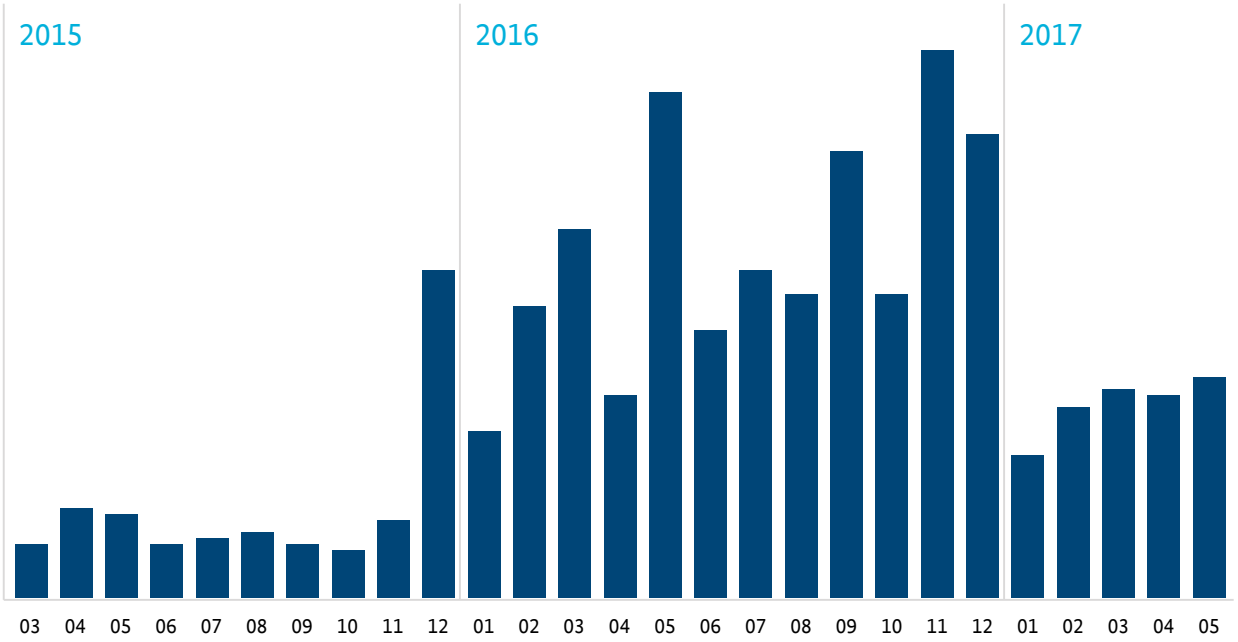


Abbildung 1 Schadprogramme, die am Netzübergang der Regierungsnetze durch AntiVirus-Schutzmaßnahmen automatisiert gefiltert wurden

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 gezählten Angriffen auf die Bundesverwaltung. Mittels automatisierter AntiVirus-Schutzmaßnahmen wurden pro Monat durchschnittlich fast 52.000 solcher E-Mails in Echtzeit abgefangen, bevor sie die Postfächer der Empfänger erreichten. Davon wurden monatlich im Durchschnitt rund 11.000 schädliche E-Mails nur aufgrund eigens erstellter AntiVirus-Signaturen erfasst. Der erneute Anstieg dieser Zahlen um 18 Prozent im Vergleich zum Vorjahresbericht ist vor allem auf die massenhafte Verbreitung von Ransomware im Jahr 2016 zurückzuführen, der auch außerhalb des Regierungsnetzes zu beobachten war. Die Angreifer verwendeten dazu häufig E-Mail-Anhänge mit in Archiven gepacktem JavaScript oder Makrocode in Office-Dokumenten, um dann das eigentliche Schadprogramm aus dem Internet nachzuladen. Seit Jahresbeginn hat sich die Lage diesbezüglich spürbar entspannt. Im 1. Halbjahr 2017 wurden – ohne erkennbare Einbußen in der Schutzwirkung – nur noch halb so viele E-Mails mit Schadsoftware abgefangen wie im 2. Halbjahr 2016. Den automatisierten AntiVirus-Schutzmaßnahmen nachgelagert betreibt das BSI ein eigenes System zur Detektion von Schadprogrammen, das für die Bundesverwaltung zusätzlichen Schutz bietet.

Gestaffelte Verteidigung

Die verschiedenen Schutzmaßnahmen an den Netzübergängen und auf den Client-Systemen können nicht immer alle Angriffsversuche zuverlässig abwehren. Daher werden im Regierungsnetz auch weitere Maßnahmen zur Detektion und Reaktion eingesetzt, die in solchen Fällen greifen, diese Angriffe verhindern oder deren negativen Effekte minimieren.

So werden im Regierungsnetz ausgehende Netzverbindungen auf Webseiten blockiert, die Schadprogramme verteilen. Ebenso werden Verbindungsversuche von bereits aktiven Schadprogrammen zu Kontrollservern unterbunden, die für die Steuerung und den Datenabfluss genutzt werden. Auf diese Weise können bereits infizierte Systeme erkannt und ein unberechtigter Datenabfluss verhindert werden. Idealerweise wird der Angriff aber bereits im Vorfeld verhindert, in dem zum Beispiel der Aufruf einer zur Schadprogrammverteilung oder zum Phishing genutzten Website verhindert werden kann.

Mit dieser Methode wurden täglich rund 5.100 Verbindungsversuche zu Schadcodeservern verhindert. Vereinzelt sind darunter auch lang laufende Watering-Hole-Angriffe, bei denen Täter mit Spionagehintergrund Schadcode auf Webseiten platzieren, die für Regierungsmitarbeiter relevant sind. Der Schadcode wird dabei im Abstand von mehreren Monaten durch neue Varianten ausgetauscht.

In weniger als 70 Fällen mussten Bundesbehörden aufgrund auffälliger Verbindungsversuche eines ihrer Systeme über eine mögliche Schadprogramminfektion unterrichtet werden. Diese niedrige Zahl potenzieller Infektionen ist auch auf die engmaschigen E-Mail-Filter zurückzuführen, die als Reaktion auf Ransomware-Kampagnen wie Locky eingerichtet wurden.

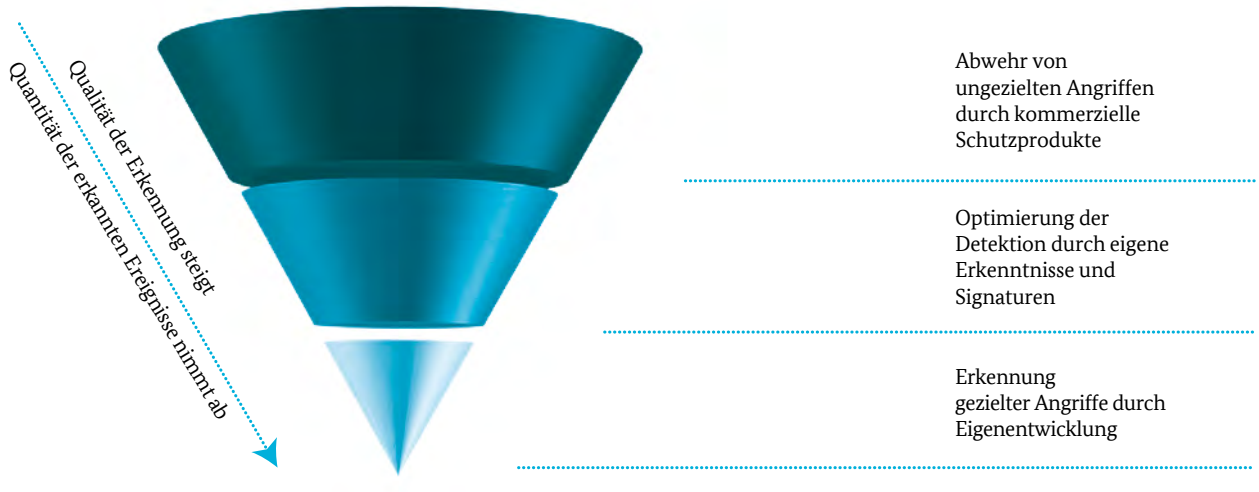


Abbildung 2 Gestufte Schutzmaßnahmen in den Regierungsnetzen gegen E-Mail-basierte Angriffe

Erkenntnisse aus der Informationssicherheitsberatung

Die Veränderung der behördlichen Arbeitsabläufe durch die Digitalisierung verändert auch die Anforderungen an den Schutz der dort verarbeiteten Informationen. Sicherheitsmaßnahmen müssen im Rahmen des etablierten Managementsystems für Informationssicherheit (ISMS) permanent an diese veränderten Rahmenbedingungen angepasst werden, denn die schnell fortschreitende Digitalisierung der Behördenstrukturen weiß auch ein Angreifer zu nutzen. Daneben kommen auch mit dem Internet der Dinge, der Industrie 4.0 beziehungsweise der Digitalisierung des technischen Umfelds neue Herausforderungen auf das ISMS in den Behörden zu. Wenn IP-basierte Embedded Systems wie etwa smarte Klimaanlagen mit dem Behördennetz vernetzt werden sollen, ergibt dies neue Risikopotenziale für die Informationssicherheit, die durch eine geeignete Behandlung aufgefangen werden müssen.

Die Etablierung von zentralen IT-Dienstleistern im Bereich des Bundes sowie die verstärkte Nutzung der Netze des Bundes stellt das ISMS in den Behörden vor weitere Herausforderungen, die parallel zum Regelbetrieb und der Digitalisierung angegangen werden müssen

- Zum einen müssen die Behörden ihre bisherigen heterogenen Netzstrukturen und Rechenzentren zu einem gemeinsamen Standard konsolidieren sowie an die neuen Gegebenheiten anpassen.

- Zum anderen muss in allen Schritten der Konsolidierung und der Anpassung die Informationssicherheit sichergestellt werden.

Ein weiterer, zunehmend wichtiger werdender Aspekt ist, dass Mitarbeiter an Abläufen und Lösungen interessiert sind, die sie aus dem Consumer-Bereich kennen und wertschätzen. Die Realisierung solcher Lösungen führt zu vielfältigen Anforderungen an das ISMS. Die Behörden sind daher stärker als zuvor gefordert, Anforderungen an die Informationssicherheit in Einklang mit den Anforderungen an „Usability“ zu bringen und für die Sicherheitsmaßnahmen bei den Mitarbeitern Akzeptanz zu schaffen. Außerdem muss die Ausbildung und Weiterbildung der IT-Sicherheitsexperten in den Behörden permanent vorangetrieben und ausgebaut werden, um den Angreifern auch in diesem Umfeld ebenbürtig begegnen zu können.

Erkenntnisse aus Meldungen aus der Bundesverwaltung

Nach § 4 Abs. 3 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) sind die Bundesbehörden verpflichtet, das BSI unverzüglich bei erfolgten oder versuchten Angriffen zu unterrichten, die für die Abwehr von IT-Sicherheitsgefahren insbesondere auch bei anderen Behörden relevant sind.

Dies dient neben der Veranlassung von Sofort-Maßnahmen insbesondere auch der konsolidierten Langzeitanalyse der IT-Sicherheitslage. Dabei wird geprüft, ob und inwieweit vorhandene zentrale Schutzmaßnahmen wirksam und wirtschaftlich sind. Außerdem wird festgestellt, ob es einen Bedarf für erweiterte Schutzmaßnahmen gibt.

Auch wenn diese Meldungen aufgrund der sehr unterschiedlichen Bedrohungslage über die Jahre unregelmäßig verteilt sind, bilden sie doch einen zusätzlichen Indikator zur Bewertung der Bedrohungslage.

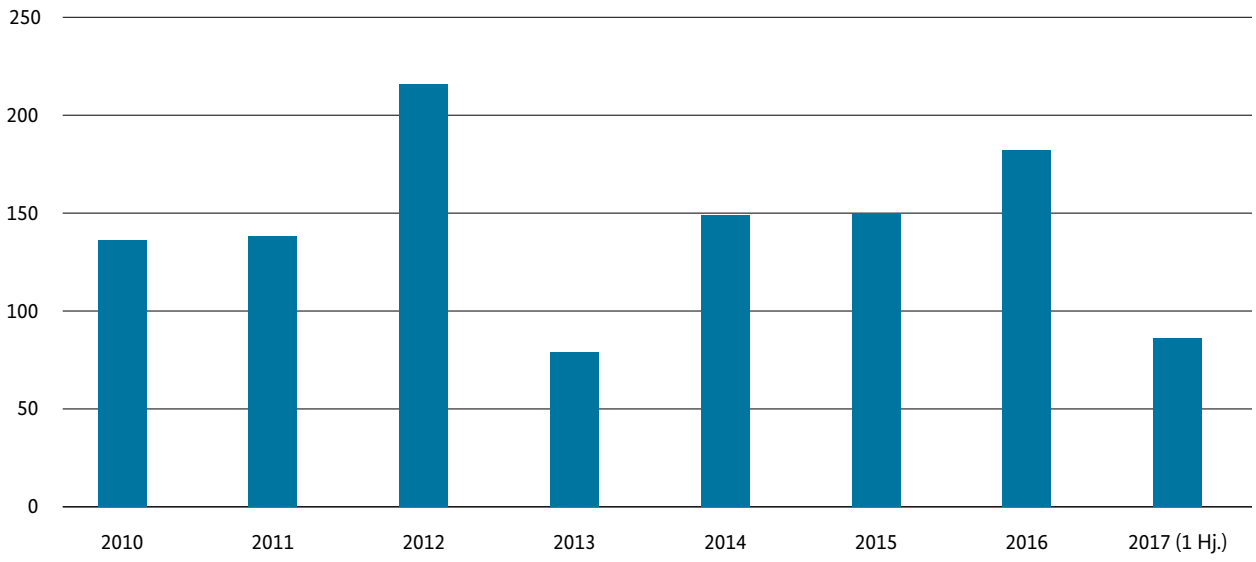


Abbildung 3 Anzahl der SOFORT-Meldungen nach § 4 Abs. 3 BSIG

Auch 2017 blieb Ransomware die maßgebliche Quelle für Schadprogramminfektionen. Verstärkt gemeldet wurden auch Angriffe auf Telefon- und Videokonferenzanlagen.

1.2 Die Gefährdungslage in der 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.

Erkenntnisse aus Meldungen nach dem IT-Sicherheitsgesetz

Das IT-Sicherheitsgesetz trat im Juli 2015 in Kraft. Dabei wurden auch Meldepflichten für Betreiber Kritischer Infrastrukturen bestimmt, welche zeitlich gestuft eingeführt wurden. Sie bestehen

- seit Inkrafttreten des Gesetzes für gemäß Atomgesetz, Energiewirtschaftsgesetz oder Telekommunikationsgesetz verpflichtete KRITIS-Betreiber
- seit Inkrafttreten der BSI-Kritisverordnung (03.05.2016) für KRITIS-Betreiber in den Sektoren Energie, Ernährung, Informationstechnik und Telekommunikation sowie Wasser
- mit Inkrafttreten des zweiten Teils der BSI-Kritisverordnung (30.06.2017) für KRITIS-Betreiber aus den Sektoren Finanz- und Versicherungswesen, Gesundheit sowie Transport und Verkehr.

Insgesamt sind seit Einführung der Meldepflicht bis 30. Juni 2017 34 Meldungen beim BSI eingegangen. Davon fallen 18 in den Sektor Informationstechnik und Telekommunikation, elf in den Sektor Energie, drei in den Sektor Wasser und zwei in den Sektor Ernährung.

Aufgrund der eingegangenen Meldungen kann festgestellt werden, dass häufig menschliche Fehler wie beispielsweise falsche Konfigurationen zu einer IT-Störung führten. Weitere häufige Ursachen sind Hardwaredefekte oder fehlerhafte Software. Letzteres äußerte sich in der Regel durch fehlerhafte Updates. Je nach Aufbau der Infrastruktur des Betreibers wirkten sich diese Defekte und Störungen teilweise bis auf die Verfügbarkeit der Kritischen Infrastruktur aus.

Gefährdungsdifferenzierung nach Branchen

Die hohe IT-Durchdringung in den Kritischen Infrastrukturen geht mit einer hohen Abhängigkeit von IT einher. Dadurch sind nicht nur die IT-Systeme selbst Cyber-Sicherheitsgefährdungen ausgesetzt, sondern auch die Erbringung der jeweiligen kritischen Dienstleistungen. Diese Schadenspotenziale vervielfältigen sich. So entsteht für die Kritischen Infrastrukturen bei gleicher Bedrohungslage wie für andere Unternehmen ein besonders hohes Schadenspotenzial.

Zusätzlich kommen bei der Dienstleistungserbringung in den KRITIS-Sektoren IT-Systeme zum Einsatz, die nicht mit herkömmlicher Büro- oder Rechenzentrums-IT vergleichbar sind. Zum Beispiel werden in den KRITIS-Sektoren „Transport und Verkehr“, „Ernährung“, „Wasser“ und „Energie“ viele Spezialsysteme und industrielle Steuerungssysteme eingesetzt. In der Regel erfordern diese Systeme

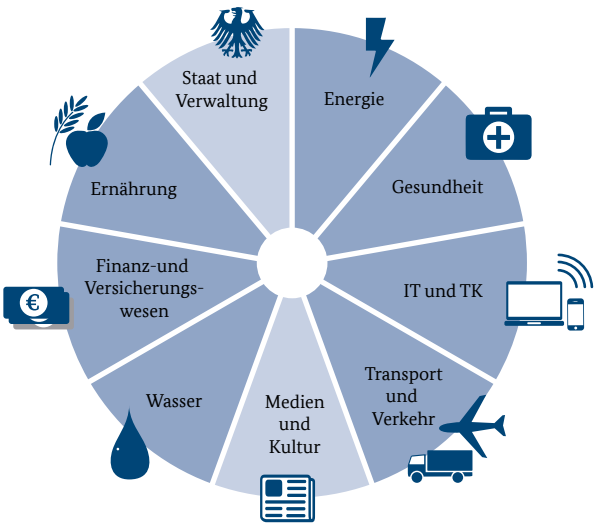


Abbildung 4 Sieben der neun KRITIS-Sektoren fallen unter die KRITIS-Neuregelungen des IT-Sicherheitsgesetzes [1]

[1] Für den KRITIS-Sektor Medien und Kultur hat der Bund keine Regelungskompetenz, Gleiches gilt für die Landes- und Kommunalbehörden im Sektor Staat und Verwaltung. Für die im Sektor Staat und Verwaltung umfassten Bundesbehörden gibt es bereits seit der BSIG-Novellierung 2009 den jetzigen Neuregelungen vergleichbare Pflichten.

eine besondere Behandlung beim Schutz vor Cyber-Bedrohungen, die gleichzeitig den betrieblichen Anforderungen an Verfügbarkeit und Zuverlässigkeit genügen muss. Systeme, die weit verbreitet und über das Internet erreichbar sind sowie eine wichtige Rolle bei der Erbringung der kritischen Dienstleistung spielen, sind wegen der hohen Schadenpotenziale von besonderer Relevanz. Dies hat unter anderem der wiederholt erfolgreiche Cyber-Angriff auf das Stromversorgungsnetz der Ukraine gezeigt. So waren im Dezember 2015 mindestens 225.000 Personen in der Ukraine von einem mehrstündigen Ausfall der Stromversorgung betroffen, der durch einen gezielten Cyber-Angriff verursacht wurde. Im Dezember 2016 gab es einen erneuten Stromausfall in Kiew, der Hauptstadt der Ukraine. Laut Aussage des geschäftsführenden Direktors des staatlichen Energieversorgers Ukrenergo handelte es sich abermals um einen gezielten Cyber-Angriff. Zwischen 100.000 und 200.000 Einwohner wurden für über eine Stunde nicht mehr mit Strom versorgt.

Auch am Ausfall der Router der Deutschen Telekom im November 2016, bei dem durch einen Cyber-Angriff der Internetzugang bei bundesweit ca. 900.000 Kundenanschlüssen gestört wurde, zeigte sich deutlich das Gefährdungspotenzial eines Cyber-Angriffs auf die TK-Infrastruktur (siehe Infokasten auf Seite 12).

Ein weiteres Beispiel sind die entdeckten Schwachstellen in der Fernzugangssoftware von Baustellenampeln, die über das Internet zugänglich sind (siehe Infokasten auf Seite 14). In diesem Fall kam es nicht zu Schadensfällen. Die Absicherung von Spezialsystemen birgt ihre eigenen Problematiken, die im vorliegenden Fall nur für eine erhöhte Exposition sorgten.

Nach wie vor stehen die Betreiber Kritischer Infrastrukturen im Fokus von Angreifern mit politischer Motivation, zum Beispiel Hacktivisten und anderen staatlich geduldeten Akteuren. Da ein erfolgreicher Angriff öffentlichkeitswirksam die Wirtschaft oder das tägliche Leben der Bevölkerung beeinträchtigen würde, bleiben die Kritischen Infrastrukturen ein lohnendes Ziel für diese Angreifergruppierungen. Dies gilt vor allem auch für politisch motivierte Angreifer, die durch einen Angriff die eigene politische Agenda in den Mittelpunkt der öffentlichen Aufmerksamkeit rücken wollen.

Sonstige Erkenntnisse zur Gefährdungslage Wirtschaft

Wirtschaftsunternehmen in Deutschland sind aufgrund ihres technologischen Know-hows und durch ihre Auslandsaktivität interessante Ziele für Cyber-Spionage. In den letzten Jahren haben viele Unternehmen reagiert und eigene Computer-Notfall-Teams (CERTs) sowie branchenübergreifende Organisationen zum Informationsaustausch gegründet.

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 gehört zum Beispiel der CEO-Betrug (siehe Kapitel 2), bei dem Angestellte von Unternehmen dazu verleitet werden sollen, große Geldbeträge auf Konten zu überweisen, die der Kontrolle der Angreifer unterliegen. Bei Ransomware-Angriffen ist zu beobachten, dass von Unternehmen mehr Lösegeld gefordert wird als von privaten Anwendern.

Einem weltweiten Trend folgend hatte Ende 2015 und Anfang 2016 die Zahl der beobachteten Cyber-Spionage-Angriffe gegen Wirtschaftsunternehmen auch in Deutschland stark nachgelassen. Mittlerweile steigt die Zahl der beobachteten Angriffe jedoch wieder an, seit Sommer 2016 werden wieder neue Angriffe auf deutsche Unternehmen beobachtet. Besonderes Medieninteresse galt dabei dem Angriff mit der Schadsoftware Winnti auf einen deutschen Industriekonzern (siehe Infokasten auf Seite 15). Dem BSI sind auch weitere Angriffe mit Winnti auf deutsche Unternehmen bekannt.

Auch APT-Gruppen führten Spionage-Angriffe auf deutsche Unternehmen aus. Bemerkenswert ist, dass bei Angriffen auf deutsche Unternehmen die Gruppen APT28 und APT29 kaum in Erscheinung traten. Abgesehen von Rüstungsunternehmen scheinen sich diese Gruppen vorrangig auf Regierungseinrichtungen und politische Organisationen zu konzentrieren. Nicht zuletzt wegen der umfangreichen Auslandstätigkeit und der internationalen Verflechtung deutscher Unternehmen hat das BSI öffentliche Berichte daraufhin ausgewertet, welche Cyber-Spionage-Gruppen weltweit in verschiedenen Branchen aktiv sind. Neben Regierungseinrichtungen und der Opposition in nicht-demokratischen Staaten sind die Bereiche Rüstung, Energie und Medien diejenigen mit den meisten aktiven Tätergruppen (siehe Abbildung 5).

Auch Kriminelle wenden zunehmend Techniken an, die bisher nur aus Spionage-Angriffen bekannt waren. So griff beispielsweise die Lazarus-Gruppe weltweit Banken an, um gefälschte Überweisungen über das SWIFT-Netzwerk zu veranlassen. Die Carbanak-Gruppe wiederum

Cyber-Angriff auf einen deutschen Industriekonzern

Sachverhalt
In einem deutschen Industriekonzern ist es Mitte 2016 zu fragmentarischen Datenabflüssen durch einen Cyber-Angriff gekommen. Nach Einschätzung des Konzerns habe es sich möglicherweise um eine Angreifergruppe aus dem südostasiatischen Raum gehandelt. Diese Einschätzung wird vom BSI geteilt, allerdings lässt sich nicht eindeutig feststellen, ob tatsächlich nur eine einzige Hackergruppe hinter dem Angriff steckt. Die Täter verschafften sich Zugriff auf das interne Netzwerk und breiteten sich dann weltweit über verschiedene Standorte aus. Der Vorfall wurde etwa zwei Monate nach der Erstinfektion detektiert, als auf Systemen Fehlanmeldungen beobachtet wurden. Dieser Umstand ist ein Hinweis darauf, dass die Täter Zugangsdaten, die sie auf kompromittierten Systemen erbeutet haben, zur Ausbreitung auf weitere Systeme genutzt haben. Sie besaßen zudem die für APT-Gruppen übliche Fähigkeit, sich über längere Zeit unbemerkt in einem Unternehmensnetzwerk auszubreiten.

Ursache und Schadenswirkung
Für den Angriff genutzt wurde die Schadsoftware Winnti, die öffentlichen Berichten zufolge von asiatischen Tätern eingesetzt wird und ausgefeilte Techniken nutzt, um den Verkehr zu den Kontrollservern der Täter zu tarnen. Dabei werden die Adressen der Kontrollserver dynamisch auf legitimen Webseiten hinterlegt, die darauf ausgelegt sind, von Nutzern bearbeitet zu werden. Da diese legitimen Webseiten typischerweise TLS / SSL-verschlüsselt angesprochen werden, ist es für Netzwerkverteidiger kaum möglich, den Schadsoftware-Verkehr zweifelsfrei zu identifizieren. Winnti ist eine vergleichsweise fortschrittliche und für die Täter komfortable Software. In der Regel wird sie zusammen mit der in Asien häufig genutzten Schadsoftware PlugX beobachtet, die den Tätern die volle Kontrolle über einen infizierten Rechner bietet. Die Tätergruppe hinter Winnti hat ihren Ursprung in der Entwicklung krimineller Fake-Anti-Viren-Malware und wechselte dann zu finanziell motivierten Angriffen auf Spielefirmen. Der genaue Angriffsvektor ist entweder nicht gefunden oder zumindest nicht öffentlich berichtet worden. In der Regel erfolgen Angriffe dieser Art durch Spearphishing-E-Mails, die Anhänge mit Schadcode oder Links auf maliziöse Webseiten enthalten. In seltenen Fällen erfolgt die initiale Kompromittierung über nicht mehr gewartete, aus dem Internet erreichbare Server, von denen sich die Täter im Fall von suboptimalen Netzarchitekturen in das interne Netz ausbreiten. Betroffen waren Daten, die den Tätern oder ihren Auftraggebern einen technologischen Vorteil hätten verschaffen können. Der Industriekonzern bestätigte, dass bruchstückhaft technologische Daten gestohlen wurden. Nach Angaben des Konzerns ist es aber unklar, ob durch den Datenabfluss ein Schaden, etwa geistigen Eigentums, entstanden sei.

Reaktion
Die Bereinigung der großflächigen Infektion nahm das Unternehmens-CERT mit Unterstützung von externen Spezialisten mehrere Monate in Anspruch. Der Konzern entschied sich zudem dazu, die Experten dabei von einem Journalisten begleiten zu lassen. Dieser durfte nach Abschluss der Bereinigungsmaßnahmen in mehreren Artikeln über den Vorfall berichten. Aus der Sicherheits-Gemeinde erhielt der Konzern dafür Zuspruch.

Empfehlung
Potenzielle Ziele von APT-Gruppen sind prinzipiell alle Unternehmen, die auf dem Weltmarkt tätig sind oder technologische Spitzenpositionen einnehmen. Das Ziel der Täter ist dabei, an technologische oder marktoperative Informationen zu gelangen. Der Vorfall verdeutlicht, dass das Sicherheitsniveau auch internationaler Standorte an den Standard des Hauptstandorts angeglichen werden muss, wenn diese Außenstellen in das Unternehmensnetzwerk integriert werden. Alternativ kann eine klare Trennung der Netzwerke und Domänen aufrechterhalten werden. Die Infektion eines Systems sollte nicht dazu führen, dass ganze Netzbereiche oder zentrale Server kompromittierbar werden. Zudem ist kontinuierliches Netzwerk-Monitoring unersetzlich, um erfolgte Kompromittierungen schnell zu entdecken.

kompromittierte Finanzinstitute und Geldautomaten, um ebenfalls Überweisungen zu fälschen. Dabei setzen beide Gruppen Techniken ein, die über die bei normaler Crimeware beobachteten Methoden hinausgingen. Dazu zählt das zugeschnittene Social Engineering auf ausgewählte Mitarbeiter und das Lateral Movement, also das Ausbreiten im internen Netz, indem erbeutete Zugangsdaten verwendet und Nutzerrechte ausgeweitet werden.

Cyber-Spionage bleibt weiterhin eine Herausforderung, gegen die sich Unternehmen wappnen müssen. Da die initialen Angriffe sehr oft in den weniger abgesicherten Netzwerken von Auslandsstandorten oder zugekauften Tochterunternehmen ihren Ursprung nehmen, sollte der Fokus darauf liegen, unternehmensweit ein einheitliches IT-Sicherheitsniveau zu erlangen. Da in vielen Unternehmen die IT-Netze zu wenig voneinander getrennt sind, gelingt es den Angreifern sonst zu leicht, sich weltweit im Unternehmensnetz auszubreiten. Wenn Standard-Sicherheitsmaßnahmen unternehmensweit etabliert wurden, sollten in der Folge Prozesse für das Netzwerk-Monitoring erarbeitet und eingeführt werden. Wenn diese Infrastrukturen und geschultes Personal existieren, kann zusätzlich über den gezielten Einkauf von Threat Intelligence nachgedacht werden.

Regierungseinrichtungen	APT6/1.php, APT12/NumberedP., APT28/Sofacy, APT29/CozyBear, APT32/OceanLotus, Cadelle/Chafer, Callisto/DancingSal., CharmingKitten, Danti, DarkHotel, Dropping-Elephant, EmissaryPanda, Gamaredon, GazaCybergang, GothicPanda, Greenbug, Groundbait, HammerPanda, Infy, KeyBoy, Longhorn, LotusPanda, Machete, Mofang, Naikon/OverrideP., NanHaiShu, OilRig, Operation-Cleaver, Remsec/ProjectSauron, ScarletMimic, Shamoon, Snake, Suckfly, TidePool/Ke3chang, Transparent-Tribe, TropicTrooper/PirateP., ViceroyTiger
Militär/ Rüstung	APT28/Sofacy, AridViper, Callisto/DancingSal., CharmingKitten, C-Major/PureStrike, Dropping-Elephant, Gamaredon, GazaCybergang, GothicPanda, HammerPanda, LotusPanda, Machete, Mofang, Naikon/OverrideP., OilRig, Operation-Cleaver, Remsec/ProjectSauron, Snake
Energie	APT10, APT18/Wekby, APT29/CozyBear, CharmingKitten, ElectricPowder, EmissaryPanda, Greenbug, Kraken/Laziok, Longhorn, Machete, OnionDog, OperationCleaver, Sandworm, Shamoon, TropicTrooper/PirateP.
Opposition	Ahtapot, APT32/OceanLotus, Bookworm, FlyingDragon, Groundbait, Group5, Infy, Neodymium, Operation-Cleaver, Operation Manul, Promethium, ScarletMimic, Sima, StealthFalcon
Medien	APT28/Sofacy, APT32/OceanLotus, BugDrop, Callisto/DancingSal., DarkHotel, GazaCybergang, Groundbait, Infy, Operation Manul, Sandworm, ShroudedCrossbow, StealthFalcon, Tick
Finanzen	APT18/Wekby, APT29/CozyBear, EmissaryPanda, EquationGroup, GazaCybergang, HammerPanda, Longhorn, OilRig, Sandworm, Suckfly
Telko	APT18/Wekby, Codoso, EmissaryPanda, HammerPanda, Longhorn, Machete, OilRig, Remsec/ProjectSauron
NGO	APT29/CozyBear, Callisto/DancingSal., CharmingKitten, HammerPanda, Infy, NilePhish, Operation-Cleaver, RocketKitten
Universitäten	APT10/menuPass, BugDrop, Codoso, Greenbug, DarkHotel, Longhorn, RocketKitten
High-Tech	APT18/Wekby, CharmingKitten, Codoso, LEAD/Winnti, Tick
Transport/ Logistik	Cadelle/Chafer, OilRig, OnionDog, Remsec/ProjectSauron, Shamoon
Luft- und Raumfahrt	APT28, EmissaryPanda, HammerPanda, Greenbug, Longhorn
Gesundheit	APT10/menuPass, LEAD/Winnti, Suckfly
Kanzleien	APT29/CozyBear, Codoso, DeepPanda, NanHaiShu

Abbildung 5 Auflistung der in verschiedenen Branchen im Berichtszeitraum weltweit aktiven Cyber-Spionage-Gruppen,

Cyber-Sicherheit by Design: Manipulierbare Baustellenampeln & Wasserwerke

Sachverhalt
Im August 2016 erhielt das BSI einen Hinweis auf den möglichen Missbrauch einer bekannten Schwachstelle in einer Software, die unter anderem in Baustellenampeln genutzt werden kann. Die betroffenen Ampeln sind direkt aus dem Internet erreichbar und damit potenziell manipulierbar. Außerdem wurde das BSI auf mehrere offene, aus dem Internet einsehbare Steuerungssysteme von Wasserwerken in Deutschland aufmerksam gemacht.

Ursache und Schadenswirkung
In den Ampeln wird eine veraltete Fernwartungssoftware (RealVNC) eingesetzt, die bekannte Schwachstellen aufweist und dadurch einen unautorisierten Zugriff ermöglicht. Updates für diese Schwachstellen sind vorhanden, wurden jedoch nicht eingespielt. Bei einigen der gemeldeten Lichtsignalanlagen wurde dem BSI berichtet, dass der autorisierte Benutzer nicht abgemeldet war, wodurch ein direkter Zugriff auf das System möglich war. Eine automatische Logout-Funktion war offenbar nicht vorhanden. Eine Übernahme und Steuerung der Ampeln wäre damit grundsätzlich denkbar, was möglicherweise einem gefährlichen Eingriff in den Straßenverkehr entspräche. In den Wasserwerken wurden Human Machine Interfaces (HMI), also Benutzerschnittstellen, eingesetzt. Mindestens ein lesender Zugriff aus dem Internet war möglich. Weitere Zugriffe bis hin zu einer Steuerung von außen können nicht ausgeschlossen werden.

Reaktion
Im vorliegenden Fall konnte das BSI die beschriebene Konstellation einer potenziellen Fernsteuerung der Anlagen nicht bestätigen. Das BSI schätzt jedoch einen möglichen Missbrauch der Signalsteuerung von Baustellenampeln grundsätzlich als kritisch ein.

Die Betreiber der Wasserwerke wurden durch das BSI unmittelbar kontaktiert und auf den Sachverhalt aufmerksam gemacht. Diesen war die Erreichbarkeit der Systeme aus dem Internet nicht bewusst. Sie reagierten sehr kooperativ und schlossen die offenen Zugänge kurzfristig. Bei einer später durch das BSI durchgeführten Nachprüfung waren die Anlagen öffentlich nicht mehr erreichbar.

Empfehlung
Hersteller von Baustellenampeln und anderen über das Internet vernetzten Systemen sind gefordert, der IT-Sicherheit ihrer Produkte mindestens die gleiche Bedeutung beizumessen wie der Ergonomie oder dem Preis. Im Sinne eines „Security-by-Design"-Ansatzes sollte IT-Sicherheit bereits bei der Entwicklung der Produkte mitgedacht und implementiert werden. Zur Unterstützung einer sicheren Entwicklung hat das BSI im „ICS-Security-Kompendium – Testempfehlungen und Anforderungen für Hersteller von Komponenten" Fragestellungen formuliert, um Herstellern zu helfen, ihre Komponenten zu testen und Schwachstellen zu vermeiden. Das Dokument steht auf der BSI-Webseite zur Verfügung.

Betreiber Kritischer Infrastrukturen, die HMI einsetzen, sollten überprüfen, welche der Steuerungen grundsätzlich gefährdet sind. Vor allem sollten sie bei Steuerungssysteme mit Internetzugang (zum Beispiel für Fernwartung) überlegen, ob ein Fernzugriff zwingend benötigt wird, und, falls ja, wie die Steuerungssystemen aus dem Internet heraus sichtbar sind. Für den Fernzugang sollten dann Sicherheitsmaßnahmen wie zum Beispiel VPN etabliert werden und es sollte geprüft werden, ob die vorgesehenen IT-Sicherheitsmaßnahmen (Soll-Ist-Vergleich) greifen. Zudem sollten Betreiber die Empfehlungen aus dem ICS-Security-Kompendium des BSI beachten, das ebenfalls auf der Webseite des BSI zur Verfügung steht.

Die IT-Sicherheit von vernetzten Systemen wird zukünftig immer mehr zum Qualitätsmerkmal werden. Die Cyber-Sicherheitsstrategie der Bundesregierung sieht die Entwicklung eines entsprechenden Gütesiegels vor, das derzeit im BSI entwickelt wird. Im Rahmen einer Zertifizierung können Hersteller die IT-sicherheitstechnische Qualität eines Produkts schon jetzt sichtbar machen.

Störungen bei Telekom-Routern

Sachverhalt
Am Sonntag, den 27. November 2016, kam es an Anschlüssen der Deutschen Telekom zu Störungen, die unter anderem den allgemeinen Internetzugang sowie die Internet-Telefonie (VoIP) und IPTV-Dienste betrafen. Von dieser Störung waren bundesweit ca. 900.000 Kundenanschlüsse betroffen. Die Router der Telekom waren zwar immun gegen den Versuch der Infektion durch eine in Routern des Herstellers Zyxel gefundene Schwachstelle, reagierten jedoch aufgrund einer weiteren, bis dahin unbekannten Schwachstelle fehlerhaft. Dies führte zu den massiven Störungen.

Ursache und Schadenswirkung
Ursache der Beeinträchtigungen war ein weltweiter Cyber-Angriff mit dem Ziel, Internetrouter mit Schadcode zu infizieren und diese zum Teil eines Botnetzes zu machen. Bei der verwendeten Schadsoftware handelte es sich um eine Weiterentwicklung der Botsoftware Mirai. Die Cyber-Kriminellen nutzen unter anderem eine in Routern des Herstellers Zyxel gefundene Schwachstelle in der Implementierung des Protokolls TR-064. Dieses wird normalerweise zur einfachen Konfiguration des Routers durch den Kunden verwendet. Kritisch wurde die gefundene Schwachstelle, weil das Protokoll fälschlicherweise auch aus dem Internet heraus angesprochen werden konnte. Genutzt wurde hierfür bei dem genannten Routermodell der Port 7547. Er ist eigentlich dem Protokoll TR-069 zugeordnet, das von einigen Internetservice-Anbietern verwendet wird, um Router aus der Ferne zu administrieren oder automatisiert Updates einzuspielen. Im vorliegenden Falle machte sich der Angreifer dies zunutze, indem er wahllos jeden im Internet auffindbaren Router mit dem zuvor in Mirai implementierten Angriffsvektor auf Port 7547 kontaktierte. Ziel war die Infektion des Gerätes und die Übernahme der Kontrolle.

Reaktion
Eine kurzfristige Lösung des Problems konnte durch einen Neustart des Routers erreicht werden, allerdings waren die Angriffsversuche so zahlreich, dass bereits nach wenigen Minuten die Router erneut abstürzten. In Zusammenarbeit mit dem Gerätehersteller hat die Telekom durch die schnelle Bereitstellung eines Updates eine endgültige Lösung herbeigeführt, sodass sich die Situation innerhalb weniger Tage normalisierte.

Empfehlung
Im Zusammenhang mit den Vorfällen bei der Telekom standen insbesondere der Fernkonfigurationsdienst nach TR-069 und die Freigabe des dazugehörigen Ports 7547 über das Netz der Telekom hinaus in der Kritik. Bei entsprechender sicherer Implementierung und Konfiguration ist TR-069 für Heimnetzrouter zum jetzigen Zeitpunkt als sicher zu bewerten. Auch das Update für die Router wurde über TR-069 automatisiert eingespielt. So konnte der Aufwand für die betroffenen Kunden klein gehalten werden. Die Kritik an der Erreichbarkeit der Router über den für TR-069 vorgesehenen Port aus dem Internet kann nur als teilweise gerechtfertigt angesehen werden. Eine netzseitige Sperre der Telekom hätte die Kollateralschäden in Form von Ausfällen verhindern können. Wird aber der für TR-069 standardisierte Port gesperrt, können damit Drittanbieter von Heimnetzroutern über diesen Weg ihren Kunden keine Firmware-Updates und andere Supportleistungen mehr zur Verfügung stellen. Eine Möglichkeit wäre die Beschränkung des Zugriffs auf die Fernwartungsfunktion der Router durch sogenannte Zugangskontrolllisten (ACL), die sich auf den Routern selbst befinden.

1.3 Die Gefährdungslage in der Gesellschaft

Vernetzung und Digitalisierung haben zunehmend Einfluss auf die Gesellschaft und den Alltag der Bürgerinnen und Bürger. IT-Lösungen sind ein selbstverständlicher Faktor in vielen gesellschaftlichen Lebensbereichen. Ein Leben ohne das Internet ist in der heutigen Gesellschaft kaum noch vorstellbar, mobile Geräte wie Smartphones und Tablets werden von Millionen Menschen genutzt.

Der hohe Durchdringungsgrad von IT in allen Bereichen des gesellschaftlichen Lebens ist mit vielen Chancen verbunden, er birgt aber auch Risiken in den Bereichen Sicherheit und Datenschutz. Das Thema Cyber-Sicherheit im Sinne von umfassenden IT-Sicherheitsvorkehrungen und einer verbesserten Handlungsfähigkeit im Falle eines Cyber-Angriffs ist daher die Voraussetzung für eine erfolgreiche Digitalisierung.

Gefährdung durch das Internet der Dinge

Im Rahmen der zunehmenden Digitalisierung hält das Internet der Dinge (Internet of Things, IoT) mehr und mehr Einzug in Haus, Wohnung und den persönlichen Bereich der Anwender. Immer mehr vernetzte Geräte ermöglichen immer neue Anwendungen zur Komfortsteigerung, beispielsweise im Bereich der Haushaltsgerätesteuerung, der Hausüberwachung oder im Gesundheitsmanagement. Gleichzeitig werden ehemals bestehende Hürden für den Endverbraucher abgebaut, indem verstärkt funkbasierte Lösungen oder Powerline-Technologien eine zuvor notwendige Verkabelung ablösen. Dies führt zu einer immer höheren Vernetzungsdichte.

Die IT-Sicherheit spielt bei IoT-Geräten bisher jedoch keine oder nur eine untergeordnete Rolle. Für eine Kaufentscheidung des Kunden sind in der Regel die Gerätefunktionalität und der damit verbundene Komfortgewinn sowie der Kaufpreis ausschlaggebend. Dies führt dazu, dass ein neuer Bereich der Gefährdung entsteht, eine größere Angriffsfläche, die von Cyber-Kriminellen für ihre Zwecke genutzt werden kann.

Die Angriffe auf IoT-Geräte erfolgen in der Regel direkt über das Internet oder über vorhandene Funkschnittstellen „over-the-air“. Hierbei sind verschiedene Gefährdungslagen mit unterschiedlichen Bedrohungen zu unterscheiden:

- Das IoT-Gerät wird angegriffen, um dem Nutzer direkten Schaden zuzufügen. So können zum Beispiel Smart-Home-Komponenten zur Zutrittssteuerung angegriffen und manipuliert werden, um einen Einbruch vorzubereiten. Über eine kompromittierte Webcam können vertrauliche Informationen über die Bewohner und deren Verhalten in Erfahrung gebracht werden.

- Das IoT-Gerät wird kompromittiert und zum Angriff auf andere Infrastrukturkomponenten oder Services missbraucht. Häufig werden ungesicherte oder nicht ausreichend gesicherte IoT-Geräte kompromittiert und zu Botnetzen zusammengeführt, um gezielte DDoS-Attacken gegen Webseiten oder Webservices von Dritten durchzuführen. Hierbei bleibt der Angriff für den Nutzer häufig unentdeckt, da er selbst von dessen Auswirkungen nicht direkt betroffen ist. Diese Vorgehensweise ist etwa beim Mirai-Botnetz zu beobachten.

- Das IoT-Gerät wird durch ein Schadprogramm außer Betrieb gesetzt und ist für den Endnutzer zumindest vorübergehend nicht mehr nutzbar. Hiervon waren in jüngster Vergangenheit speziell kleine und mittelständische Unternehmen (KMUs) betroffen, deren Infrastruktur teils tagelang über das Internet nicht mehr erreichbar war.

Die möglichen Auswirkungen der zuvor genannten Cyber-Angriffe sind vielfältig. Neben direkten Angriffen auf die Privatsphäre, persönliche Daten, Zugangsinformationen sowie Vermögenswerte des Endnutzers führt der Missbrauch von IoT-Geräten durch DDoS-Angriffe auf größere (kritische) Infrastrukturkomponenten und Services zu massiven wirtschaftlichen Schäden.

Gefährdung durch mobile Kommunikation

Für viele Menschen sind Smartphones und Tablets unverzichtbar geworden. Sie bereichern die Kommunikation und Unterhaltung, sie ermöglichen Navigation und Interaktion über soziale Netzwerke. Mit wenigen Handgriffen installierte Anwendungsprogramme – Apps – machen dies möglich. Die immer intensivere App-Nutzung sorgt aber auch dafür, dass auf den Geräten immer mehr, zum Teil sensitive Daten verarbeitet werden. Adressbücher, Standort- und Zugangsdaten, E-Mails und andere Kommunikationsdaten machen Mobilgeräte zu einem immer lohnenderen Angriffsziel für Kriminelle. Ihre Sicherheit wird durch zahlreiche Aspekte beeinflusst:

- Anwender räumen dem Datenschutz und der Sicherheit bei der App-Auswahl oft keine oder bestenfalls eine untergeordnete Rolle ein. Die Kombination von Nützlichkeit und Bequemlichkeit sowie die Kosten sind ausschlaggebend für die Auswahl einer App. Dabei stellt der mögliche Abfluss persönlicher beziehungsweise kritischer Daten einen mit potenziell erheblichen Gefährdungen verbundenen Kontrollverlust dar.

- Die Installation von Software-Aktualisierungen, um Sicherheitslücken zu beseitigen, ist Voraussetzung für den sicheren Betrieb mobiler Endgeräte. Aufgrund der Vielfalt der Gerätetypen, sowohl auf Hardware- als auch auf Softwareebene, ist eine kurzfristige und flächendeckende Versorgung mit Aktualisierungen durch Hersteller und Anbieter allerdings kein einfaches Unterfangen. Trotz Initiativen der Industrie, dies zu beschleunigen, waren im aktuellen Berichtszeitraum viele Mobilgeräte insbesondere mit dem Betriebssystem Android auf einem sicherheitskritischen Softwarestand.

- Ein Teil der auf mobilen Geräten anfallenden persönlichen und sensitiven Informationen wird nicht oder nur unzureichend verschlüsselt und oft in einer Cloud gespeichert. Der Nutzer vertraut somit seine Daten dem Cloud-Anbieter an. Falls der Zugriff nicht ausreichend geschützt ist, können sowohl die Nutzerdaten als auch die Zugangsdaten für die Cloud selbst in falsche Hände geraten.

- Mobilgeräte verbinden sich oft mit öffentlichen Hotspots. Hier werden die Daten in der Regel unverschlüsselt übertragen und können somit von unbefugten Dritten

mitgelesen werden. Eindeutige Nutzerkennungen wie die International Mobile Subscriber Identification (IMSI) sind hiervon potenziell betroffen.

- Betreiber von Mobilfunknetzwerken sowie App-Anbieter sind in der Lage, Mobilgeräte zu orten und damit auch den Standort des Besitzers festzustellen. Schwachstellen in der Infrastruktur des Mobilfunkbetreibers können dazu führen, dass eine Ortung von Mobilfunkgeräten auch durch Dritte möglich ist. Angreifer können so ein umfassendes Bewegungsprofil des Opfers anlegen.

- Nach wie vor können Telefonate, die über die Mobilfunktechnologie der zweiten Generation (2G / GSM) geführt werden, auf der Funkschnittstelle abgehört werden. Auch 3G- und 4G-Funktechnologie ist hiervon betroffen, da der Angreifer in vielen Fällen eine Umschaltung auf 2G-Standard provozieren kann. Nutzerkennungen wie die IMSI können auf der Funkschnittstelle ebenfalls abgegriffen werden.

- Auch die zunehmende Nutzung von SMS als Authentifizierungsfaktor sowie zur Autorisierung von Transaktionen (mTAN-Verfahren) birgt Risiken. Angreifer können durch die Ausnutzung von Schwachstellen in der Netzwerkinfrastruktur den SMS-Verkehr umleiten und so die verschickten Codes missbrauchen. So gab es im Berichtszeitraum etwa Schwachstellen im für den Austausch zwischen Mobilfunknetzen wichtigen SS7-Protokoll und damit die Möglichkeit, SMS-Nachrichten beim Online-Banking abzufangen. Ein entsprechender Missbrauch ist auch durch Schadsoftware auf dem Endgerät möglich.

Die Auswirkungen dieser zahlreichen Schwachstellen auf den Schutz der Privatsphäre und der sensitiven Daten sind ebenso beachtlich wie mannigfaltig. Einerseits können durch den Abfluss persönlicher Daten, sei es durch Apps auf dem Endgerät, beim Netzwerkbetreiber oder Cloud-Anbieter, detaillierte Rückschlüsse über das Verhalten, die Interessen, die Aufenthaltsorte und die Gesinnung des Nutzers abgeleitet werden. Diese Informationen könnten anschließend ohne Zustimmung des Betroffenen beispielsweise zu Werbezwecken verwertet beziehungsweise auf unbestimmte Zeit gespeichert, zu kriminellen Zwecken oder zur Diskreditierung einer Person ausgenutzt werden.

Andererseits sind die Mobilgeräte selbst das Ziel aktiver Angriffe. Sollten Sicherheitsupdates nicht vorhanden oder eingespielt worden sein, kann ein Angreifer, wie bei stationären Rechnern auch, die Kontrolle über das Mobilgerät übernehmen. Neben dem üblichen Missbrauch der Ressourcen (zum Beispiel Einbindung in ein Botnetz) ist das monetäre Risiko von Schadsoftware im mobilen Kontext sehr hoch, da kostenpflichtige Telefonate, SMS-Nachrichten oder andere Premium-Dienste ohne Zutun des Betroffenen ausgeführt werden können.

Erkenntnisse aus Angriffen auf öffentliche Institutionen und Funktionsträger

Die Gefahr einer Beeinflussung der politischen Meinungsbildung bei Wahlen ist insbesondere im Zusammenhang mit den Präsidentschaftswahlen in den USA und Frankreich sowie der Parlamentswahl in den Niederlanden in den Fokus der öffentlichen Diskussion gerückt. Auch in Deutschland besteht die Möglichkeit, dass Täter versuchen werden, die digitalen Medien zur Beeinflussung der öffentlichen Meinungsbildung vor der Bundestagswahl 2017 zu nutzen.

Falschdarstellungen (Fake News) verbreiten sich rasant in den Sozialen Netzwerken und werden teilweise auch von etablierten Medien ungeprüft aufgegriffen. Social Bots (automatisierte Programme, die vortäuschen, Menschen mit echten Identitäten zu sein) sammeln Informationen über Nutzer (zum Beispiel von Facebook), streuen gezielt bestimmte Meldungen (zum Beispiel durch Tweets auf Twitter) und beteiligen sich an Diskussionen, um Mehrheitsmeinungen zu suggerieren und Meldungen zu Top-Themen zu machen.

Darüber hinaus sind Social Bots dazu in der Lage, bestimmten Zielgruppen individualisierte Nachrichten zu schicken, in denen die potentiellen Opfer (zum Beispiel Mitglieder des Wahlkampfteams einer Organisation) dazu verleitet werden sollen, Links zu schadhaften Webseiten aufzurufen. Folgt ein User diesen Links, besteht die Gefahr, dass auf seinem Rechner Schadsoftware installiert wird. So können im nächsten Schritt dort vorhandene vertrauliche Daten abgegriffen werden. Weitere informationstechnische Angriffe mit Hilfe von Social Bots sind denkbar. Beispielsweise könnten durch massenhaft generierte Kommentare Informationsseiten zur Wahl oder von Kandidaten in Sozialen Netzwerken unleserlich beziehungsweise unbrauchbar gemacht werden. Daneben sind noch Identitätsdiebstahl oder weitere Angriffsformen vorstellbar.

Zwar liegen dem BSI keine konkreten Hinweise über geplante Cyber-Angriffe im Zusammenhang mit der Bundestagswahl vor, dennoch muss Deutschland – auch vor dem Hintergrund der Cyber-Angriffe, die es in den USA und in Frankreich gab – auf dieses Szenario vorbereitet sein. Mögliche Ziele für Cyber-Angriffe im Kontext von Wahlen sind insbesondere Parlamente, Abgeordnete, Behörden, Parteien (Zentralen, Geschäftsstellen, Kandidaten), Medien und Medienvertreter sowie für die jeweilige Wahl genutzte IT auf allen föderalen Ebenen.

1.4 Angriffsmethoden und -mittel

Ein wirksamer Schutz vor Cyber-Angriffen ist nur möglich, wenn Gefährdungen im Cyber-Raum sowie die eigene Gefährdungslage zumindest im Überblick bekannt sind. Dieses Wissen ist Voraussetzung, um geeignete präventive und reaktive Maßnahmen gegen diese Gefährdungen 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. Denn Angriffswerkzeuge und -methoden sind einfach und kostengünstig verfügbar und beschaffbar. Neueste Erkenntnisse über Schwachstellen und Angriffsverfahren werden bereits nach kurzer Zeit für Cyber-Angriffe angewendet. Doch trotz der großen Anzahl unterschiedlicher Angriffsziele und möglicher Angriffsmethoden lassen sich Trends und Tendenzen erkennen, die für eine erfolgreiche Abwehr genutzt werden können.

1.4.1 Schwachstellen in Software

Wie auch in den letzten Jahren gab es 2016 / 17 eine hohe Anzahl kritischer Schwachstellen in den vom BSI regelmäßig betrachteten Softwareprodukten (siehe Abbildung 6). Dieser Trend trifft generell auch auf andere, hier nicht explizit berücksichtigte Softwareprodukte zu.

Untersuchungen wie der Coverity Scan Open Source Report zeigen, dass die durchschnittliche Anzahl Fehler je Zeile Quellcode (Defect Density) in den vergangenen Jahren leicht gesunken ist. Das lässt auf eine Verbesserung der Softwareentwicklungsprozesse schließen. Im Gegenzug nimmt aber auch der Umfang der Codebasis von Softwareprodukten zu, so dass bei jedem hinreichend komplexen Softwareprodukt von der Existenz kritischer Schwachstellen auszugehen ist. Dies gilt sowohl dort, wo die Software integraler Teil eines Hardwareprodukts ist, zum Beispiel bei Herzschrittmachern; solche modernen Implantate sind technisch gesehen nichts anderes als eingebettete Systeme, die durch Software gesteuert werden und die bereits vereinzelt erfolgreich gehackt wurden. Dies gilt aber auch dort, wo Software eine optionale Zusatzfunktion eines kombinierten Hard- und Softwaresystems ist (zum Beispiel Office-Paket für ein Smartphone). Da nur ein Teil der gefundenen Fehler beseitigt oder veröffentlicht wird, ist eine Gefährdung durch nicht öffentlich bekannte Schwachstellen, für die es noch keine Sicherheits-Updates gibt, immer latent vorhanden. Daher sollte davon ausgegangen werden, dass die eingesetzte Software immer Schwachstellen enthält, die auch ausgenutzt werden („Assume Breach"– Paradigma).

Schwachstellen-Lebenszyklus

Falls Sicherheits-Updates zeitnah durch den Anwender eingespielt werden, besteht im Allgemeinen keine Gefährdung durch öffentlich bekannte geschlossene Schwachstellen. Dies betrifft den überwiegenden Anteil der vom BSI betrachteten Schwachstellen. Die Responsible-Disclosure-Strategie, nach der sich alle Beteiligten auf eine bestimmte Frist einigen,

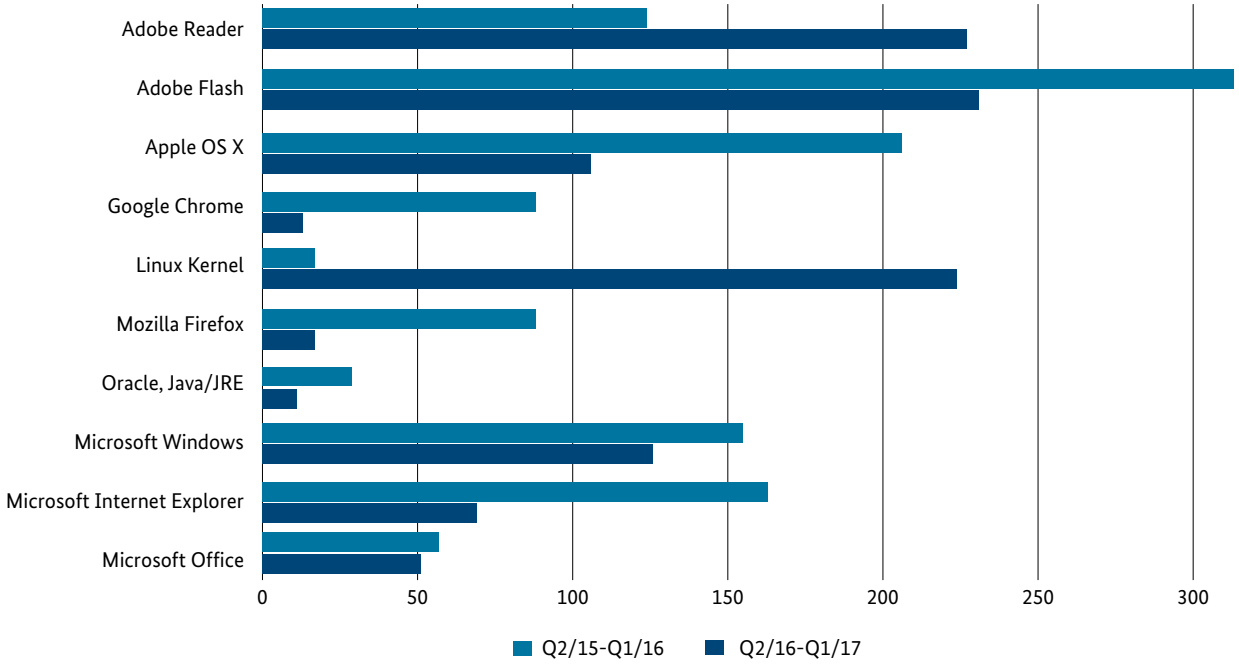


Abbildung 6 Behobene kritische Schwachstellen nach Produkt

Datendiebstahl bei Yahoo

Sachverhalt

Im September 2016 räumte das US-amerikanische Internetunternehmen Yahoo ein, Ende 2014 Opfer eines Cyber-Angriffs geworden zu sein, bei dem Profildaten von 500 Millionen registrierten Nutzern gestohlen wurden. Bis dato handelte es sich hierbei vermutlich um den umfassendsten Diebstahl von Nutzerdaten weltweit. Die dabei erbeuteten Datensätze enthielten neben den Namen der Nutzer auch deren E-Mail-Adressen, Telefonnummern, Geburtsdaten und Passwort-Hashes. Im Dezember 2016 musste Yahoo schließlich bekannt geben, bereits im August 2013 Opfer eines noch viel größeren Datendiebstahls geworden zu sein. Dabei wurden Nutzerdaten von einer Milliarde Benutzerkonten entwendet.

Ursache und Schadenswirkung

Yahoo hat die Passwörter auf zweifache Weise verschlüsselt – über Codierung und mit einer Technik namens Hashing. Doch können Hacker inzwischen gesicherte Passwörter knacken, indem sie riesige Lexika mit ähnlich verschlüsselten Begriffen anlegen und sie mit Datenbanken gestohlener Passwörter abgleichen. Zusätzlich wurde die aktive Ausnutzung einer Schwachstelle bei der Verarbeitung sogenannter Cookies bekannt. Cookies sind kleine Textfragmente mit Informationen über den aktuellen Benutzer, die im Browser gespeichert werden. Hierüber kann ein Benutzer auf Webanwendungen nach einmaliger Anmeldung auch später noch zugreifen, ohne erneut seine Zugangsdaten zu übermitteln. Im Falle von Yahoo war es möglich, diese Cookies zu fälschen. Somit konnten Angreifer ohne Kenntnis der aktuellen Zugangsdaten auf Yahoo-Benutzerkonten zugreifen. Die Sicherheitslücken wurden mittlerweile geschlossen.

Reaktion

Im Interesse der deutschen Nutzer hat das BSI mit Yahoo Kontakt aufgenommen, um Informationen zu Einzelheiten des Angriffs, zum genauen Ausmaß des eingetretenen Schadens sowie zu den getroffenen Maßnahmen zu erhalten. Yahoo! EMEA Ltd. in Dublin verweigerte dem BSI jedoch jede Auskunft und verwies stattdessen an die irische Datenschutzbeauftragte, ohne diese jedoch zur Auskunft an das BSI zu ermächtigen. Daher liegen dem BSI bis heute keine konkreten Informationen vor, welche der Aufarbeitung dieser Vorfälle und schließlich der Beratung und Warnung der Anwender zur Prävention möglicher weiterer, ähnlicher Vorfälle dienen könnten. Ebenso wenig konnte sich das BSI bislang davon überzeugen, ob die von Yahoo getroffenen Maßnahmen zur Gewährleistung der Sicherheit ihrer Systeme im Sinne der Anwender geeignet und ausreichend sind.

Empfehlung

Diese Vorfälle zeigen, welche Ausmaße eine Kompromittierung von Diensteanbietern haben kann. Zudem wird deutlich, dass es zwingend notwendig ist, ein ganzheitliches Sicherheitskonzept zu etablieren. Das BSI ging angesichts der großen Zahl der betroffenen Konten davon aus, dass auch deutsche Nutzer zu den Opfern gehören. Es hat Anwendern, die einen Yahoo-Account haben oder in der Vergangenheit hatten, geraten, das dort genutzte Passwort sowie auch die bei Yahoo angegebenen persönlichen Sicherheitsfragen und Antworten zu ändern und es auch für andere Internet-Dienste, Online-Shops oder Social-Media-Accounts nicht mehr zu nutzen. Angesichts der wiederholten Fälle von Datendiebstahl sollten aber auch die Anwender genauer hinschauen, welche Dienste sie zukünftig nutzen wollen und dabei die Sicherheit zu einem Entscheidungskriterium machen. Auch eine Prüfung durch den Gesetzgeber, ob die bestehenden Auskunftsverpflichtungen der Diensteanbieter ausreichend sind, scheint sinnvoll.

Sicherheitslücken bei 1.000 Onlineshops in Deutschland

Sachverhalt

Cyber-Kriminelle nutzten Sicherheitslücken der E-Commerce-Software Magento aus, um schädlichen Programmcode in Onlineshops einzuschleusen. Dieser spähte Zahlungsinformationen und weitere von Kunden bei einer Bestellung eingegebene persönliche Daten aus und übermittelte diese an die Täter.

Ursache und Schadenswirkung

In zahlreichen Online-Shops waren veraltete Versionen von „Magento“ im Einsatz. Im September 2016 wurden weltweit knapp 6.000 von diesen „Online-Skimming“-Angriffen betroffene Online-Shops identifiziert, darunter auch mehrere Hundert in Deutschland betriebene Shops. Die von den Angreifern ausgenutzten Sicherheitslücken wurden aber von vielen Shop-Betreibern trotz vorhandener Softwareupdates nicht geschlossen. Dies ermöglichte den Cyber-Kriminellen weiterhin, bei Bestellungen eingegebene Daten von Kunden auszuspähen. Bis Januar 2017 stieg die Anzahl bekannter betroffener Onlineshops in Deutschland auf mindestens 1.000 an.

Reaktion

Das CERT-Bund des BSI benachrichtigte im September 2016 die jeweils zuständigen Netzbetreiber in Deutschland zu bekannten betroffenen Online-Shops. Provider wurden aufgefordert, ihre betroffenen Kunden (Shop-Betreiber) entsprechend zu informieren. Der eingeschleuste Code wurde bei vielen Shops jedoch nicht entfernt oder die Shops wurden erneut kompromittiert. Parallel zu einer erneuten Benachrichtigung deutscher Netzbetreiber veröffentlichte das BSI daher im Januar 2017 eine Pressemitteilung, um auch öffentlich auf den Sachverhalt hinzuweisen, die Shop-Betreiber zu sensibilisieren und zum Handeln aufzurufen. Das Umsetzungsgesetz zur NIS-Richtlinie erweitert zudem seit Juni 2017 die Instrumentarien der Provider, in dem die Handlungsbefugnisse deutlich gestärkt wurden.

Empfehlung

Anwender, die von ihren Netzbetreibern oder anderweitig über Software-Sicherheitslücken in eingesetzten Produkten informiert werden, sollten diese umgehend schließen, indem entsprechende Updates ausgeführt werden. Verzögerungen spielen den Cyber-Kriminellen in die Hände, die die Sicherheitslücken weiterhin ausnutzen können. Im März 2017 durchgeführte Stichproben zeigten, dass zahlreiche Shop-Betreiber auf die Warnungen der Provider und des BSI reagiert und den schädlichen Code entfernt sowie die Sicherheitslücken durch ein Update geschlossen hatten.

Wie viele Schwachstellen hat eine Software?

Die Menge der öffentlich bekannten Schwachstellen, wie sie beispielsweise in der CVE-Datenbank aufgeführt sind, ist immer nur eine Teilmenge aller Schwachstellen eines Produkts. Sie lässt keinen Rückschluss auf die Anzahl der nichtöffentlichen Schwachstellen beziehungsweise der noch unentdeckten Schwachstellen zu. Auch kann daraus keine Aussage abgeleitet werden, wie sich neue oder veröffentlichte Schwachstellen entwickeln werden. Darum gibt es auch keine Grundlage für Trendanalysen oder Lagebilder zum Beispiel auf Basis von Daten der CVE-Datenbank. Es gibt auch keine Korrelation zwischen der Art der Schwachstelle und der Zeit, die die Schwachstelle unentdeckt oder nichtöffentlich entdeckt bleibt. Und schließlich sind insbesondere bei der Zählung von CVE-Nummern mehrere Faktoren zu beachten, die einen Vergleich von Zahlen nur bedingt sinnvoll erscheinen lassen:

- Manche Softwarehersteller weisen nur öffentlich bekannten Schwachstellen eine CVE-Nummer zu. Vertraulich gemeldete oder intern gefundene Schwachstellen bleiben ohne CVE-Nummer.
- Andere Softwarehersteller fassen mehrere Schwachstellen zu einer einzigen CVE-Nummer zusammen, es sei denn, eine der Schwachstellen hatte bereits eine eigene CVE-Nummer.
- Ferner werden auch nicht alle Schwachstellen als solche erkannt und eventuell nur als normale Fehlerbehebung eingestuft, wodurch initial eine CVE-Nummer als nicht notwendig erscheint. Bei der späteren Erkennung der Sicherheitsrelevanz wird dann je nach Hersteller manchmal eine CVE-Nummer zugewiesen.
- Ein Wechsel der Zählphilosophie eines Herstellers von Zeit zu Zeit ist nicht unüblich.
- Außerdem sind die Einträge in der offiziellen CVE-Datenbank nur mit erheblicher Zeitverzögerung zu finden.

innerhalb derer eine Schwachstelle beseitigt wird, bevor dann Details veröffentlicht werden, scheint zu funktionieren. Immer seltener werden Informationen zu Schwachstellen veröffentlicht, bei denen der Hersteller erst zeitgleich mit der Öffentlichkeit Kenntnis von der Schwachstelle erlangt.

Wenn hingegen Informationen zu einer nicht geschlossenen Schwachstelle vorliegen, die detailliert genug sind, um von einem Angreifer genutzt zu werden, handelt es sich um eine sogenannte Zero-Day-Schwachstelle. Da nach kurzer Zeit eine Ausnutzung zu erwarten ist, stellen diese eine unmittelbare Gefährdung auch für die Allgemeinheit dar. Eine aktuelle Studie der RAND Corporation geht von einer durchschnittlichen Zeit von 22 Tagen zwischen dem öffentlichen Bekanntwerden einer Schwachstelle und der Verfügbarkeit eines Exploits aus, wobei die Zeitspanne im Einzelfall auch wesentlich kürzer sein kann. Aus diesem Grund ist die schnelle Bereitstellung von Sicherheits-Updates durch den Hersteller und deren schnelle Installation durch den Anwender so wichtig.

Eine Responsible-Disclosure-Vereinbarung (zum Beispiel mit einer Veröffentlichungsfrist von 90 Tagen) ist damit für alle drei Seiten vorteilhaft: Der Finder einer Schwachstelle vermeidet das Risiko für die Ausnutzung der Schwachstelle mitverantwortlich gemacht zu werden, der Hersteller der Software kann in einer angemessenen Zeit den Fehler analysieren und beheben und der Nutzer kann davon ausgehen, dass der Hersteller nicht unbegrenzt lange die Verfügbarkeit eines Patches herauszögern kann.

Bug-Bounty-Programme begrenzt sinnvoll

Es gibt verschiedene Ansätze, die Anzahl offener Schwachstellen in Softwareprodukten zu verringern. Intensive Sicherheitsuntersuchungen oder der Aufkauf von Schwachstelleninformationen (sogenannte „Bug-Bounty-Programme“) können zur Erkennung einzelner Schwachstellen führen, sie sind aber nicht hinreichend, um fehlerfreie Produkte zu erhalten.

Da einem Angreifer im Regelfall eine einzige Schwachstelle genügt, um sie in einem Softwareprodukt auszunutzen, ein Hersteller oder Verteidiger hingegen alle Schwachstellen eliminieren muss, ist die Suche und Beseitigung von Schwachstellen zwar notwendig, aber nicht hinreichend. Es muss davon ausgegangen werden, dass immer Schwachstellen vorhanden sind, die früher oder später erfolgreich ausgenutzt werden können („Assume Breach“).

Für einen angemessenen Schutz sind daher weitere Maßnahmen notwendig, bei deren Umsetzung Schnelligkeit und Qualität abgewogen werden müssen. Hierzu gehört kurzfristig, einzelne Klassen von Exploits wie Stack-Overflows oder Typ-Interpretationsfehler zu verhindern. So können beispielsweise Stack-Overflows durch geeignete Maßnahmen des Programmierers bei der Erstellung von Programmen entweder verhindert werden oder zumindest ihre produktive Ausnutzung unmöglich gemacht werden. Nachhaltiger sind allerdings strategische

Maßnahmen, durch die die Auswirkungen des Angriffs eingedämmt werden können. Je nach Schutzbedarf gehört hierzu beispielsweise eine physikalische Isolation oder Separierung von kritischen Systemen. Unverzichtbarer Anteil eines Maßnahmenkatalogs ist auch eine angemessene Protokollierung in Verbindung mit einer Auswertung, die darauf ausgerichtet ist, Schwachstellenausnutzung zu erkennen. Denn die durch die Separierung aufgebauten Sicherheitsgrenzen dienen nicht nur der Begrenzung von Schäden, sondern können auch zur frühzeitigen Erkennung von Angriffen dienen.

1.4.2 Schadsoftware

Unter dem Begriff Schadprogramme (engl. Malware) werden alle Arten von Computerprogrammen zusammengefasst, die unerwünschte oder schädliche Funktionen auf einem Computersystem ausführen. Die Unterscheidung in Trojaner, Viren, Würmer und so weiter ist dabei heute kaum noch von Bedeutung, die Begriffe werden meist synonym für alle Arten von Schadprogrammen genutzt. Die erfolgreiche Infektion von Systemen mit Schadprogrammen bildet die Grundlage für gängige Geschäftsmodelle der Cyber-Kriminalität wie Ransomware oder Botnetze und wird auch für andere Formen von Cyber-Angriffen wie zum Beispiel APT-Angriffe eingesetzt. Während 2016 noch täglich ca. 350.000 neue Schadprogrammvarianten gesichtet wurden, zeichnet sich aktuell ein Rückgang ab. Von Januar bis Mai 2017 wurden rund 280.000 neue Schadprogrammvarianten pro Tag beobachtet. Insgesamt zeichnet sich nach dem durch die massenhafte Verbreitung von Ransomware-Trojanern geprägten Jahr 2016 derzeit ein deutlicher Rückgang im Versand von Schadprogramm-Spam ab.

Infektionswege

Die häufigsten Infektionswege für Schadprogramme sind E-Mail-Anhänge sowie die vom Anwender unbemerkte Infektion beim Besuch von Webseiten, sogenannte Drive-by-Downloads. Auch der direkte Download von Schadprogrammen per Weblink ist häufiger zu beobachten. Infektionen durch die direkte Ausnutzung anderer Schwachstellen, wie im Fall der Ransomware WannaCry, kommen vergleichsweise selten vor. Zur Infektion setzten die Angreifer häufig auf Schadcode in Form von JavaScript-Dateien. Auch der Schadcode in Form von in Office-Dokumenten eingebetteten Makros ist weit verbreitet. In beiden Fällen wird nach Ausführung des eingebetteten Schadcodes das eigentliche Schadprogramm meist aus dem Internet nachgeladen oder lokal erzeugt.

Erkennen von Schadprogrammen

Klassische, signaturbasierte AV-Produkte bieten nur einen Basisschutz vor Schadprogramminfektionen, da neue Schadprogrammvarianten schneller erzeugt werden, als sie analysiert werden können. Schadprogramm-Spam-Wellen sind oft schon beendet, bevor neue AV-Signaturen erstellt und eingespielt werden konnten.

Die Analyse von Schadprogrammen wird zudem immer öfter durch integrierte Funktionen erschwert, mit denen Ana-

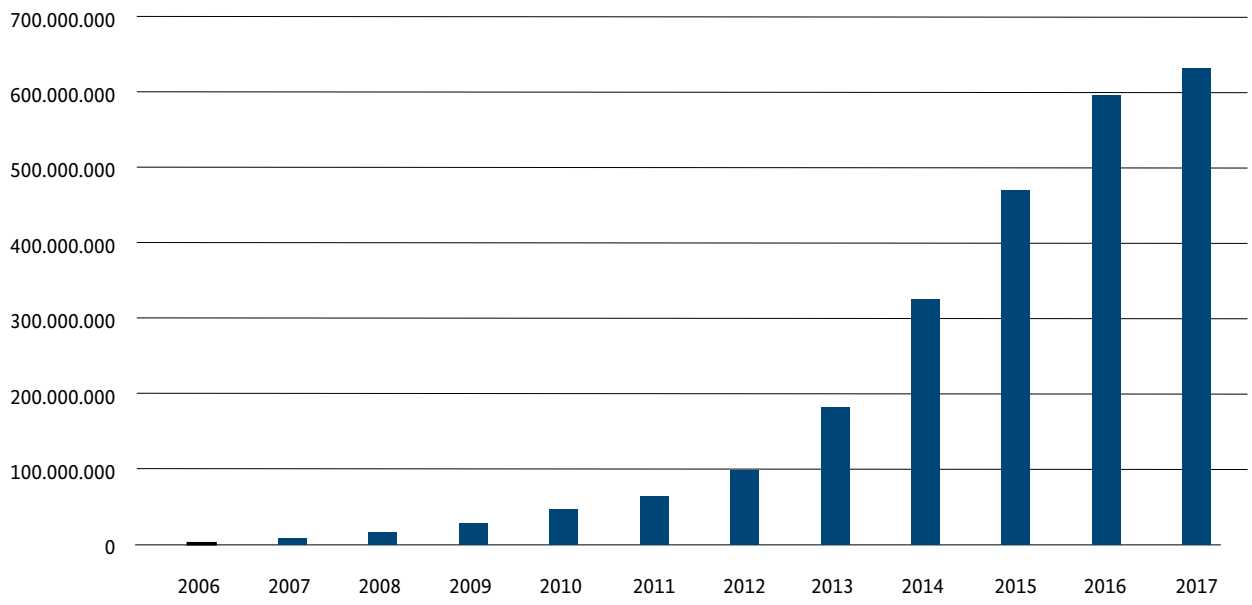


Abbildung 7 Bekannte Schadprogramme (2017 bis Mai), Quelle: AV-TEST

lyse-Tools und -Umgebungen erkannt werden. Auch Makro-Viren nutzen inzwischen verschiedene Techniken, um zu erkennen, ob sie in einer Analyseumgebung ausgeführt werden. Um die Kommunikation eines Schadprogramms zu verschleiern, werden unter anderem kompromittierte Webseiten Dritter als Steuerungsserver und als Verbreitungsweg missbraucht. So wird etwa die gute Reputation einer schon bestehenden, kompromittierten Webseite ausgenutzt, um potenzielle URL-Filter zu umgehen.

Infektionen mit Schadprogrammen, insbesondere mit Ransomware, nach ungezielten Angriffen wurden in der Cyber-Sicherheits-Umfrage 2016 der Allianz für Cyber-Sicherheit von Unternehmen als häufigste Angriffsart benannt, der sie zum Opfer gefallen sind.

Bedrohung weiterhin kritisch

Wie in den Vorjahren sind Schadprogramme auch im aktuellen Berichtszeitraum eine der größten Bedrohungen für Privatanwender, Unternehmen und Behörden. Trotz des zahlenmäßigen Rückgangs kann keine Entwarnung gegeben werden. Aufgrund der fortschreitenden Digitalisierung und Mobilität geraten auch mobile und alternative Plattformen zunehmend in den Fokus der Angreifer.

Durch die fortlaufende technische Weiterentwicklung der Schadprogramme verlieren klassische Abwehrmaßnahmen zunehmend an Wirksamkeit. Mittels teilweise sehr sorgfältig gestalteten Social Engineerings gelingt es den Angreifern, auch aufmerksame Nutzer zur unbeabsichtigten Mitwirkung bei der Ausführung von Schadprogrammen zu gewinnen. Auf klassische AV-Lösungen und Firewalls allein sollten sich IT-Administratoren daher nicht verlassen, sondern IT-Sicherheit als Gesamtkonzept unter Einbeziehung der Nutzer umsetzen.

1.4.3 Ransomware

Ransomware ist ein Schachtelwort aus den englischen Begriffen ransom (deutsch: Lösegeld) und malware (deutsch: Schadprogramm). Es bezeichnet Schadprogramme, die den Zugriff auf oder die Nutzung von Daten, Anwendungen oder Geräten einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes wieder freigeben.

Cyber-Angriffe mittels Ransomware verletzen das Sicherheitsziel der Verfügbarkeit von Daten und Systemen. Gleichzeitig handelt es sich um eine Form digitaler Erpressung.

Man unterscheidet zwischen

- Ransomware, die den Zugang und die Nutzung eines Gerätes sperrt oder unterbindet, zum Beispiel indem die Anzeige mit einem Bild oder einer Webseite überlagert und eine normale Bedienung unterbunden wird, und
- Ransomware, die Nutzerdaten mittels symmetrischer und/oder asymmetrischer Verfahren verschlüsselt und gegen Zahlung eines Lösegeldes den verwendeten Schlüssel oder ein Tool zur Entschlüsselung der Daten verspricht.

Die Lösegeld-Zahlungen werden hierbei vielfach über digitale Währungen wie Bitcoin und anonyme Webseiten im Tor-Netzwerk abgewickelt.

Der Großteil der bekannten Ransomware-Familien zielt weiterhin auf Geräte mit dem Betriebssystem Microsoft Windows. Vereinzelt gibt es auch Ransomware-Familien, die das Desktop-Betriebssystem Apple MacOS oder Web-Server befallen. Auch Ransomware-Varianten für mobile Betriebssysteme wie Google Android werden eingesetzt.

Im Bereich der Desktop-Betriebssysteme wurde seit Juli 2016 hauptsächlich Ransomware mit Verschlüsselungsfunktion detektiert, während Ransomware mit Sperrbildschirm wie LeakerLocker für mobile Betriebssysteme wie Google Android relevant war. In diesen Bereichen unterscheidet sich die Lage im Berichtszeitraum nicht gegenüber dem Vorjahr.

Die primären Angriffsvektoren sind weiterhin Anhänge von Spam-E-Mails sowie Drive-by-Angriffe mittels Exploit-Kits. In einzelnen Fällen wird Ransomware als Programm-Update getarnt und der Anwender so zur Installation verleitet. Ransomware für Mobilplattformen wird überwiegend vom Nutzer selbst installiert (Social Engineering) oder als legitime App getarnt über alternative App-Stores verteilt. Diese Angriffsvektoren sind jedoch nicht neu und werden allgemein zur Verbreitung von Schadprogrammen verwendet. Ein neuer Angriffsvektor im Bereich Ransomware ist die Ausnutzung von Software-Schwachstellen über das Internet und in lokalen Netzen, die im Mai 2017 zur initialen Infektion und Weiterverbreitung der Ransomware WannaCry genutzt wurden.

Sabotage durch Ransomware Petya

Sachverhalt
Ende Juni verbreitete sich eine Schadsoftware namens NotPetya / ExPetr weltweit in Unternehmensnetzen. In Einzelfällen hatte der Angriff massive Auswirkungen auf die Produktion und kritische Geschäftsprozesse von betroffenen Unternehmen. Auch in Deutschland waren mehrere Unternehmen betroffen. Der Schwerpunkt der Cyber-Attacke lag in der Ukraine, dort ereigneten sich die ersten Fälle, insbesondere in Kritischen Infrastrukturen. In der Ukraine gab es bereits mehrfach IT-gesteuerte Sabotage-Angriffe auf Stromnetze, Flughäfen und das Bahnsystem. Die ersten internationalen Fälle betrafen Unternehmen, die Zweigstellen oder Niederlassungen in der Ukraine besaßen.

Ursache und Schadenswirkung
Die Schadsoftware gab vor, Daten zu verschlüsseln und diese gegen Zahlung eines Lösegelds wieder zu entschlüsseln. Sowohl technische als auch strategische Merkmale unterschieden diese Schadsoftware jedoch von anderen Ransomware-Familien. ExPetr nutzte nicht nur wie WannaCry den EternalBlue-Exploit. Zusätzlich umfasste es auch eine Komponente, die Windows-Passwörter aus dem Speicher eines infizierten Systems stahl, sowie ein weiteres legitimes Administrationswerkzeug, das es ermöglicht, sich in einem Netzwerk von einem Rechner zum anderen zu verbinden. So erreichte ExPetr eine Reihe von Unternehmensbereichen, die für Produktion oder operative Tätigkeiten relevant sind.

Ähnlich wie bei WannaCry investierten weltweit Sicherheitsfirmen, Behörden und private Sicherheitsforscher große Aufwände, um ExPetr zu analysieren. Innerhalb kurzer Zeit wurde festgestellt, dass der initiale Verbreitungsweg offenbar eine ukrainische Finanzsoftware namens M.E. Doc war. Die Webseite des Anbieters war kompromittiert worden, sodass über die Auto-Update-Funktionalität der Schadcode an Nutzer der Software übertragen wurde.

Bei der Suche nach Wegen, die Verschlüsselung auch ohne Lösegeldzahlung aufheben zu können, erkannten mehrere Sicherheitsforscher, dass die Ransomware-Funktionalität in bestimmten Teilen nicht vollständig oder grob fehlerhaft implementiert worden war. Dies könnte ein Hinweis darauf sein, dass ExPetr nicht als kriminelles Ransomware-Werkzeug gedacht war, sondern eher als Sabotage-Werkzeug mit strategischer Absicht in der Ukraine eingesetzt werden sollte. Die Verbreitung außerhalb der Ukraine wäre dann unbeabsichtigt gewesen. Dies ist konsistent mit der Beobachtung, dass sich ExPetr nicht über das Internet ausbreitet, sondern lediglich im internen Netzwerk und in bereits geöffneten Verbindungen nach weiteren Opfersystemen sucht. Als Sabotage-Werkzeug ist ExPetr ähnlich effektiv wie Shamoon oder KillDisk, indem es durch Überschreiben wichtiger Festplattenteile das Starten von Rechnern unmöglich macht.

Reaktion
Das BSI hat technische Analysen durchgeführt, sowie im Nationalen Cyber-Abwehrzentrum (Cyber-AZ) eine Bewertung der bekannten Fakten vorgenommen. Entsprechende Informationen und Warnungen wurden an die Zielgruppen des BSI ausgesprochen. Das BSI wies in seinen Warnungen darauf hin, dass ExPetr sich fehlende Sicherheitsfunktionen in internen Netzwerken zunutze macht. Es breitet sich mit Methoden in Netzwerken aus, die als Lateral Movement bekannt sind und sonst vor allem von professionellen APT-Gruppen verwendet werden. Anders als der in Medienberichten geprägte Begriff eines „Killswitches“ empfiehlt das BSI, nachhaltige Konfigurationen vorzunehmen, die das Lateral Movement grundsätzlich unterbinden oder zumindest erschweren.

Empfehlung
Die Cyber-Angriffswelle mit ExPetr hat zum wiederholten Male deutlich gezeigt, wie anfällig auch kritische Geschäftsprozesse in Unternehmen und Institutionen in einer digitalisierten Welt sind. Man wird die Kompromittierung eines einzelnen Rechners nicht immer verhindern können, dies darf jedoch nicht zum Ausfall eines ganzen Netzwerks führen. Das BSI empfiehlt daher, Netzwerke zu segmentieren, lokale Administratorenkonten auf Rechnern zu deaktivieren oder zumindest mit rechnerspezifischen Passwörtern zu versehen. Zudem sollten sich lokale Administratoren nicht über das Netzwerk auf anderen Rechnern einloggen können. Generell sollten Verbindungen zwischen Arbeitsplatzsystemen unterbunden und Daten mittels eigens dafür eingerichteter Fileserver ausgetauscht werden. Nachhaltige Maßnahmen umfassen aber auch, dass Anbieter von Software ihre Update-Mechanismen und die Sicherheit ihrer Webseiten garantieren und pflegen müssen.

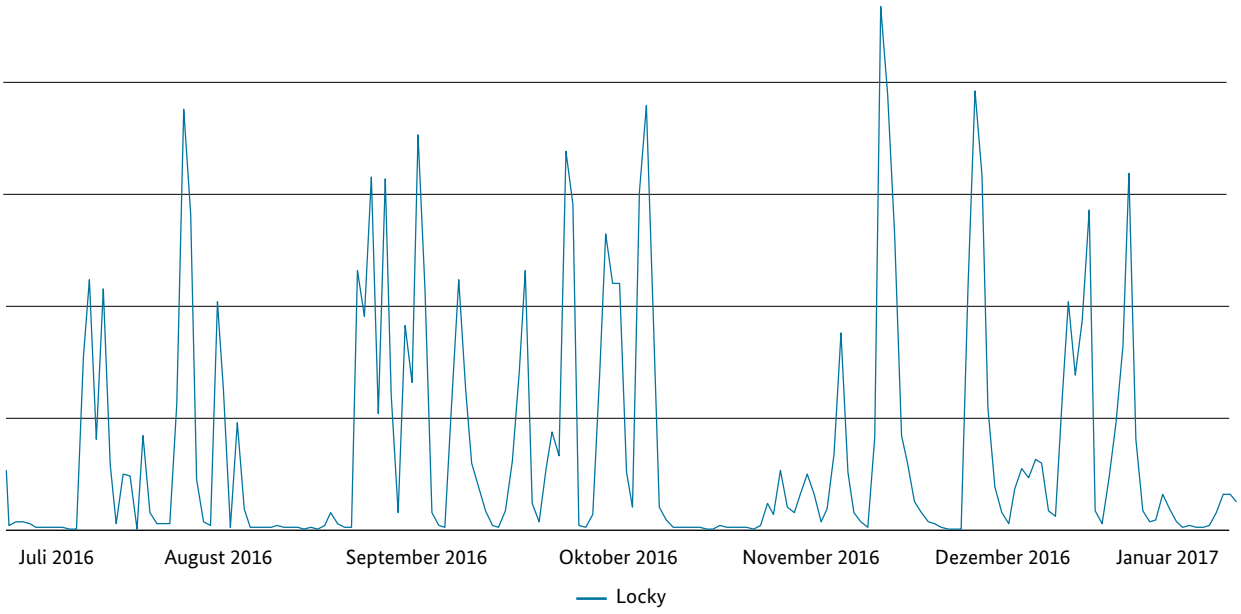


Abbildung 8 Verlauf der Anzahl der vom BSI analysierten Anhänge aus Spam-E-Mails von Juli 2016 – Dezember 2016, die der Ransomware Locky zugeordnet werden konnten

Gefährdungslage schwankt analog zu Spam-Lage

Die dem BSI vorliegenden Detektionsdaten für Ransomware-Infektionen zeigen, dass Deutschland im Berichtszeitraum am häufigsten von den Ransomware-Familien Locky, Cerber, CryptXXX, Crysis sowie Petya / Goldeneye und dem Downloader Nemucod betroffen war.

Die konkrete Gefährdung durch Ransomware in Deutschland schwankt dabei mit der allgemeinen Spam-Lage. Fast täglich gibt es Berichte über neue Ransomware-Typen und -Varianten. Die Webseite https://id-ransomware.malwarehunterteam.com/ listete Anfang April 2017 über 350 Familien allein für Ransomware mit Verschlüsselungsfunktion auf. Diese Vielzahl spielt in der tatsächlichen Gefährdungslage für Deutschland jedoch keine große Rolle.

Für einen Großteil der nach Deutschland versendeten Spam-E-Mails sind Spam-Botnetze wie Necurs verantwortlich. Im Berichtszeitraum gab es wiederholt starke Spam-Wellen, über die Nutzer mit Ransomware infiziert werden sollten. Daneben gab es jedoch auch wiederholt Zeiträume, in denen der Versand von Spam-E-Mail zur Installation von Ransomware ausblieb, einmal im November 2016, zum anderen Anfang 2017 (siehe Abbildung 8).

Beim überwiegenden Teil der Ransomware-Angriffe handelte es sich um ungezielte Massenangriffe. Daneben gab es auch Vorfälle, die auf ein gezielteres beziehungsweise manuelles Vorgehen bei der Infektion mit Ransomware schließen lassen. Ein Beispiel hierfür ist die Ransomware Goldeneye, die im Dezember 2016 gegen verschiedene Organisationen in Deutschland eingesetzt wurde, indem angebliche Bewerbungen auf tatsächliche Stellenausschreibungen per Mail versandt wurden (siehe Infokasten auf S. 28).

Ab dem 12.05.2017 kam es weltweit zu Infektionen mit der Ransomware WannaCry (siehe Infokasten auf S. 26). Im Gegensatz zu bisherigen Ransomware-Angriffen verbreitet sich dieses Schadprogramm wie ein Computer-Wurm selbstständig im internen Netzwerk sowie im Internet ohne Nutzer-Interaktion weiter. Dazu nutzt das Schadprogramm eine Schwachstelle im SMBv1-Protokoll von Microsoft Windows, die im März 2017 von Microsoft gepatcht und im Rahmen der Shadow-Brokers-Veröffentlichungen im April 2017 bekannt wurde. Im weltweiten Vergleich waren die Auswirkungen durch WannaCry in Deutschland begrenzt: Dem BSI wurden Infektionen in KRITIS-Unternehmen sowie bei mehreren Privatpersonen gemeldet.

Eine andere Form digitaler Erpressung im Berichtszeitraum waren Angriffe auf unzureichend abgesicherte Datenbank-Systeme. Hierbei wurden Inhalte kopiert oder gelöscht und es wurde eine Erpressernachricht hinterlassen, dass die Betroffenen eine Kopie der gelöschten Daten gegen Zahlung eines Lösegeldes zurückerhalten könnten. Anfang des Jahres 2017 waren unter anderem MongoDB-, Elasticsearch- und auch MySQL-Installationen von diesen Angriffen betroffen.

WannaCry

Sachverhalt
Mit der Ransomware WannaCry wurde Anfang Mai 2017 eine große Sorge der IT-Sicherheitsgemeinschaft wahr. Ein Schadprogramm, das Dateien verschlüsselt und damit den Betrieb von Systemen und Dienstleistungen bis zur Zahlung einer Erpressungssumme unmöglich macht, kombiniert mit einem Schwachstellen-Scanner, der selbstständig ohne Nutzerinteraktion die Schadsoftware auf andere verwundbare Systeme im internen Netz weiterverbreitet, wurde aktiv. Es war eine „kleine Version" eines Krypto-Wurms.

Ursache und Schadenswirkung
Ausgenutzt wurde eine SMBv1-Server Schwachstelle, für die von Microsoft bereits Mitte März ein Patch bereitgestellt wurde und deren Existenz später im Rahmen von Shadow-Broker-Veröffentlichungen öffentlich bekannt wurde. Aus sicher verschiedensten Gründen wurde der zur Verfügung gestellte Patch jedoch nicht überall eingespielt mit der Folge, dass ungepatchte Systeme für den Angriff anfällig waren. Im Fall von WannaCry war die Zahlungsfunktion, also die versprochene Möglichkeit, gegen Lösegeld ein Entschlüsselungsprogramm zu bekommen, fehlerhaft, sodass jegliche Lösegeldzahlung vergeblich war und es kaum Hoffnung auf Wiederherstellung gab.

In Deutschland wurde mit der Deutschen Bahn ein Unternehmen öffentlich und medienwirksam getroffen, indem Anzeigetafeln an Bahnhöfen ausfielen und die Erpresser-Meldung anzeigten. Wenige weitere Fälle wurden öffentlich bekannt. Wenige Hundert Systeme sind darüber hinaus mit der Double-Pulsar-Hintertüre infiziert, ohne dass die Verschlüsselung aktiv wurde. Entsprechende Informationen werden CERT-Bund (wie auch anderen nationalen CERTs) von der Shadowserver Foundation zur Verfügung gestellt. Die Betroffenen können dann über die zuständigen Netzbetreiber durch das BSI benachrichtigt werden. International war die Betroffenheit in einzelnen Ländern deutlich höher. Vor allem Russland war betroffen, aber auch in Großbritannien waren über 60 Krankenhäuser betroffen, was unmittelbare Auswirkungen auf die Behandlung von Patienten nach sich zog.

Reaktion
Ein überraschender Fehler der Programmierer führte bei WannaCry dazu, dass die Domain, über die die Verschlüsselung ausgelöst wurde, kurzfristig durch einen Sicherheitsforscher „blockiert" werden konnte. Damit wurden zwar Systeme mit einem Teil der Schadsoftware infiziert, aber die Verschlüsselung wurde nicht aktiv. Hierdurch konnte deutlich größerer Schaden verhindert werden.

Herausfordernd bei dem Fall ist, dass der eigentliche Infektionsweg bislang auch international nicht sicher nachvollzogen werden konnte. Der Fall WannaCry war ein mustergültiges Beispiel, wie die Zusammenarbeit national im Cyber-Abwehrzentrum, aber vor allem auch mit den internationalen Partnern des BSI funktioniert: Es gab einen regen Austausch über die jeweilige Betroffenheit, Ausbreitung und (Nicht-)Wirkung. Auch das gerade im Rahmen der europäischen Gesetzgebung (EU-NIS-Richtlinie) frisch gegründete CSIRT-Netzwerk aller europäischen CERTs arbeitet erstmalig länderübergreifend an einem konkreten Fall zusammen. Der Sachverhalt zeigt aber insbesondere auch, dass derartige wurmähnliche Ereignisse mit Sabotagefunktion keine Fiktion sind, sondern trotz der vielen Warnungen und Empfehlungen, Systeme sicher aufzusetzen, tatsächlich vorkommen und zu teils erheblichen Schäden führen. Nur die schnelle Reaktion hat dazu geführt, dass die entstandenen Schäden weit hinter dem möglichen Ausmaß zurückblieben.

Empfehlung
Grundsätzliche Empfehlungen gegen Ransomware-Schadsoftware sind:

- Halten Sie Ihr System auf dem aktuellen Patchstand, damit keine Schwachstellen ausgenutzt werden können. Hierfür bieten die Hersteller für Privatanwender Services an. Für kommerzielle Nutzer sollten in den IT-Dienstleistungsverträgen entsprechende Klauseln für schnellstmögliches Testen und Patchen enthalten sein.

- Sichern Sie regelmäßig die eigenen Daten und die kritischen Systeme, um die Gefahr zu reduzieren, auf Forderungen von Erpressern eingehen zu müssen. Sie können dann Ihre Systeme mit geringstmöglichen Verlusten zeitnah wiederherstellen. Prüfen Sie die gesicherten Backups zudem regelmäßig auf Wiedereinspielbarkeit und üben Sie den Prozess.

- Separieren Sie Ihr Netzwerk in sinnvoll kleine Segmente, sodass eine Betroffenheit eines Systems nicht zu einer vollständigen Infektion des ganzen Unternehmens-/Behördennetzes führen kann.

Weitere Informationen und Handlungsempfehlungen zum Schutz vor Ransomware hat das BSI in einem Dossier zusammengefasst, das auf der BSI-Webseite heruntergeladen werden kann.

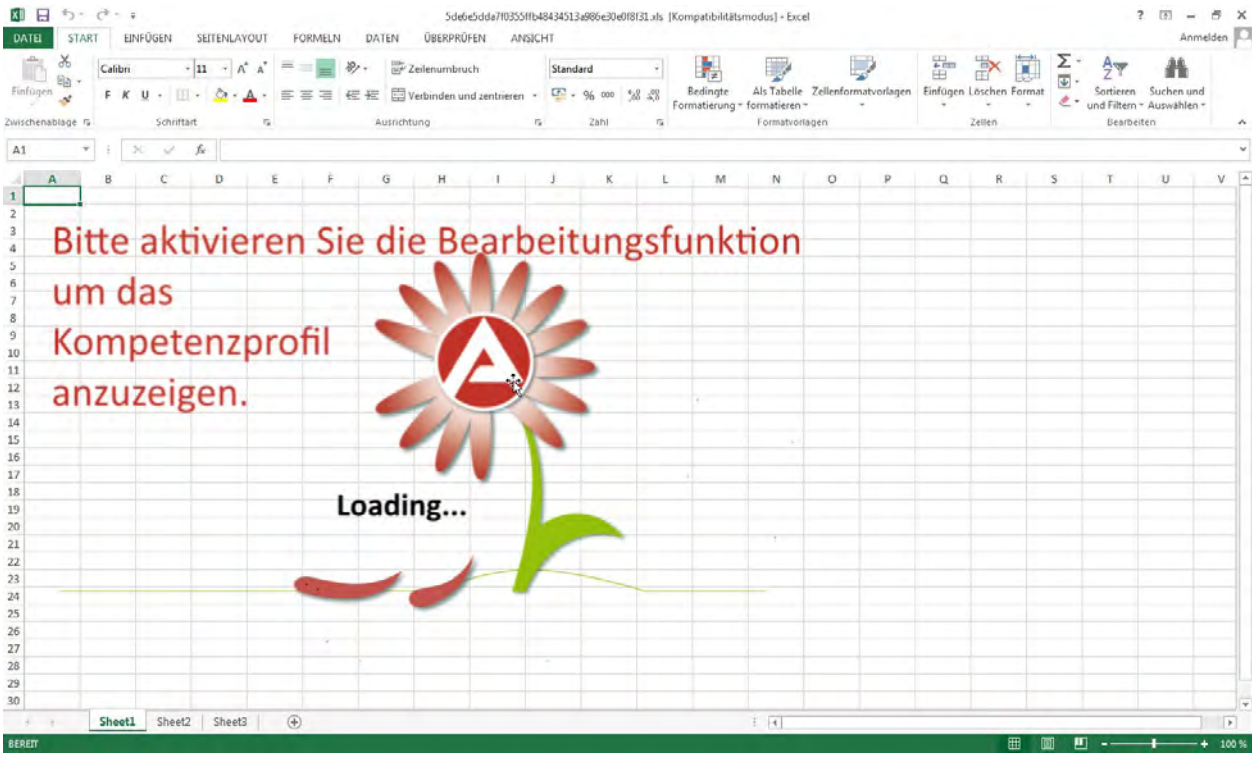


Abbildung 9 Screenshot aus der Goldeneye-Ransomware-Kampagne (Dateiname im Original: „Bewerbung“+Vorname+Nachname+„.xls“)

Weiterhin Geschäftsmodell für Cyber-Kriminelle

Ransomware ist ein etabliertes und erfolgreiches Geschäftsmodell für Cyber-Kriminelle, in dem heute vorzugsweise Ransomware mit Verschlüsselungsfunktion zum Einsatz kommt. Die Vielzahl der beobachteten Ransomware-Varianten zeigt, dass weiterhin in Ransomware investiert wird. Daher ist davon auszugehen, dass dieser Schadprogramm-Typ auch in den nächsten Jahren eine relevante Bedrohung bleiben wird.

Weitere Informationen zum Thema Ransomware hat das BSI im Juli 2016 in einem umfangreichen Lagedossier zum Thema Ransomware zusammengestellt. Das Lagedossier ist auf der BSI-Webseite verfügbar und geht auf Typen und Funktionsweisen von Ransomware ein, stellt die Angriffsvektoren vor und beschreibt Schutzmaßnahmen aus den Bereichen Prävention, Detektion und Reaktion.

Ransomware in Personalabteilungen

Sachverhalt
Cyber-Kriminelle versendeten im Dezember 2016 gefälschte E-Mails mit angeblichen Bewerbungen gezielt an Mitarbeiter in Personalabteilungen von Unternehmen. Die E-Mails enthielten als Dateianhänge ein PDF- sowie ein Excel-Dokument. In dem PDF-Dokument, welches wie eine legitime Bewerbung wirkte, wurden Personalverantwortliche von Unternehmen persönlich angesprochen und es wurde Bezug auf eine tatsächlich offene Position im jeweiligen Unternehmen genommen. Das Excel-Dokument mit der angeblichen Bewerbungsmappe enthielt ein schädliches Makro. Beim Öffnen des Dokuments wurden die Empfänger aufgefordert, die „Bearbeitungsfunktion“ und damit die Ausführung von Makros zu aktivieren.

Ursache und Schadenswirkung
Kam ein Empfänger der Aufforderung auf einem PC mit Windows-Betriebssystem nach, die Bearbeitungsfunktion zu aktivieren, wurde dessen PC mit der Ransomware „Goldeneye“ infiziert. Dabei handelt es sich um eine Weiterentwicklung der Ransomware-Kombination „Petya / Mischa“, die im März 2016 ebenfalls mit gefälschten Bewerbungen verbreitet wurde. Goldeneye verschlüsselt Dateien und modifiziert den Bootsektor der Festplatte. Ein Zugriff auf das System oder die Daten ist anschließend nicht mehr möglich. Die Opfer wurden aufgefordert, über das Internet ein Lösegeld von rund 1.000 Euro in Form von Bitcoins an die Täter zu bezahlen, um ein Entschlüsselungsprogramm zu erhalten. Während bei Petya / Mischa eine Schwachstelle in der Implementierung der Verschlüsselung eine Entschlüsselung der Daten auch ohne Zahlung des Lösegelds ermöglichte, war dies bei der Weiterentwicklung Goldeneye nicht mehr möglich.

Ransomware ist ein für Cyber-Kriminelle seit Jahren etabliertes Geschäftsmodell und betrifft Desktop-Betriebssysteme wie Microsoft Windows und Apple Mac OS, Serversysteme unter Linux sowie mobile Betriebssysteme wie Google Android. Infektionsvektoren von Ransomware für Desktop-Systeme sind aktuell hauptsächlich E-Mail-Anhänge oder Drive-by-Angriffe mittels Exploit-Kits. Bei Ransomware-Vorfällen werden Versäumnisse bei der Prävention deutlich aufgezeigt: Schlecht gepflegte Systeme, fehlende, veraltete oder nicht überprüfte Backups, schwache Administrator-Passworte und fehlende Netzsegmentierung erleichtern den Angriff erheblich und führen zu beträchtlichen Schäden.

Das Schadensausmaß ist davon abhängig, wie die betroffene Institution technisch und organisatorisch vorbereitet ist: Selbst wenn Präventivmaßnahmen nicht gegriffen haben und die Störung nicht abwenden konnten, kann eine gute Bewältigungsstrategie den Schaden erheblich begrenzen.

Reaktion
Je eher die IT-Sicherheitsverantwortlichen einer Organisation über mögliche Anzeichen eines Cyber-Angriffs informiert werden, desto eher können sie die Suche nach den Verursachergeräten in Gang setzen. Und je eher die Verursacher gefunden sind, desto schneller können sie abgeschaltet und der Verschlüsselungsvorgang abgebrochen werden. Kann das IT-Team sicherstellen, dass alle infizierten Geräte identifiziert wurden, kann mit dem Abschalten beziehungsweise Isolieren dieser Geräte auch sichergestellt werden, dass die Gefahr gebannt ist.

Empfehlung
Das BSI hat auf seiner Webseite das „Lagedossier Ransomware“ veröffentlicht, das zahlreiche konkrete Hilfen für die Prävention und die Reaktion im Schadensfall enthält. Damit es nicht zu einem Verlust von Daten kommt, sollten Anwender bereits im Vorfeld Backups anlegen, aus denen der Datenbestand wiederhergestellt werden kann. Um eine Infektion durch Ransomware von vornherein zu vermeiden, sollten vorhandene Schwachstellen in genutzter Software geschlossen und die Anwender für die Thematik sensibilisiert werden. Das Unternehmensnetzwerk sollte segmentiert werden, damit eine einzelne Infektion nicht auf gesamte Netz durchschlagen kann.

1.4.4 Botnetze

Botnetz-Infrastrukturen bieten Cyber-Kriminellen Zugriff auf große Ressourcen an Rechnerkapazität und Bandbreite, die sie für ihre kriminellen Handlungen nutzen können. Aufgrund der Professionalisierung und Kommerzialisierung der Cyber-Kriminalität ist der Betrieb eines Botnetzes auch für technische Laien vergleichsweise einfach und kostengünstig realisierbar.

Auch 2016 und 2017 wurden Botnetze im großen Stil zum Informationsdiebstahl, für Distributed-Denial-of-Service-Angriffe (DDoS-Angriffe) auf Computersysteme, zum Spamversand und zur Verteilung von Schadprogrammen genutzt. Die zugrunde liegende Botsoftware ist in der Regel modular aufgebaut und kann flexibel für verschiedene Angriffszwecke verwendet werden, ohne dass eine Neuinfektion des angegriffenen Systems erforderlich ist.

Im Berichtszeitraum wurden von Sicherheitsforschern täglich bis zu 27.000 Botinfektionen deutscher Systeme registriert und über das BSI an die deutschen Internet-Provider gemeldet. Die Provider informieren ihre Kunden über die Infektion und bieten zum Teil auch Hilfestellung bei der Bereinigung der Systeme an.

Schwerpunkt Online-Banking-Betrug

Die gemeldeten Infektionen verteilten sich im Berichtszeitraum auf 108 verschiedene Botnetzfamilien. Eine genauere Betrachtung der zwanzig häufigsten Familien Anfang März 2017 zeigt, dass der Großteil vorrangig zum Online-Banking-Betrug verwendet wird. An zweiter Stelle folgen Dropper, die einzig dem Nachladen weiterer Schadprogramme dienen. Auf den weiteren Rängen finden sich Botnetzfamilien für Klickbetrug beziehungsweise Bitcoin-Mining, Spamversand und DDoS (siehe auch Infokasten Mirai S. 41).

Aufgrund des hohen Marktanteils sind überwiegend Microsoft-Windows-Systeme von Bot-Infektionen betroffen. Abbildung 10 zeigt eine Verteilung anhand einer Stichprobe Ende März 2017. Als Datenbasis dienen die Botnetzfamilien, die das verwendete Betriebssystem des Opfersystems an einen Sinkhole-Server übertragen. Der hohe Anteil an aktuellen Windows-Versionen zeigt dabei, dass auch neuartige Schutzmechanismen der Betriebssysteme keinen nachhaltigen Schutz gegen Infektionen bieten.

Neben Microsoft Windows rücken zunehmend weitere Betriebssysteme und Hardwareplattformen in den Fokus der Cyber-Kriminellen. Aktuell sind etwa zehn Botnetzfamilien bekannt, die sich ausschließlich auf Android konzentrieren und zum Informationsdiebstahl eingesetzt werden. Jede sechste beobachtete Botnetz-Familie für Windows-Geräte verfügt ebenfalls über eine Schadsoftwarekomponente für Android-Systeme. Sie werden überwiegend beim Online-Banking-Betrug genutzt, um beim mTAN-Verfahren die per SMS gesendete TAN abzufangen. Ende März 2017 handelte

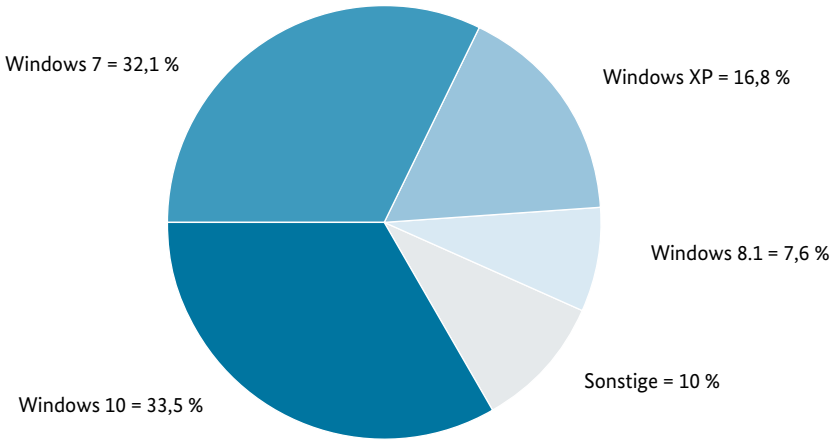


Abbildung 10 Botinfektionen nach Betriebssystemen, Stichprobe 29.03.2017

es sich bei sechs Prozent der gemeldeten Opfersysteme um ein Android-System. Der größte Teil der Android-Infektionen lässt sich dabei auf maliziöse Apps zurückführen, die aus Drittanbieterquellen bezogen wurden.

Darüber hinaus werden neben linuxbasierten Webservern zunehmend auch Geräte des Internets der Dinge wie beispielsweise Heimrouter, Überwachungskameras oder internetfähige Multimediageräte kompromittiert und in Botnetze eingebunden. Vereinzelt wurden auch kompromittierte Systeme auf Basis von Mac OS X beobachtet.

Erfolgreiche Abwehr

Um Botnetz-Infektionen zu detektieren, werden von Sicherheitsforschern sogenannte Sinkhole-Systeme betrieben, die anstelle der regulären Command-and-Control-Server (C&C-Server) die Kontaktanfragen von Bots entgegennehmen. Möglich wird dies durch eine Registrierung der verwendeten Domänennamen oder auch der IP-Adressen. Da nicht für alle weltweit existierenden Botnetze valide C&C-Adressen für Sinkhole-Systeme registriert werden können, stellen die im Berichtszeitraum gemeldeten 27.000

Zerschlagung der Botnetz-Infrastruktur Avalanche

Sachverhalt
Am 30.11.2016 hoben die Zentrale Kriminalinspektion Lüneburg und die Staatsanwaltschaft Verden in einer spektakulären internationalen Operation erfolgreich die Botnetz-Infrastruktur Avalanche aus. Dabei unterstützte sie das BSI maßgeblich. Die Server der Botnetz-Infrastruktur wurden abgeschaltet, Täter wurden verhaftet und Nutzer infizierter Systeme über die Internet-Serviceprovider informiert.

Ursache & Schadenswirkung
Bei Avalanche handelte es sich um die bis dahin größte bekannte Botnetz-Infrastruktur. Mehr als 20 Botnetzfamilien konnten identifiziert werden. Eine international agierende Tätergruppe hatte hunderttausendfach private und geschäftliche Computersysteme mit unterschiedlicher Schadsoftware infiziert. Die Täter nutzten diese Infrastruktur zur Verbreitung von Spam- und Phishing-E-Mails sowie von Schadsoftware wie Ransomware (Erpressungstrojaner) oder Banking-Trojaner.

Reaktion
Die erfolgreiche Aktion ist das Resultat einer über vierjährigen intensiven Ermittlungs- und Analysearbeit. Behörden und Institutionen aus mehr als 30 Ländern waren an der Aktion beteiligt, darunter neben dem BSI auch Europol, das FBI, die Non-Profit-Organisation Shadowserver sowie das Fraunhofer-Institut für Kommunikation, Informationstechnik und Ergonomie (FKIE). Die internationale Zusammenarbeit bei dieser Aktion führte zu sechs Festnahmen, 37 Hausdurchsuchungen und der Beschlagnahme von 39 Servern in verschiedenen Ländern. 221 weitere Server wurden durch die Hosting-Provider abgeschaltet. Über 830.000 Botnetz-Domänen wurden beschlagnahmt oder auf sogenannte Sinkhole-Server umgeleitet. Systeme mit aktiven Infektionen verbinden sich nun zu diesen 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. Diese können dann ihre Kunden schriftlich über die Infektion informieren. Auf diese Weise werden nur Kunden informiert, deren Systeme aktuell infiziert sind und deren IP-Adressen im Verlauf dieser Aktion identifiziert werden konnten. Insgesamt geht das BSI von mehreren Tausend betroffenen deutschen Anwendern aus. 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.

Empfehlung
Auch wenn die Botnetz-Infrastruktur abgeschaltet wurde, kann die Bereinigung der infizierten Systeme bei den Endkunden nur durch diese selbst vorgenommen werden. User, die durch ihren Internet-Provider benachrichtigt wurden, sollten ihre Geräte auf eine Infektion mit Schadprogrammen überprüfen und Sicherheitslücken schließen. Die Schadprogramme auf den betroffenen Systemen wurden durch die Zerschlagung der Botnetz-Infrastruktur nicht gelöscht. Es kann daher nicht ausgeschlossen werden, dass die Täter zu einem späteren Zeitpunkt wieder Kontrolle über die jeweiligen Botnetze erhalten. Betroffene sollten daher möglichst bald handeln. Die abgeschalteten Botnetze bestanden zwar nach aktuellem Kenntnisstand des BSI überwiegend aus Windows-Systemen und Android-Smartphones. Dennoch kann eine Infektion bei Smartphones mit Apple iOS, Microsoft Windows Phone oder Betriebssystemen wie Apple Mac OS X oder Linux nicht ausgeschlossen werden.

Infektionen nur eine Untergrenze für Deutschland dar. Die Höhe der sichtbaren Infektionen wird maßgeblich durch die Art und Anzahl der von den Sicherheitsforschern registrierten Sinkhole-Adressen beeinflusst und schwankt deshalb sehr stark. Aufgrund der Erfahrungen aus erfolgreichen Botnetz-Abschaltungen ist davon auszugehen, dass die Dunkelziffer deutlich höher liegt und sich mindestens in einem sechsstelligen Bereich bewegt.

Der erfolgreiche Schlag gegen die Avalanche-Botnetz-Infrastruktur (siehe Infokasten Seite 31) hat nachdrücklich demonstriert, dass eine erfolgreiche Bekämpfung von Botnetzen die Zusammenarbeit von Strafverfolgern, Behörden und Sicherheitsforschern erfordert und dabei drei Säulen gleichzeitig adressiert werden müssen:

I. Abschalten der Infrastruktur sowie Sinkholing der Malware-Domänen

II. Ermittlungen gegen Kriminelle mit Festnahmen und Durchsuchungen

III. Information von Betroffenen mit infizierten Systemen

Nach dem Takedown der Avalanche-Infrastruktur sind die Endanwender gefordert, ihre Systeme zu bereinigen. Seit Ende November 2016 werden versuchte Botzugriffe auf ehemalige Avalanche-Server auf einen Sinkhole-Server umgeleitet. Die Zugriffsversuche werden durch das BSI an die deutschen Internetprovider gemeldet, damit diese ihre Kunden informieren. Die Bereinigung der Kundenrechner kann nur durch die jeweiligen Nutzer erfolgen, diese Aufgabe kann weder der Provider noch das BSI übernehmen. Das Sinkholing der Malware-Domänen endet voraussichtlich Ende 2017. Wenn Nutzer bis dahin trotz Benachrichtigung ihre Systeme nicht bereinigt haben, besteht die Gefahr, dass Kriminelle die zwar inaktiven, aber immer noch infizierten Systeme übernehmen. Es zeigt sich bereits jetzt, dass die Bereinigung aller Endsysteme eine große Herausforderung ist und viele Anwender trotz Benachrichtigung nicht reagieren. So werden auch sieben Monate nach Beginn des Sinkholings und der konsequenten Information der Betroffenen durch die Provider täglich immer noch mehr als 2.100 IP-Adressen an Provider in Deutschland gemeldet. Das entspricht etwa 46 Prozent der ursprünglich in Deutschland erkannten Infektionen. Der höchste beobachtete Infektionswert lag zwischenzeitlich sogar bei 13.340 eindeutigen IP-Adressen. Weltweit sind nach den erkannten IP-Adressen sogar immer noch über 62 Prozent der Systeme unverändert infiziert.

Das Gesetz zur Umsetzung der europäischen Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-RL) gibt den Telekommunikations-Providern seit Juni 2017 zusätzliche Befugnisse, solche infizierten Systeme vom Netz zu nehmen.

Bedrohungslage weiterhin hoch

Wie die aktuellen Entwicklungen zeigen, ist die Bedrohungslage durch Botnetze im Vergleich zum Vorjahr weiterhin hoch. Das IoT-Botnetz Mirai hat 2016 die Bedrohung, die in diesem Zusammenhang von dem Internet der Dinge ausgeht, eindrucksvoll veranschaulicht (siehe Infokasten Mirai S. 41). Dabei fällt einerseits die hohe Anzahl unzureichend geschützter, öffentlich erreichbarer Systeme auf, andererseits die Schlagkraft der Angriffe, die von dieser Art Botnetze ausgeht.

Aufgrund der Veröffentlichung des Mirai-Quellcodes im Herbst 2016 sind zudem zahlreiche Mirai-Weiterentwicklungen entstanden, die kontinuierlich versuchen, neue Opfersysteme zu finden und zu akquirieren. Dieser Quellcode kann nun auch von Jugendlichen ohne nennenswerte Computerkenntnisse, sogenannten Skriptkiddies, genutzt werden. Hierdurch sind Botnetze aus IoT-Geräten zur Normalität geworden. Hinzu kommt, dass Necurs, eines der größten bekannten Botnetze, das unter anderem für große Mengen Spam-Mails verantwortlich ist, über DDoS-Funktionalität verfügt. Durch diese Faktoren steigen die Eintrittswahrscheinlichkeit und die Auswirkung von DDoS-Angriffen.

Mirai

Ende September 2016 wurde überraschend der Mirai-Quellcode veröffentlicht. Es handelte sich dabei um den vollständigen Quelltext inklusive einer Anleitung, so dass auch Laien diesen sehr einfach erweitern und in ausführbaren Code umwandeln können. Teil des Quellcodes waren auch Listen von Kennungen und Kennwörtern verwundbarer IoT-Systeme. Ein Nutzer unter dem Pseudonym „Anna-senpai“ erklärte, dass die Malware für ihn ihren Dienst erledigt hätte und er sich aus dem DDoS-Geschäft zurückziehen wolle. Seitdem wurde der Quellcode ungehindert weiter verbreitet und für diverse Weiterentwicklungen verwendet, so dass aktuell mehrere Hundert Botnetze in unterschiedlicher Größe und Ausgestaltung existieren, die im Funktionsumfang erweitert und technisch optimiert wurden.

1.4.5 Advanced Persistent Threats (APT)

Der Begriff „Advanced Persistent Threat“ (APT) wird häufig mit nachrichtendienstlichen Akteuren gleichgesetzt. Das Ziel von APTs ist es typischerweise, Informationen im staatlichen oder gesamtwirtschaftlichen Interesse zu erlangen. Die Vorgehensweise ist dabei zielgerichtet, erfolgt über längere Zeiträume und bedarf häufig wegen großer manueller Aufwände einer größeren Personalstärke. All dies ist konsistent mit den Charakteristiken, die man Nachrichtendiensten zuschreibt.

Seit jeher gibt es jedoch auch Anzeichen dafür, dass manche APT-Kampagnen nicht direkt von Nachrichtendiensten, sondern vielmehr von gut organisierten nichtstaatlichen Gruppen durchgeführt werden.

APT-Angriffe durch kommerzielle Dienstleister

Sicherheitsunternehmen haben in den letzten Jahren immer wieder Berichte über großangelegte, weltweite Cyber-Spionage-Kampagnen vorgelegt. Mehrere dieser Kampagnen waren allerdings in der Auswahl der Unternehmensbranchen und Regierungsorganisationen sehr unspezifisch. Es war daher zweifelhaft, dass ein konkreter Nachrichtendienst ein Interesse an dieser breiten Zielauswahl haben könnte. Hinzu kam die Beobachtung, dass manche Gruppen auch an Wochenenden und in den (lokalen) Nachtzeiten aktiv sind. Beide Phänomene werden von Sicherheitsfirmen als Indiz gewertet, dass solche Kampagnen von Dienstleistern durchgeführt werden. Im englischen Raum haben sich dafür Begriffe wie „Contractor“ (Auftragnehmer), „Hackers for hire“ (Hacker zum Mieten) und auch das plakative „Gunslingers“ (Revolverhelden) durchgesetzt.

Eine der ersten Vermutungen, dass es sich bei dem Angreifer um selbständige Dienstleister handeln könnte, stammt aus dem Bericht des US-Unternehmens Symantec zu der Gruppe Hidden Lynx (September 2013). Auch die Gruppen APT3 / GothicPanda und Nitro / DynamitePanda werden von Sicherheitsfirmen als Dienstleister klassifiziert. Es ist denkbar, dass mehrere Nachrichtendienste desselben Staates auf dieselben Dienstleister zugreifen.

Eine ähnliche Form sind sogenannte APT-Boutiquen, die professionelle Cyber-Spionage-Software entwickeln und an Unternehmen oder Staaten verkaufen. Hierbei gibt es verschiedene Formen der Transparenz. Während Unternehmen wie FinFisher oder Hacking Team keinen Hehl daraus machen, dass sie solche Software entwickeln und verkaufen, gibt es auch Entwickler wie die von Kaspersky aufgedeckte Poseidon-Gruppe, die eher im Verborgenen agieren und ihre Dienste offenbar nicht an Regierungen, sondern an Unternehmen verkaufen.

Während der Begriff des „Contractors“ noch eine (im Sinne des Auftraggebers) legale Konstellation nahelegt, gibt es auch APT-Gruppen, die eine starke Überschneidung mit kriminellen Aktivitäten aufweisen. Ein Beispiel hierfür ist die Gruppe Winnti, die nach der Malware benannt wurde, mit deren Einsatz sie bekannt wurde. Die Täter generierten seit 2007 vor allem sogenannte „Fake-Anti-Viren-Schadsoftware“, um Opfer dazu zu bewegen, eine Lizenz für gefälschte Sicherheitssoftware zu bezahlen. Etwa 2013 zeichnete Kaspersky in einer Analyse nach, wie die Winnti-Gruppe Spielehersteller angriff, dies allerdings auch noch mit eindeutig finanziellen Interessen. Seitdem haben sich die Angriffe mittels Winnti diversifiziert und wurden auch in Vorfällen bei Unternehmen beobachtet, die eher Cyber-Spionage-Charakter haben. 2016 wurde beispielsweise öffentlich bekannt, dass es bei einem deutschen Industriekonzern zu Datenabflüssen durch Winnti gekommen ist.

Vermischung von Interessen

Diese Beispiele zeigen, wie fließend die Grenzen zwischen Kriminalität und Cyber-Spionage sind. Möglich ist sogar, dass Nachrichtendienste eines Staates das vergleichsweise komfortable und professionelle Schadprogramm Winnti nutzen, um ihren Aktivitäten den Anschein rein krimineller Aktivität zu geben. Beispielsweise berichtete die Sicherheitsfirma FireEye, dass nach juristischen und diplomatischen Maßnahmen der USA gegen China die beobachtbare Aktivität der meisten China zugeschriebenen APT-Gruppen stark nachgelassen hat.

Am deutlichsten wäre die Vermischung von finanziell motivierten kriminellen Gruppen und Staaten, wenn sich die von Sicherheitsunternehmen geäußerte Vermutung bestätigen sollte, dass die Lazarus-Gruppe gefälschte Überweisungen im SWIFT-Netz der Banken im Auftrag des nordkoreanischen Staates durchgeführt hat. Eine ähnlich deutliche Vermischung zeigt sich darin, dass das eigentlich für Online-Banking-Betrug benutzte kriminelle GameOver-Zeus-Botnetz in der Ukraine mit Suchbegriffen gefüttert wurde, die auf Spionage hindeuten. Sicherheitsforscher vermuten, dass die Betreiber des Botnetzes mit diesen Suchbegriffen im Auftrag eines Nachrichtendienstes gearbeitet haben.

Die fließenden Grenzen zwischen APTs und Crimeware führen auch dazu, dass Techniken aus Spionage-Angriffen inzwischen auch in kriminellen Kampagnen genutzt werden. So betreibt die Carbanak-Gruppe bei ihren Angriffen auf Banken das sogenannte Lateral Movement, um sich im internen Netzwerk auszubreiten, bis sie fingierte Überweisungen auslösen kann. Selbst bei Ransomware wie Samsam wurde Lateral Movement beobachtet: Die Täter breiteten sich so lange im internen Netzwerk aus, bis sie auf Server stießen, die sensible Daten enthielten, sodass eine Verschlüsselung der Daten mit hoher Wahrscheinlichkeit zur Zahlung des Lösegelds führen würde.

Schwierige Täterzuordnung

Diese Sachverhalte zeigen, dass es im Cyber-Spionage-Bereich strukturelle Überschneidungen zwischen Kriminellen und Nachrichtendiensten gibt. Sowohl Kriminelle als auch staatliche Akteure sind zu professionellen Angriffen fähig. Auch die Beauftragung krimineller Gruppen durch Nachrichtendienste ist denkbar. Da Techniken und offenbar auch Schadcodes ausgetauscht werden, kann man bei tiefgreifenden Netzwerkkompromittierungen anhand der eingesetzten Methoden nicht mehr auf einfachem Weg zwischen Crimeware und Spionage-Angriff unterscheiden. Es bedarf aufwändiger technischer Analyse, vieler Informationen zu konkreten Vorfällen bei Organisationen sowie einer Reihe von Erkenntnissen und Maßnahmen außerhalb des Cyber-Raums, um eine belastbare Zuordnung zu Tätern vornehmen zu können.

Die technischen Gegenmaßnahmen sind jedoch in beiden Bereichen zu großen Teilen identisch. Beispielsweise erhöhen die im Ransomware-Dossier des BSI genannten Maßnahmen zur Abwehr von schadhaften E-Mail-Anhängen auch die Schutzwirkung gegen viele gezielte Angriffe. Generell sollten in einem ersten Schritt zunächst täteragnostische Sicherheitsmaßnahmen umgesetzt werden. Dazu zählen sowohl präventive als auch Maßnahmen zur Detektion erfolgter Kompromittierungen. Erst wenn diese Maßnahmen eingeführt wurden, kann nach einer Analyse der eigenen Exposition und Risikosituation gezielt Threat Intelligence eingekauft werden, um bestehende Monitoring-Lösungen mit Signaturen und Informationen zu ergänzen.

1.4.6 Social Engineering

Immer wenn Angreifern dank aktueller Software sowie Firewalls und Virenscannern keine Kompromittierung mittels technischer Angriffe auf Sicherheitslücken gelingt, fokussieren sie sich auf den Faktor Mensch als vermeintlich schwächstes Glied in der Sicherheitskette. Analog zum klassischen Trickbetrug wird so versucht, mittels manipulativer Methoden die Opfer zu bewegen, Schadsoftware zu installieren oder sensible Daten herauszugeben. Die unterschiedlichen Varianten dieser Social Engineering genannten Vorgehensweise nutzen Strategien wie zum Beispiel das Vortäuschen einer persönlichen Beziehung zum Opfer, ein Gewinnversprechen oder andere lukrative Möglichkeiten wie etwa beim Online-Shopping.

Gezielte Angriffe auf Unternehmen oder Mitarbeiter

In den letzten Jahren wurden meist breit gestreute Phishing-Kampagnen durchgeführt, die beispielsweise mit einem Gewinnspiel lockten oder über eine Paketzustellung informieren wollten. Heute ist der Anteil der gezielten Phishing-Angriffe – das sogenannte Spear-Phishing – deutlich größer, bei denen einzelne Unternehmen oder Mitarbeiter adressiert werden. Dabei nutzen Angreifer eine Vielzahl öffentlicher Quellen wie die Firmenwebseite oder soziale Medien, um möglichst viele Informationen über das anvisierte Unternehmen und den jeweiligen Mitarbeiter zu sammeln und anschließend Phishing-Mails möglichst authentisch wirken zu lassen. Diese gezielten Phishing-Angriffe werden nicht mehr ausschließlich über E-Mail getätigt, sondern werden zunehmend durch Kontaktaufnahmen in sozialen Medien oder Telefonanrufe flankiert, bei denen eine dem Opfer bekannte Identität vorgetäuscht wird. Um den Anschein der Vertrauenswürdigkeit zu erwecken, setzen die Angreifer dabei häufig auf die Reputation etablierter Unternehmen oder Marken. Hierzu werden auch unter falschem Namen Waren in Verkaufsplattformen angeboten oder manipulierte Apps in Appstores publiziert. Häufig wird bei Social Engineering auch der Name von bekannten Behörden oder anderen öffentlichen Einrichtungen missbraucht. Dies senkt die Hemmschwelle der Opfer, einen Link oder Dateianhang anzuklicken oder von der in einem Marktplatz üblichen Bezahlmethode abzuweichen.

Phishing-Angriffe werden zunehmend in Bereichen beobachtet, in denen es üblich ist, E-Mails von Unbekannten zu erhalten. Dies gilt insbesondere bei den verbreiteten maliziösen E-Mail-Kampagnen mit Fokus auf Personalabteilungen, bei denen auf real existierende Bewerbungsverfahren Bezug genommen wird.

Eine verbreitete Angriffsmethode ist auch die Support-Masche, bei der sich Anrufer als Callcenter-Mitarbeiter von renommierten Herstellern wie Microsoft, Dell oder Lenovo ausgeben. Unter dem Vorwand, ein seitens des Herstellers erkanntes Problem auf dem Rechner des Opfers beheben zu wollen, wird das Opfer zur Installation einer Fernwartungssoftware verleitet. Folgt das Opfer dieser Anweisung des angeblichen Technikers, so erlangt der Angreifer die vollständige Kontrolle über den Rechner des Opfers.

Sensibilisierung als probates Gegenmittel

Social Engineering ist nach wie vor eine häufig genutzte Methode der Angreifer. Dies erklärt sich insbesondere dadurch, dass es durch den Angriffsvektor über die „Schwachstelle Mensch“ nicht erforderlich ist, Schwachstellen in Hardware oder Software auszunutzen oder technische Sicherheitsmaßnahmen zu umgehen. Das BSI warnt daher schon seit vielen Jahren vor diesen Angriffsmethoden.

Zu beobachten ist aktuell eine zunehmende Professionalisierung der Angriffe. Sie erschwert immer mehr ein einfaches Erkennen durch Mitarbeiter oder auch durch technische

Spearphishing gegen Spitzenpersonal

Sachverhalt
Das BSI hat im Juni 2017 professionelle Cyber-Angriffe auf private E-Mail-Postfächer von Funktionsträgern aus Wirtschaft und Verwaltung beobachtet. Bei dieser Angriffskampagne werden täuschend echt erscheinende Spearphishing-Mails an ausgewählte Führungspersonen gesandt. Die Angreifer geben vor, Auffälligkeiten bei der Nutzung des Postfachs beobachtet zu haben oder neue Sicherheitsfunktionalitäten anbieten zu wollen. Der Nutzer wird aufgefordert, einen Link anzuklicken und auf der sich öffnenden Webseite sein Passwort anzugeben. Die Kampagne richtete sich gegen Yahoo- und Gmail-Konten. Bereits 2016 konnte das BSI beobachten, dass Webseiten registriert wurden, die sich für Spearphishing-Angriffe gegen Kunden der deutschen Webmail-Dienstleister gmx.de und web.de eignen und deren Infrastruktur der aktuellen Kampagne ähnelt. Zwar waren diese Domains nicht Ziel der Angriffe im Juni 2017, es zeigt aber, dass die Täter diese Mailprovider auch als möglichen Angriffsweg identifiziert haben.

Ursache und Schadenswirkung
Durch die Preisgabe des Passworts erhalten die Täter Zugriff auf das persönliche E-Mail-Postfach eines Opfers und dessen Inhalte. Die Angreifer haben so die Möglichkeit, weitere – gegebenenfalls auch dienstliche – Informationen über die Zielperson zu sammeln und diese für spätere gezielte Angriffe zu nutzen. Mit Zugriff auf das Postfach können die Angreifer zudem auch im Namen des Nutzers kommunizieren und dessen Identität missbrauchen.

Reaktion
In den Regierungsnetzen konnte das BSI einen Angriff der Kampagne abwehren. Grundsätzlich können Phishing-Mails dieser Art in den Regierungsnetzen mit sehr hoher Wahrscheinlichkeit detektiert und abgewehrt werden. Der Schutz privater E-Mail-Postfächer von Funktionsträgern liegt jedoch außerhalb der Zuständigkeit des BSI oder der jeweiligen Organisation. Funktionsträger in Verwaltung und Wirtschaft sollten daher dafür sorgen, dass auch ihre privaten Mail-Accounts abgesichert sind. Dies ist wichtiger Teil des digitalen Persönlichkeitsschutzes.

Empfehlung
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. Folgende Maßnahmen schützen nicht nur gegen gezielte Spearphishing-Angriffe auf Spitzenpersonal, sondern auch gegen großflächige, weniger professionelle kriminelle Phishing-Angriffe:

- Geschäftliche Inhalte sollten nicht über private Postfächer kommuniziert und bearbeitet werden.
- E-Mail-Kommunikation sollte verschlüsselt werden.
- Anwender sollten eine Zwei-Faktor-Authentifizierung nutzen. Manche Webmail-Dienstleister bieten diese Funktionalität bereits an.
- Passwörter sollten grundsätzlich nicht auf Webseiten eingegeben werden, die aus Mails heraus verlinkt wurden.
- Mails, die auf einen gezielten Angriff gegen die geschäftliche Funktion hindeuten, sollten nicht gelöscht, sondern dem IT-Personal der Organisation gezeigt werden.
- Wenn das Passwort auf einer nicht vertrauenswürdigen Seite eingegeben wurde, sollte es im Zweifelsfall auf der Originalseite geändert werden.

Funktionsträger aus Staat und Politik unterstützt das BSI direkt bei der Umsetzung dieser Maßnahmen.

Systeme. Unternehmen setzen zunehmend auf Sensibilisierungsmaßnahmen zur Schulung der Mitarbeiter. Meist werden diese Schulungen aber nur sporadisch angeboten, das heißt, es mangelt an Regelmäßigkeit und dem zeitnahen Hinweis auf aktuelle Methoden und Varianten der Angreifer. Umfassender Schutz gegen Social Engineering kann nur durch kontinuierliche und in ein Gesamtkonzept eingebundene Sensibilisierungsmaßnahmen erzielt werden.

1.4.7 CEO-Betrug

CEO-Betrug ist eine Variante des Social Engineering, die seitens der Angreifer mit großem Aufwand betrieben wird. Dieser erhöhte Aufwand erklärt sich insbesondere durch die potenziell signifikanten Schadenssummen, die Kriminelle erzielen und die in Einzelfällen mehrfache Millionenhöhe erreichen können. Das BSI konnte feststellen, dass diese Betrugsmasche immer ausgefeilter und professioneller eingesetzt wird.

Beim CEO-Betrug wird in besonderem Maße Zielaufklärung betrieben. Zu den technischen Grundfertigkeiten solcher Angreifer gehört die Beschaffung von Informationen über Unternehmen und Mitarbeiter. Dazu werden unterschiedliche Quellen genutzt: die Unternehmenswebseite, Presse- und Börsenmitteilungen, Einträge in sozialen Medien und im Handelsregister. Auch gibt es Fälle, in denen die Angreifer im Vorfeld telefonischen Kontakt mit Mitarbeitern aufgenommen haben, um Ansprechpartner und weitere Details über das Unternehmen in Erfahrung zu bringen. Mitunter werden bei der Durchführung auch Techniken genutzt, die bei einem Anruf dem Opfer eine bekannte Rufnummer vortäuschen.

Zudem werden die an die Opfer versendeten E-Mails mit großer Professionalität und Sorgfalt vorbereitet und zugestellt. Der Angreifer gibt sich als Geschäftsführer (CEO), Finanzchef (CFO) oder ein vergleichbares Mitglied der Geschäftsleitung aus und versucht, das Opfer zur schnellstmöglichen und zugleich vertraulichen Überweisung von größeren Geldbeträgen zu veranlassen. Um das Opfer von der Echtheit der Anfrage zu überzeugen, verwendet der Angreifer häufig korrekte Absenderadressen und imitiert durch Wortwahl, Signatur und Bilder die echten E-Mails aus der Chefetage so gut, dass auf den ersten Blick nichts Ungewöhnliches auffällt. Häufig werden auch real existierende Mitarbeiter als Referenz zur Verifikation der Rechtmäßigkeit der Transaktion angegeben, die das Opfer dann aber angesichts des simulierten Zeitdrucks nicht kontaktiert.

Teilweise werden die dringenden Zahlungsanweisungen in den E-Mails durch Telefonanrufe unterstützt, die von dem angeblichen Mitarbeiter der Managementebene oder einem hinzugezogenen „Berater“ stammen. Damit dieser Betrugsversuch erfolgreich ist, suggerieren Angreifer und „Berater“ dem Opfer einen hohen Zeitdruck, indem sie den Geschäftserfolg oder gar die Existenz des Unternehmens von der zeitnahen Transaktion abhängig machen.

1.4.8 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 ein hohes Sicherheitsniveau erreicht werden kann, kommen vermehrt auch Verfahren auf den Markt, deren Sicherheit nicht das Niveau einer persönlichen Identifizierung und Überprüfung eines Ausweisdokuments erreichen kann.

Unsichere Identifizierung über Videokanal

Insbesondere die vermehrt 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 verändern, 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.

Das BSI hat im Rahmen von Sicherheitsanalysen nachgewiesen, dass es bereits mit Standardequipment effektiv möglich ist, einen gefälschten Ausweis zu erstellen und im Rahmen einer Videoübertragung in Echtzeit den Eindruck entsprechender individueller, optisch variabler Sicherheitsmerkmale zu erzeugen.

CEO-Betrug

Sachverhalt
Dem BSI wurden zahlreiche Fälle von CEO-Betrug gemeldet. Zu den Betroffenen zählen auch Unternehmen der Kritischen Infrastrukturen und Behörden. So wurde eine Mitarbeiterin einer deutschen Landesbehörde per Mail „persönlich beauftragt", eine „vertrauliche Finanztransaktion" in Höhe von 961.000 Euro durchzuführen. Der Mail-Verkehr, der vorgeblich vom Präsidenten des Amtes stammte, wurde durch einen Anruf einer angeblichen Anwältin begleitet, die der Aufforderung Nachdruck verleihen sollte. Der höchste dem BSI bekannte Schaden in einem Einzelfall belief sich auf einen Verlust von 40 Millionen Euro bei einem Automobilzulieferer. Eine europäische Bank hat allein im ersten Halbjahr 2016 von ihren Kunden 50 Fälle von CEO-Betrug gemeldet bekommen. Insgesamt versuchten die Angreifer dabei, über 20 Millionen Euro zu erbeuten. In 20 dieser Fälle wurde der Angriff bereits im Unternehmen verhindert. Bei 20 weiteren Fällen wurden die Zahlungen durch die Bank aufgehalten oder konnten zurückgeholt werden. In den restlichen zehn bekannten Fällen entstand ein Schaden von insgesamt fünf Millionen Euro. Die Dunkelziffer ist deutlich höher.

Ursache und Schadenswirkung
Beim CEO-Betrug werden die Opfer sowohl per E-Mail als auch telefonisch kontaktiert. Ziel des Angreifers ist es, Mitarbeiter eines Unternehmens zur Transaktion eines hohen Geldbetrags von einem Geschäftskonto auf ein fremdes Konto zu verleiten. Zu den Zielgruppen zählen insbesondere Mitarbeiter im Finanz- und Rechnungswesen, die Zugriff auf Unternehmenskonten haben. Im Fokus stehen dabei zunehmend nicht nur international agierende Konzerne, sondern auch Unternehmen aus dem Mittelstand.

Reaktion
Im Zweifel sollte immer der persönliche Kontakt zu dem angeblichen Absender der E-Mail gesucht werden. Zudem kann in solchen Fällen der Betrugsversuch aufgedeckt werden, wenn zum Beantworten der E-Mails nicht der Antworten-Button des E-Mailprogramms verwendet wird, sondern eine neue E-Mail verfasst und an die Adresse der in der Mail genannten Person geschickt wird. Dadurch kann maskierten Absenderadressen entgegengewirkt werden. Weiterhin kann durch Monitoring massenhaftes Empfangen solcher E-Mails entdeckt werden, sodass die Absenderadresse gesperrt werden kann.

Empfehlung
Schutz gegen CEO-Betrug bieten Schulungsmaßnahmen, die die Mitarbeiter für betrügerische und manipulative Verhaltensweisen sensibilisieren. Dabei sollten Mitarbeiter aus kritischen Bereichen wie zum Beispiel der Buchhaltung im Fokus stehen. Als Präventivmaßnahme ist für Zahlungsanweisungen das Vier-Augen-Prinzip zu empfehlen, um zusätzliche Sicherheit zu etablieren.

Empfehlungen umsetzen

Um fehlerhafte Identifizierungen zu erschweren, sollten Anbieter von Video-Identifizierungsverfahren mindestens die folgenden Empfehlungen umsetzen, die das BSI gemeinsam mit Anbietern und weiteren Beteiligten erarbeitet hat:

- Absicherung der Kommunikation (verpflichtende Ende-zu-Ende-Verschlüsselung der Videoverbindung, Umsetzung der Empfehlungen aus der Technischen Richtlinie TR-02102 des BSI)
- Abgleich von Form und Inhalt der optischen Sicherheitsmerkmale mit den auf dem Ausweis enthaltenen Merkmalen und mit Referenzen (mittels Standbildern oder durch technische Unterstützung)
- Zufällige Aufforderung zur Überdeckung und Bewegung des Ausweisdokuments und des Gesichts beziehungsweise des Kopfes, Prüfung auf Artefakte mittels Ausschnittvergrößerung
- Psychologische Fragestellungen und Beobachtungen im Prozess (Plausibilität, Absicht der handelnden Person)
- Automatisierte Gültigkeits- und Plausibilitätsprüfungen der Ausweisdaten.

Um das Sicherheitsniveau unterschiedlicher Verfahren zur Identifizierung einheitlich bewerten zu können, hat das BSI eine Technische Richtlinie verfasst. Damit wird es möglich, aus verschiedenen gleichermaßen geeigneten Verfahren eines bestimmten Vertrauensniveaus (nach eIDAS-Verordnung) auszuwählen. Die Richtlinie kann als Grundlage für eine einheitliche Prüfung etwa durch akkreditierte Konformitätsbewer-

tungsstellen verwendet werden. Dies schafft Rechtssicherheit für Diensteanbieter und vermeidet anwendungsspezifische Zusatzanforderungen. In entsprechenden Fachgesetzen ist dann nur noch festzustellen, welches Vertrauensniveau für den konkreten Einsatzzweck jeweils erforderlich ist.

Aufgrund der beschriebenen Schwachstellen ist davon auszugehen, dass videobasierte Verfahren selbst mit den genannten zusätzlichen Maßnahmen nicht das hohe Vertrauensniveau erreichen können, das bei persönlicher Identifizierung oder Nutzung der Online-Ausweisfunktion des Personalausweises möglich ist. Videobasierte Verfahren sollten daher nicht zur Identifizierung von Personen in sicherheitsrelevanten Bereichen verwendet werden.

1.4.9 Kryptografie

Kryptografie ist nach wie vor ein zentraler Baustein für die Wirksamkeit vieler IT-Sicherheitsmechanismen. Aktuelle kryptografische Mechanismen liefern grundsätzlich ausgezeichnete Sicherheitsgarantien. Zwei Parteien, die ihre lokalen Rechner zuverlässig kontrollieren und kein Geheimnis miteinander teilen, können über ein Netzwerk hinweg eine abhörsichere Verbindung zueinander aufbauen – selbst wenn das gesamte restliche Netzwerk von einem Gegner kontrolliert wird. Bei Verwendung starker Verfahren ist zudem die für den Gegner verfügbare Rechenleistung weitgehend irrelevant.

Allerdings können verschiedene Aspekte dazu führen, dass ein kryptografisches System praktisch versagt. Dazu zählen:

- Mangelnde Sicherheit der Endpunkte
- Fehler in Implementierungen
- Fehler auf Protokollebene
- Sicherheitsprobleme im Zusammenhang einer Rückwärtskompatibilität eingesetzter Protokolle
- Probleme mit der initialen Verteilung öffentlicher Schlüssel oder eine mangelnde Übereinstimmung zwischen Sicherheitszielen und Sicherheitsleistungen der kryptografischen Mechanismen.

Insbesondere Fehler in weit verbreiteten Implementierungen können die Sicherheit vieler Systeme gefährden. Die Tatsache, dass viele Systeme keine oder nur selten Softwareupdates erhalten oder in Sicherheitsanalysen nicht berücksichtigt werden, sorgt zudem dafür, dass Schwächen auch lange nach ihrer Aufdeckung im produktiven Einsatz vorkommen können. Dieser letzte Punkt betrifft vor allem eingebettete Geräte (Internet of Things), Hardwarekomponenten größerer Systeme mit eigener Firmware oder mobile Internetgeräte.

Daneben gibt es eine Reihe von Angriffspfaden, die sich hauptsächlich für gezielte Angriffe auf einzelne Nutzer eignen, zum Beispiel die Extraktion von Schlüsselmaterial durch Seitenkanalanalyse einer Implementierung oder durch Fault-Attacken.

Problematisch ist auch, wenn der Angreifer über kryptoanalytische Fähigkeiten verfügt, die qualitativ über den Stand der öffentlichen Forschung weit hinausgehen. Im Bereich der Public-Key-Kryptografie gehen zudem praktisch sämtliche Sicherheitsgarantien verloren, sobald der Gegner über einen skalierbaren universellen Quantencomputer verfügt, da die zugrunde liegenden mathematischen Probleme (Faktorisierung und Diskreter Logarithmus) durch Shors-Algorithmus auf einem Quantencomputer in polynomieller Zeit gelöst werden könnten.

Sicherheitsvoraussetzungen

Auch beim Einsatz kryptografischer Systeme müssen verschiedene Voraussetzungen erfüllt sein, damit die angestrebten Sicherheitsziele tatsächlich erreicht werden:

- Die beteiligten Parteien müssen ihre eigenen Computersysteme kontrollieren, die kryptografischen Endpunkte müssen gegen Fremdsteuerung oder sonstige Kompromittierung geschützt sein.
- Es muss mindestens eine vertrauenswürdige Verteilung einzelner öffentlicher Schlüssel durch andere Mechanismen gewährleistet sein.
- An den Endpunkten darf die Kommunikation nicht auf direktem Wege überwacht werden können, zum Beispiel über kompromittierende Abstrahlung oder durch Einsatz von Abhöreinrichtungen.
- Die Implementierungen kryptografischer Verfahren müssen mathematisch korrekt und darüber hinaus gegen Angriffe auf Implementierungsebene gehärtet sein.
- Die verwendeten kryptografischen Protokolle dürfen keine Sicherheitslücken enthalten. Dies ist für komplexe Protokolle deutlich schwerer sicherzustellen als die Sicherheit der verwendeten kryptografischen Grundfunktionalitäten wie Blockchiffren oder Public-Key-Verschlüsselungen.
- Die Sicherheitsgarantien zu modernen kryptografischen Mechanismen sind in der Regel sehr stark, aber technisch auch sehr spezifisch. Wenn angestrebte Sicherheitsziele und Sicherheitsgarantien eines kryptografischen Protokolls nicht exakt übereinstimmen, können Sicherheitslücken auftreten.

Kollisionsangriff auf SHA-1

Sachverhalt
SHA 1 (Abkürzung für sicherer Hash-Algorithmus) ist eine standardisierte kryptologische Hashfunktion, die seit vielen Jahren sehr verbreitet ist. Mit einer Hashfunktion soll ein eindeutiger Hashwert für digitale Daten wie zum Beispiel für Nachrichten berechnet werden. Die Idee dahinter: Haben zwei Nachrichten den gleichen Hashwert, sind sie identisch. Hashfunktionen werden daher zum Beispiel als Grundlage zur Erstellung einer digitalen Signatur verwendet.

Im Februar 2017 veröffentlichten Forscher von Google und der Universität Amsterdam einen Artikel über eine praktische Kollision der Hashfunktion SHA-1. Sie hatten als Beispiel zwei PDF-Dateien erzeugt, die einen unterschiedlichen Inhalt haben, jedoch den gleichen SHA-1-Hashwert. Für die inzwischen veraltete Hashfunktion MD5 wurden bereits im Jahr 2005 vom BSI solche PDF-Dateien erzeugt.

Ursache und Schadenswirkung
Die Forscher konnten zeigen, dass SHA1 mit Hochleistungsrechnern gebrochen werden kann. Der Aufwand für diese Kollision ist zwar immer noch enorm, aber ungefähr um den Faktor 100.000 schneller als ein Brute-Force-Angriff ($2^{63.1}$ statt 2^{80}). Die Autoren schätzen die Kosten für die Berechnung einer Kollision auf einen Betrag zwischen 75.000 und 120.000 US-Dollar.

Empfehlung
Dieser konkret durchführbare Angriff auf SHA-1 zeigt erneut, wie wichtig es ist, diese Hashfunktion nicht mehr in Anwendungen einzusetzen, die Kollisionsresistenz benötigen, wie zum Beispiel die Signaturerstellung. Das BSI empfiehlt seit vielen Jahren, SHA-1 nicht mehr für oben genannte Anwendungen einzusetzen, sondern auf aktuelle Hashfunktionen, wie zum Beispiel die SHA-2-Familie zurückzugreifen.

Hohe Sicherheitsstandards

Bis auf wenige Ausnahmen können dem Stand des kryptografischen Wissens entsprechende Krypto-Algorithmen als sicher angesehen werden. Zur Orientierung gibt das BSI hierzu die Technische Richtlinie TR-02102 heraus. Auch viele etwas ältere Verfahren bieten bei richtigem Einsatz noch ein hohes Maß an Sicherheit.

Eine klassische, mathematische Krypto-Analyse ist bei modernen Verschlüsselungsverfahren kaum erfolgreich. Sie bleibt für die Praxis dennoch wichtig, weil die Aufdeckung theoretischer Schwächen in Krypto-Systemen eine Art Frühwarnsystem darstellt, das praktische Schwierigkeiten vermeiden hilft. Zudem haben kryptoanalytische Fortschritte das Potenzial, die Sicherheitsgarantien eines Verfahrens flächendeckend zu entwerten. Es ist insgesamt jedoch als unwahrscheinlich anzusehen, dass kryptografische Verfahren, die derzeit durch die öffentliche Forschung als dem Stand der Technik entsprechend eingeschätzt werden, etwa durch fremde Nachrichtendienste in der Praxis kryptoanalytisch gebrochen werden können.

Neben der legitimen Nutzung kryptografischer Verfahren ist in der letzten Zeit auch die Nutzung durch Kriminelle wieder in den Fokus des öffentlichen Interesses gelangt, etwa im Zusammenhang mit Ransomware. Die Nutzung kryptografischer Verfahren für kriminelle Zwecke, etwa zur Verabredung gesetzwidriger Handlungen, lässt sich technisch kaum unterbinden. Eine Prävention krimineller Anwendungen (vor allem Kryptotrojaner) ist bis zu einem gewissen Grad erreichbar, wenn Staat, Wirtschaft und Gesellschaft in die Lage versetzt werden, ihre Systeme und deren Kommunikation untereinander insgesamt so sicher wie technisch möglich zu konfigurieren. Nicht zuletzt deswegen gibt die Digitale Agenda der Bundesregierung das Ziel aus, Deutschland zum Verschlüsselungsstandort Nr. 1 zu machen.

Entwicklungsstand Quantencomputer

Aktuelle Informationssicherheit basiert unter anderem auf Public-Key-Verfahren wie RSA, ECDSA oder Diffie-Hellman, die mittels eines Quantencomputers gebrochen werden könnten. Diese Gefahr ist durch Warnungen der NSA und einen aktuellen NIST-Standardisierungsprozess für quantencomputerresistente kryptografische Verfahren öffentlich diskutiert worden.

Ein universeller Quantencomputer, der geeignet wäre, den Shor-Algorithmus für aktuell eingesetzte Schlüssellängen und Public-Key-Verfahren einzusetzen, existiert nicht. In den letzten Jahren sind jedoch deutliche Fortschritte zumindest im Bereich der relevanten Grundlagenforschung erkennbar geworden. Um von dieser Entwicklung nicht irgendwann überholt zu werden, muss bereits heute mit den Vorbereitungen für die Post-Quanten-Zeit begonnen werden. Besonders betroffen sind dabei Vertraulichkeitsdienste mit einem langfristigen Schutzbedarf sowie Signaturzertifikate mit langen Laufzeiten.

Neben einer möglichen zusätzlichen Absicherung der klassischen Public-Key-Kryptografie durch ausgewählte symmetrische Kryptoverfahren liegt das Hauptaugenmerk dabei auf der Entwicklung quantencomputerresistenter Public-Key-Verfahren, deren mathematische Basisprobleme auch durch einen Quantencomputer nicht effizient zu lösen sind.

Für die Zukunft sind erhöhte Forschungs- und Standardisierungsaktivitäten im Bereich quantencomputerresistenter Kryptografie zu erwarten, wie etwa das 2016 initiierte „Post-Quantum Cryptography Project“ des National Institute of Standards and Technology (NIST). Eine wichtige Aufgabe für das BSI in den nächsten Jahren wird es sein, diese Aktivitäten aktiv zu begleiten und eigene Projekte umzusetzen. In einer vom BSI vergebenen Studie sollen Forscher der Universität des Saarlandes und der Florida Atlantic University eine fundierte Einschätzung sowie belastbare Prognosen zum aktuellen Entwicklungsstand beziehungsweise der potenziellen zukünftigen Verfügbarkeit eines Quantencomputers erstellen. Konkret werden aktuelle technologische Ansätze und quanten-algorithmische Innovationen intensiv beleuchtet und deren Implikationen im Kontext aktuell eingesetzter Public-Key-Verfahren erörtert. Die Erkenntnisse aus dieser Studie sollen das BSI befähigen, Handlungsbedarf bezüglich der Entwicklung, Standardisierung und Verbreitung quantencomputerresistenter kryptografischer Verfahren festzustellen.

Neben quantencomputerresistenten kryptografischen Verfahren werden auch Verfahren aus dem Bereich der Quantenkryptografie als mögliche Lösung genannt, um sichere Datenverbindungen in einer Welt mit Quantencomputern zu etablieren. Hierbei handelt es sich um technische Systeme, die mittels physikalischer Effekte ein ähnliches Sicherheitsproblem lösen wie Public-Key-Krypto-Verfahren auf mathematischem Wege. Insbesondere benötigen quantenkryptografische Verfahren spezielle Hardware für die Datenverbindung und einen klassischen kryptografisch authentisierten Kanal zur Schlüsselaushandlung. Zudem sind die Sicherheitsgarantien solcher Verfahren stark von Implementierungsaspekten abhängig. Quantenkryptografie wird daher derzeit nicht als praktische oder als sicherheitstechnisch stärkere Alternative zu Post-Quanten-Verfahren betrachtet. Jedoch gibt es international sichtbare Entwicklungs- und Forschungsprojekte, insbesondere existiert in China ein Quantenkryptografie-Programm mit Weltraum-basierten Komponenten (Satelliten).

1.4.10 Seitenkanalangriffe und Zufallszahlengeneratoren

Gute Zufallszahlen sind eine Grundvoraussetzung für die Sicherheit von kryptografischen Mechanismen. Sie werden insbesondere benötigt, um die Schlüssel für die bei der Übertragung und Speicherung kritischer Daten eingesetzten kryptografischen Verfahren zu erzeugen, zum Beispiel Nonces (Einmal-Zufallszahlen), AES-Schlüssel oder RSA-Moduli. Selbst kryptografisch starke Verfahren können durch einen schwachen Zufallszahlengenerator deutlich an Sicherheit verlieren oder sogar gebrochen werden.

Seitenkanäle spielen seit zwei Jahrzehnten in der Wissenschaft und der Halbleiterindustrie eine wichtige Rolle und werden auch im Rahmen von Common-Criteria-Zertifizierungen und Zulassungen betrachtet. Kryptografische Algorithmen und Protokolle werden üblicherweise im Rahmen des Designs rein mathematisch-abstrakt untersucht. Sobald sie aber in reale Kryptogeräte eingebaut werden, kommen neue Angriffsvektoren hinzu. Solche Angriffe versuchen beispielsweise, Vorteile aus der Beobachtung des Geräts zu ziehen, während es Operationen mit beziehungsweise auf geheimen Daten ausführt. Die im Rahmen einer solchen Seitenkanalanalyse aus physikalisch beobachtbaren Größen wie etwa elektromagnetischer Abstrahlung, Stromverbrauch, Laufzeitverhalten einzelner Operationen und Cache-Zugriffszeiten abgeleiteten Informationen liefern entweder bereits den gesuchten Schlüssel oder können als Parameter (neben Geheimtexten und gegebenenfalls auch Klartexten) zur Kryptoanalyse genutzt werden.

Zur Unterstützung von Herstellern, Prüfstellen und Evaluierern hat das BSI Funktionalitätsklassen von Zufallszahlengeneratoren für verschiedene Einsatzzwecke definiert. Die Verwendung dieser Klassen ist unter anderem im Rahmen einer Common-Criteria-Zertifizierung im deutschen Schema verbindlich. Beispielsweise müssen physikalische Zufallszahlengeneratoren von in Deutschland nach Common Criteria zertifizierten Chipkarten einer der definierten Klassen entsprechen.

Darüber hinaus hat das BSI im Rahmen einer Dauerstudie den Zufallszahlengenerator (/dev/random) verschiedener Linux-Kernelversionen untersuchen lassen. Die Studienergebnisse stehen auf der Webseite des BSI zur Verfügung. Auch der Frage, ob bei dem zunehmenden Einsatz virtueller Maschinen, vor allem in Cloud-basierten Lösungen, Zufallszahlen von ausreichender Qualität bereitgestellt werden können, hat sich das BSI in einer Studie gestellt. Auch diese Studie ist auf der Webseite des BSI verfügbar.

1.4.11 Sonstige Angriffsmethoden und -mittel

Abhörtechnik

Gespräche, die über mobile Endgeräte geführt werden, können auf verschiedene Arten abgehört beziehungsweise mitgeschnitten werden. Neben den offiziellen Lawful-Intercept-Schnittstellen des Netzbetreibers, die zum Beispiel von Strafverfolgungsbehörden genutzt werden, können auch unbefugte Dritte mit sogenannten False Base Stations oder durch Ausnutzung von Schwachstellen in der SS7-Signalisierung die Inhalte der Gespräche aufzeichnen. SS7 steht dabei für „Signalisierungssystem Nummer 7“ und ist eine historisch gewachsene Familie von Protokollen. Sie kommen beispielsweise beim Verbindungsaufbau im Falle von Roaming zum Einsatz, wenn eine Signalisierung zwischen unterschiedlichen Komponenten der Mobilfunknetze notwendig ist.

Verschlüsselung kann ausgeschaltet werden

Telefonate und Daten werden auf der Luftschnittstelle zwischen mobilen Endgeräten und Basisstationen in der Regel verschlüsselt übertragen. Dabei kommt in vielen Fällen der mittlerweile unsichere A5/1-Algorithmus zum Einsatz. Mitgeschnittene Daten können somit auch ohne Zugriff auf den Schlüssel entschlüsselt werden. In vielen Fällen, in denen modernere Algorithmen zum Einsatz kommen, kann ein Angreifer mittels einer aktiven False Base Station dennoch die Nutzung des veralteten A5/1-Algorithmus erzwingen oder die Verschlüsselung ganz ausschalten.

Auch ohne den Einsatz einer False Base Station ist es unter Umständen möglich, Gespräche aus der Ferne aufzuzeichnen. Dazu veranlasst der Angreifer zunächst das Mobilfunknetzwerk, die Anrufe eines bestimmten Nutzers auf einen Rechner umzuleiten, auf dem das Gespräch aufgezeichnet wird. Dazu werden SS7-Schwachstellen in der Infrastruktur des Mobilfunkanbieters ausgenutzt.

Wie häufig False Base Stations unbefugt in Deutschland zum Einsatz kommen, wird nicht systematisch erfasst. Da die Kosten einer solchen Anlage in den letzten Jahren stark gesunken sind, ist von einer steigenden Tendenz auszugehen.

Der Erfolg eines SS7-Angriffs hängt im Einzelfall maßgeblich davon ab, ob der Mobilfunkbetreiber, in dessen Netzwerk der Nutzer eingebucht ist, Gegenmaßnahmen ergriffen hat. Je nach Mobilfunkbetreiber variiert darum aktuell das Schutzniveau. Obwohl im Berichtszeitraum immer mehr Mobilfunkbetreiber mit SS7-Firewalls diese Art von Angriffen adressieren, bleibt die Angriffsmethode auf globaler Ebene relevant.

Bedrohungen für industrielle Anlagen

Industrielle Steuerungsanlagen (Industrial Control Systems, ICS) sind durch ihren Einsatz in Kritischen Infrastrukturen sowie in der Fabrik- und Prozessautomatisierung zentrale Elemente unserer Gesellschaft. Ausfälle oder Störungen haben in der Regel gravierende physische Auswirkungen, beispielsweise in Form von Stromausfällen oder Produktionsunterbrechungen. Die Veränderungen der eingesetzten Technologien und der Infrastrukturen im Zuge von Industrie 4.0 nehmen weiterhin zu. Dies gilt auch für die Vernetzung von ICS innerhalb von Unternehmen und über Unternehmensgrenzen hinaus. Weitere Trends sind die Einbindung von Cloud-Diensten in ICS und die Auslagerung steuerungsspezifischer Daten und Prozesse in die Cloud.

Infektionen über Schadsoftware

Immer wieder werden Vorfälle in verschiedenen Produktionssystemen bekannt. Die ungezielten Angriffe sind oft erfolgreich, weil im Unternehmen oft über lange Zeiträume Altsysteme in Einsatz sind und keine geeigneten Prozesse und kein Know-how zur IT-Sicherheit für den Produktionsbereich vorhanden sind. Auf der anderen Seite erhalten Hersteller und Maschinenbauer von den Betreibern keine ausreichenden Informationen über die notwendigen Sicherheitsanforderungen, da diese von den Betreibern selbst weder eingefordert noch entsprechende Ressourcen vorgesehen werden. Zudem fehlt es bei den Herstellern vielfach an Prozessen, um mit Schwachstellen in eigenen Produkten umzugehen, diese zu kommunizieren und für eine Fehlerbeseitigung Sorge zu tragen.

Im Hinblick auf die Art der Angriffe stellen Ransomware und andere Schadsoftware auch im Industrieumfeld ein Problem dar. Die Schadsoftware gelangt meist über infizierte USB-Sticks, Wartungslaptops oder das Unternehmensnetz in das ICS. Da ICS häufig nur mangelhaft vor Schadsoftware geschützt ist oder Sicherheitsupdates nicht installiert wurden, ist eine Infektion oft einfach möglich. Erschwerend kommt hinzu, dass Sicherheitsupdates erst nach Freigabe durch den Hersteller beziehungsweise Integrator und in entsprechenden Wartungsfenstern der Anlage installiert werden können; bis dahin sind die Systeme verwundbar. Diese Problematik hat sich auch im Kontext der Ransomware „WannaCry“ gezeigt. Dabei wurden unter anderem ungepatchte ICS wie zum Beispiel Anzeigetafeln der Deutschen Bahn infiziert und in ihrer Funktion eingeschränkt.

2016 wurden über 120 Schwachstellen in verschiedenen Komponenten oder Software für industrielle Anwendungen öffentlich gemacht. In den ersten sechs Monaten 2017 waren es bereits 110.

Austausch zwischen allen Beteiligten

Die Sensibilität für IT-Sicherheit ist in den letzten Jahren beständig gestiegen. Es ist jedoch notwendig, dass in den Unternehmen entsprechende Ressourcen zur Verfügung gestellt werden, um notwendige Prozesse zur Stärkung der IT-Sicherheit zu etablieren und Vorfälle zu vermeiden. Hier ist insbesondere der Austausch zwischen allen Beteiligten zu nennen. Sicherheitsanforderungen müssen an Maschinenbauer und Hersteller kommuniziert werden, damit sie entsprechende Funktionen in ihren Produkten berücksichtigen und integrieren können. Auf der anderen Seite sind Maschinenbauer und Betreiber in der Pflicht, IT-Sicherheit schon frühzeitig während der Planung zu berücksichtigen sowie Hinweise und Auflagen zu beachten. Gleiches gilt für den Umgang der Hersteller mit Schwachstellen. Einige wenige Hersteller haben gute Prozesse etabliert, informieren die Betreiber und reagieren schnell auf entsprechende Schwachstellenmeldungen. Dies ist auch bei anderen Herstellern notwendig.

Im Speziellen sind Betreiber von Bestandsanlagen gefordert, organisatorische und technische Maßnahmen zu ergreifen, um diese zu schützen. Hier muss auf jeden Fall vermieden werden, diese Bestandsanlagen ohne Schutzmaßnahmen mit schlecht gesicherten Netzwerken (oder gar dem Internet) zu verbinden sowie anderen Risiken, beispielsweise dem dauerhaften Betrieb ohne Updates oder andere risikoreduzierende Maßnahmen auszusetzen.

DDoS-Angriff auf KrebsOnSecurity

Sachverhalt
Am 19. September 2016 meldete Octave Klaba vom französischen Webhoster OVH über Twitter zwei DDoS-Angriffe mit den extrem hohen Bandbreiten von 1.156 und 622 Gigabit pro Sekunde. Das Volumen der Angriffe übertraf die bisher größten verzeichneten Angriffe des DDoS-Mitigation-Dienstleisters Akamai um ein Vielfaches. Am Abend des folgenden Tages wurde das Weblog https://krebsonsecurity.com des Sicherheitsforschers Brian Krebs von einer massiven DDoS-Attacke mit etwa 620 Gigabit pro Sekunde getroffen. Brian Krebs hatte im Vorfeld der Angriffe kritisch über Anbieter von sogenannten Booter-Diensten berichtet, die kostenpflichtige DDoS-Attacken auf beliebige Ziele offerieren.

Ursache und Schadenswirkung
Neben der Größe waren auch die Angriffsmethoden auffällig. So wurde eine Kombination verschiedener Angriffsarten registriert, die bei DDoS-Angriffen in dieser Form bislang nicht vorkam. Aus technischer Sicht handelt es sich bei diesem Vorfall um das erste öffentliche Auftreten des Mirai-Botnetzes. Dieses Botnetz setzt sich überwiegend aus IoT-Geräten zusammen. Neben der schieren Größe des Botnetzes von mehreren hunderttausend Bots überraschte hier auch die technische Umsetzung. So ist Mirai in der Lage, sich selbstständig weiter zu verbreiten, indem bereits infizierte Systeme nach weiteren verwundbaren Geräten suchen und diese dann, wenn möglich, kompromittieren. Dabei wird eine Liste von Standard-Kennungen und -Kennwörtern verwendet, die bei Auslieferung der Geräte gesetzt sind. Systeme, bei denen die Kennwörter nach Auslieferung nicht geändert werden, können so schnell mit Mirai infiziert werden. Daneben gibt es weitere Mirai-Varianten, die Schwachstellen in Implementierungen, beispielsweise bei Routern, ausnutzen. Erfolgreich übernommene Systeme werden in das Botnetz eingegliedert und deaktivieren den Dienst, über den das Gerät kompromittiert wurde. Die Bot-Software selbst bietet neue DDoS-Angriffsmethoden wie GRE Flood oder DNS Water Torture, die durch eine effiziente Implementierung auch auf wenig leistungsfähigen Geräten eine hohe Paketrate erreichen.

Reaktion
Akamai gelang es nach einer Ausfallphase von wenigen Stunden, den Angriff abzuwehren. Da Akamai diese Dienstleistung jedoch im Rahmen eines kostenlosen, freiwilligen Angebots erbrachte, wurde sie aufgrund der anhaltenden Intensität und Dauer der Angriffe sowie der damit verbundenen Kostenaufwände zur Abwehr nicht dauerhaft zur Verfügung gestellt. Google hat sich daraufhin bereit erklärt, Krebs‘ Blog unter den kostenfreien Schutz von Google Project Shield zu stellen. Es ist seit diesem Zeitpunkt wieder dauerhaft verfügbar.

Empfehlung
Aufgrund der freien Verfügbarkeit des Quellcodes sowie der geringen technischen Hürde zum Aufbau eines eigenen Mirai-Botnetzes stellt Mirai eine massive Bedrohung dar. Die Implementierung funktionierender Angriffsmethoden ermöglicht vergleichsweise effiziente Angriffe mit bereits wenigen Tausend Bots. Erschwerend kommt hinzu, dass weltweit eine sehr hohe Zahl an technisch unzureichend gesicherten Systemen existiert, die über das Internet erreichbar und für die Ausnutzung bei solchen Angriffen anfällig sind. Hier besteht dringender Handlungsbedarf bei Herstellern und Anwendern dieser Systeme, um diese abzusichern. Nach Erkenntnissen des BSI finden dauerhaft Scan-Versuche durch Mirai-Systeme statt und ein verwundbares Gerät wird in weniger als einer Minute erfolgreich infiziert. In Deutschland befindet sich ein Großteil der Internetanschlüsse von Privatkunden hinter Routern. Wichtig ist daher, den Router, das Bindeglied zwischen Internet und Heimnetz, so zu konfigurieren, dass ein Durchgriff auf im Heimnetz befindliche vernetzte Geräte nicht möglich ist beziehungsweise dass die vernetzten Geräte keine direkte Freigabe zur Kommunikation über das Internet erhalten.

Distributed Denial of Service (DDoS)

2016 haben sich Medienberichte über Distributed-Denial-of-Service-Angriffe überschlagen. Insbesondere das Botnetz Mirai wurde öffentlich stark wahrgenommen. In diesem Kontext sind insbesondere die Angriffe auf den Blog des Journalisten Brian Krebs, der Angriff auf den DNS-Dienstleister Dyn und der Angriff auf den Hoster OVH zu nennen (siehe Infokasten auf S. 42).

Angriffe im dreistelligen Gigabit- oder gar Terabit-Bereich sind eine ernst zu nehmende Bedrohung. Gleichzeitig sind diese Angriffe allerdings auch Ausnahmeerscheinungen. Im ersten Quartal 2017 sind dem BSI zwei Angriffe in Deutschland bekannt, die jenseits der 100Gbps lagen. Das entspricht 0,005 Prozent der dem BSI bekannten Angriffe. Der Großteil der DDoS-Angriffe hat nach wie vor eine Bandbreite von weniger als ein Gbps (vergleiche Abbildung 11). Während die maximalen Ausschläge für Bandbreite, Paketrate und Dauer stark variieren, sind die durchschnittlichen Werte weitgehend konstant.

In Medienberichten wird häufig auf Angriffe mit hohen Bandbreiten eingegangen. 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 kann. Angriffe auf Anwendungsebene, zum Beispiel TCP-Verbindungen oder HTTPS-Anfragen, können sogar mit geringen Bandbreiten und geringen Paketraten einen erheblichen Schaden verursachen. Wesentliche Bestandteile eines effektiven Schutzes vor DDoS-Angriffen sind neben technischen Möglichkeiten auch organisatorische Maßnahmen. Das BSI hat hierzu entsprechende Cyber-Sicherheitsempfehlungen veröffentlicht.

Schwachstellen in Hardware

Das Kerckhoff'sche Prinzip besagt, dass ein Verschlüsselungsalgorithmus nicht von der Geheimhaltung des Verfahrens selbst, sondern ausschließlich von der Geheimhaltung des Schlüssels abhängen darf. Moderne kryptografische Verfahren halten dieses Grundprinzip vorbildlich ein. Für sie kann nachgewiesen werden, dass es die Lösung eines als schwer angenommenen mathematischen Problems erfordert, um das Verfahren zu brechen.

Allerdings bleibt ein Problem, den Schlüssel zu speichern und unbeobachtbar zu verarbeiten. Hierbei werden oftmals Hardware-Sicherheitselemente eingesetzt, die sich zwangsweise des umstrittenen Prinzips der Sicherheit durch Obskurität bedienen, um die gespeicherten Schlüssel geheim zu halten. Zum Beispiel geschieht dies,

- indem die ausgeführten Operationen per Software verschleiert werden,
- durch kryptografisches Blinding,
- durch physikalisch implementierte Maßnahmen wie eine ausgefeilte Sensorik, die die Betriebsbedingungen ständig überprüft und Angriffe erkennt,

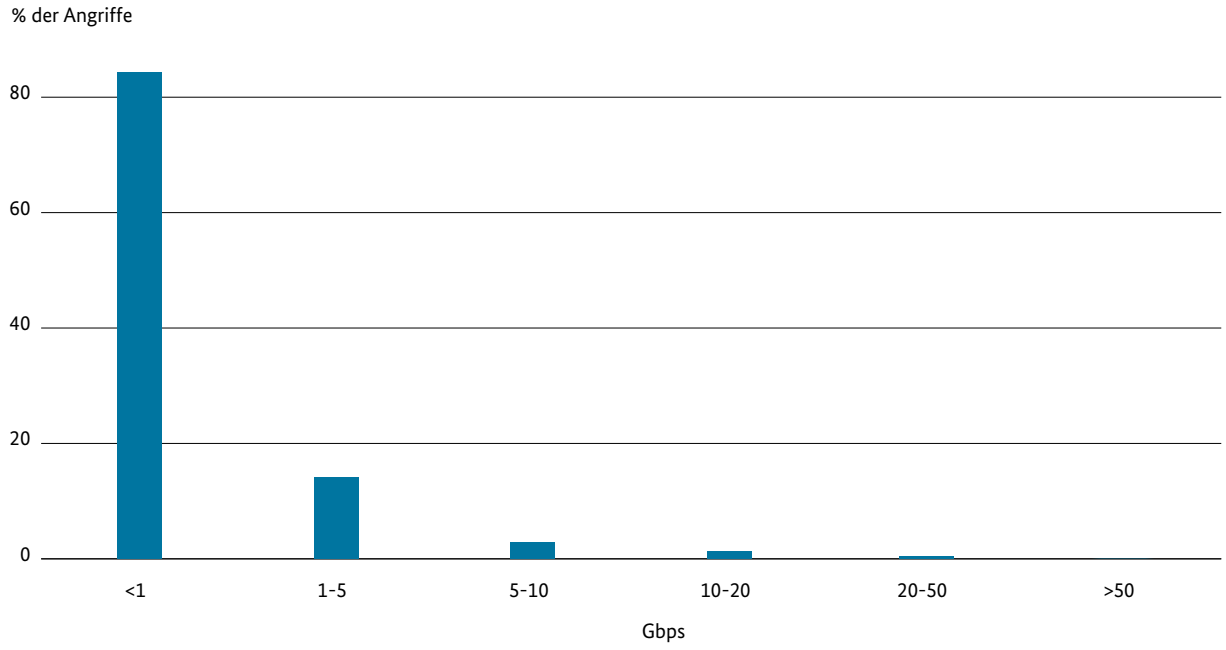


Abbildung 11 Verteilung der DDoS-Angriffe im ersten Quartal 2017 nach Bandbreite

- oder auch durch die bei heutigen Chips vorherrschende geringe Strukturgröße selbst.

All diese Maßnahmen können Ziel eines Angriffs sein. Invasive Angriffe auf die Hardware, bei denen physische Manipulationen am Chip beispielsweise per Fehlerinduktionsangriffe durch Laserbeschuss bis hin zur Modifikation der Schaltkreise vorgenommen werden, finden aufgrund des damit verbundenen Aufwands keine weite Verbreitung. Dafür gewinnen Seitenkanalangriffe weiter an Bedeutung. Da hochauflösende Oszilloskope relativ günstig am Markt beziehungsweise in Forschungseinrichtungen verfügbar sind, stellt die Messung von lokaler elektromagnetischer Abstrahlung etwa eines Kryptokoprozessors keine große Herausforderung mehr dar. Selbst bei seitenkanalresistenten Implementierungen sind unter Umständen Rückschlüsse auf das verarbeitete Schlüsselmaterial im Laufe der Zeit durch verbesserte Analysemethoden möglich. Auch wurden in den letzten Jahren verstärkt bisher nicht betrachtete physikalische Effekte für neue Seitenkanalangriffe ausgenutzt, zum Beispiel Photonen-Emissionen des Halbleiters. Aufgrund der teilweise sehr verschiedenen zugrunde liegenden physikalischen Effekte müssen auch immer wieder neue Gegenmaßnahmen entwickelt werden, um zu verhindern, dass diese Effekte für Seitenkanalangriffe ausgenutzt werden können.

Durch die Kombination von verbesserten Messmethoden für beobachtbare physikalische Effekte einerseits und spezialisierten mathematischen Auswerteverfahren dieser Messwerte andererseits sind bei unzureichenden Gegenmaßnahmen die kryptografischen Schlüssel bereits mit einer relativ geringen Anzahl an Messungen zu extrahieren.

Da die Seitenkanalangriffe fortwährend optimiert werden, stellen sie mit zunehmendem Alter der Hardware eine Bedrohung für Sicherheitselemente in der Praxis dar, selbst wenn deren Sicherheit ursprünglich nach Common Criteria erfolgreich zertifiziert werden konnte. 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. Auf diese Weise können zusätzliche Gegenmaßnahmen in Software ergriffen werden, um frühzeitig neue Angriffe abzuwehren, die verbesserte Analysemethoden nutzen.

Schwachstellen in Webanwendungen

Fast jede Behörde, jede Institution und jedes Unternehmen stellt Informationen oder Dienste über Webanwendungen im Internet zur Verfügung. Schwachstellen in diesen Webanwendungen können für den Anbieter, aber auch für den Anwender erhebliche negative Folgen haben. Diese reichen vom Imageschaden bis hin zum Diebstahl sensibler Daten.

Um möglichst viele solcher Schwachstellen bereits vor der Veröffentlichung zu finden, bietet das BSI sogenannte IS-Webchecks an. Dabei handelt es sich um Penetrationstests auf Webanwendungen, bei denen gezielt nach bekannten Schwachstellen in Webanwendungen und der Webserverkonfiguration gesucht wird. Die gefundenen Schwachstellen werden in drei Kategorien eingeteilt:

- Kritische Mängel – beinhalten beispielsweise die Gefahr, dass Daten verändert werden oder in Anbietersysteme eingedrungen wird

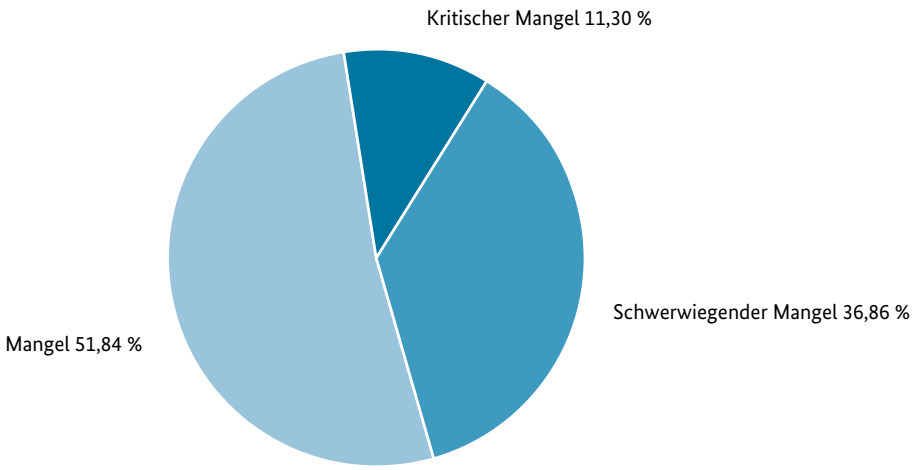


Abbildung 12 Festgestellte Mängel in Webanwendungen nach Kategorien

Schwachstellen in Content-Management-Systemen

Sachverhalt
Im April 2017 kam es zu einem Vorfall in einem Unternehmen, bei dem Angreifer durch Ausnutzung einer Sicherheitslücke in einer veralteten Plug-in-Version für ein Content-Management-System (CMS) unberechtigten Zugriff auf den Webserver erlangten, auf dem das CMS installiert war. Durch Verwendung einer sogenannten Reverse-Shell konnten die Angreifer anschließend auch auf die Daten eines weiteren auf diesem Server installierten CMS zugreifen und diese löschen. Weiterhin erhielten die Täter auf diesem Wege Zugriff auf einen Backup-Server und löschten ebenfalls die dort gespeicherten Datensicherungen der Content-Management-Systeme. Ende Januar 2017 hatte der Hersteller ein Update für das CMS veröffentlicht, das eine kritische Sicherheitslücke schloss. Bereits in den ersten Tagen nach Veröffentlichung des Updates nutzten Angreifer diese Sicherheitslücke bei noch nicht aktualisierten CMS-Installationen aus, um zehntausende Websites zu manipulieren.

Ursache und Schadenswirkung
CMS bieten komfortable Möglichkeiten, Websites zu erstellen und zu pflegen. Wie andere Software sind sie aber nicht frei von Fehlern und müssen regelmäßig gepflegt werden. Viele Betreiber handeln hierbei jedoch sehr nachlässig und spielen Updates, welche unter anderem Sicherheitslücken schließen, nicht oder erst mit langer Verzögerung ein. Nach einer Analyse von BleepingComputer waren im dritten Quartal 2016 über 60 Prozent der untersuchten Installationen des populären CMS „WordPress“ nicht auf dem aktuellen Stand, bei „Joomla“ sogar über 80 Prozent. Neben dem CMS selbst müssen auch installierte Plug-ins auf dem aktuellen Stand gehalten werden. Auch dies wird von CMS-Betreibern häufig vernachlässigt und kann daher von Angreifern als Einfallstor für Kompromittierungen ausgenutzt werden. Die kompromittierten Websites werden dann unter anderem zur Verbreitung von Schadprogrammen, zur Manipulation der Ergebnisse von Suchmaschinen (BlackHat-SEO) oder zum Spam-Versand missbraucht. Auch sogenannte „Defacements“ zur Verbreitung politischer Botschaften finden regelmäßig statt.

Reaktion
CMS sind in der Regel aus dem Internet erreichbar und stehen daher oft im Fokus von Angreifern. Cyber-Kriminelle nutzen täglich bekannte Sicherheitslücken in veralteten Versionen gängiger CMS aus, um in großem Umfang damit verbundene Websites (automatisiert) zu kompromittieren. Im vorliegenden Fall wurde das nicht gepflegte CMS nur als Einfallstor für den Angriff auf das eigentliche Ziel ausgenutzt. Das primäre CMS war auf dem aktuellen Patch-Stand und durch ein sicheres Passwort geschützt.

Empfehlung
Der Vorfall verdeutlicht noch einmal, dass auf einem aus dem Internet erreichbaren Server installierte Software – auch ältere und gegebenenfalls nicht mehr genutzte – regelmäßig aktualisiert werden muss. Wesentlich ist hier, dass nicht nur das Basis-CMS aktualisiert werden muss, sondern auch alle installierten Plug-Ins, die häufig über keine automatischen Update-Funktionen verfügen.

- Schwerwiegende Mängel – beschreiben mögliche Konfigurationsfehler, die schwerwiegende Angriffe zur Folge haben können

- Sonstige Mängel – liegen zum Beispiel bei Konfigurationsfehlern mit unbestimmtem Angriffspotenzial vor.

In die Bewertung fließt ein, welchen Schutzbedarf die zu verarbeitenden Daten haben. Die Einstufung wird zusätzlich anhand der benötigten Fähigkeiten und Mittel abgeschätzt, die für einen Angriff notwendig sind. Im Zeitraum März 2016 bis März 2017 wurden vom BSI 63 IS-Webchecks auf Webanwendungen durchgeführt. Die Prüfungen wurden stichprobenartig und hauptsächlich auf Webangeboten von Bundesbehörden in einer Mischung aus Prüfungen vor Inbetriebnahme und Wiederholungsprüfungen durchgeführt (siehe Abbildung 12).

Bei den Wiederholungsprüfungen waren eher schwerwiegende und sonstige Mängel vertreten, während kritische Mängel hauptsächlich bei Erstprüfungen vorgefunden wurden. Auffällig war, dass im Bereich der kritischen Mängel immer noch seit Jahren bekannte Schwachstellen wie Cross-Site-Skripting oder SQL-Injection gefunden wurden, die auf einer unzureichenden Eingabevalidierung beruhen. Im Bereich der schwerwiegenden Mängel wurden häufig Konfigurationsschwächen bei der SSL-Verschlüsselung vorgefunden. Als sonstige Mängel wurden meist fehlende HTTP-Header

erkannt, die die Sicherheit bei der Übertragung und Speicherung der Daten erhöhen. Abhilfe schaffen hier die Mindeststandards und Empfehlungen des BSI.

Spam und Malware-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 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 beziehungsweise im Anhang erfolgen, der auf ein Schadprogramm oder eine Webseite mit Drive-by-Exploits verweist.
- Mit Phishing-Nachrichten werden Benutzer dazu bewogen, ihre Zugangsdaten (zum Beispiel 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 oder sogar recherchierten Daten wird derzeit immer häufiger beobachtet. Dies steigert die Wahrscheinlichkeit einer Infektion im erheblichen Maße.

Necurs dominiert die Spam-Landschaft

Mit einer Größe von etwa fünf Millionen Bots war Necurs 2016 eines der größten bekannten Botnetze. Es war für die meisten in 2016 versendeten Malware-Spam-Nachrichten verantwortlich und verteilte bis Dezember primär Downloader der Krypto-Ransomware Locky und Cerber. Vor dem 16. Februar 2016 – dem „Geburtstag" von Locky – waren es vor allem Downloader für den Banking-Trojaner Dridex.

Meist wurden die Downloader als (gezippte) Skripte im Anhang versendet, die unter Windows standardmäßig vom Windows Scripting Host ausgeführt werden. Etwas weniger häufig waren MS-Office-Dokumente mit Downloader-Makros im Anhang. Vereinzelte Kampagnen verzichteten gänzlich auf einen Download und lieferten die Schadsoftware kodiert eingebettet im Skript, Dokument beziehungsweise Makro mit.

Nach Weihnachten wurde der Versand von derartigen Malware-Wellen eingestellt. Was zuerst wie die bereits Anfang 2016 beobachtete Necurs-Weihnachtspause aussah, scheint gegebenenfalls ein Strategie- beziehungsweise Kundenwechsel gewesen zu sein. Seit April 2017 wird wieder ein Zuwachs an Malware-Spam verzeichnet. Die größten bis zum 30.06.2017 beobachteten Tagesvolumina waren

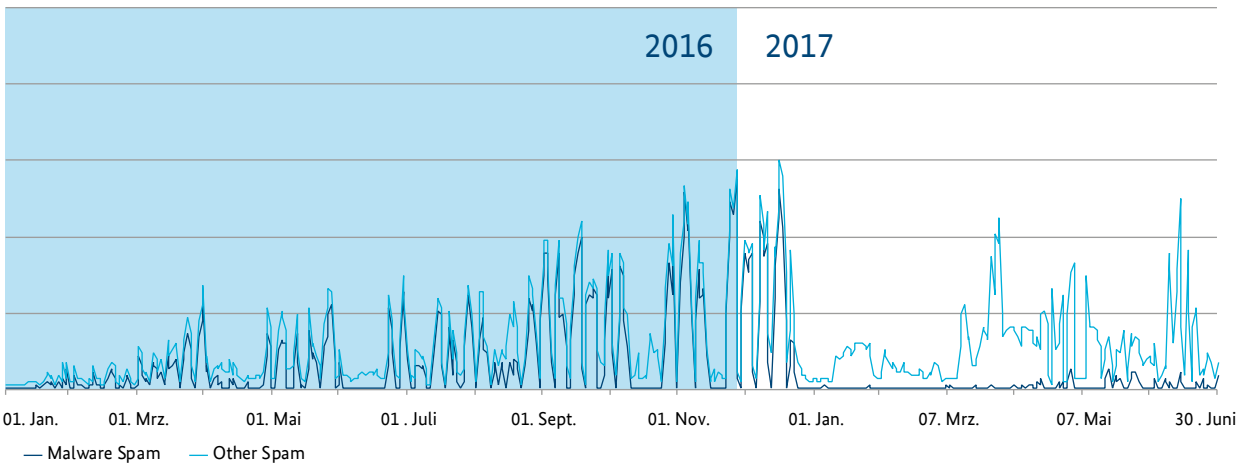


Abbildung 13 Qualitativer Verlauf von klassischem Spam und Malware-Spam

jedoch etwa um den Faktor 10 kleiner als vor Weihnachten. Die Angriffsmethoden variieren stark. So wurde zum Beispiel eine Microsoft-Word-Schwachstelle (CVE-2017-0199) bereits einen Tag vor der Veröffentlichung von Patches in angehängten RTF-Dateien ausgenutzt. Auch unterschiedliche Einbettungen der Schaddateien zum Beispiel in PDF-Dokumenten werden beobachtet.

Die ersten großen Necurs-Wellen nach der langen Pause wurden Ende März 2017 beobachtet. Diese übermittelten eine sogenannte Pump'n'Dump-Kampagne mit angeblichem Insider-Tipp zu einer sogenannten Penny-Aktie und führten kurzfristig zum extremen Anstieg des Handelsvolumens und einem moderaten Anstieg des Aktienkurses. Die Kampagne scheint für die Täter aber nicht erfolgreich gewesen zu sein, da sie nach dem kurzzeitigen Kursanstieg am ersten Tag bei fortdauernd niedrigem Aktienkurs fortgesetzt wurde. Weitere ähnliche Kampagnen mit geringeren Auswirkungen auf die Kursverläufe der betroffenen Aktien wurden auch danach beobachtet.

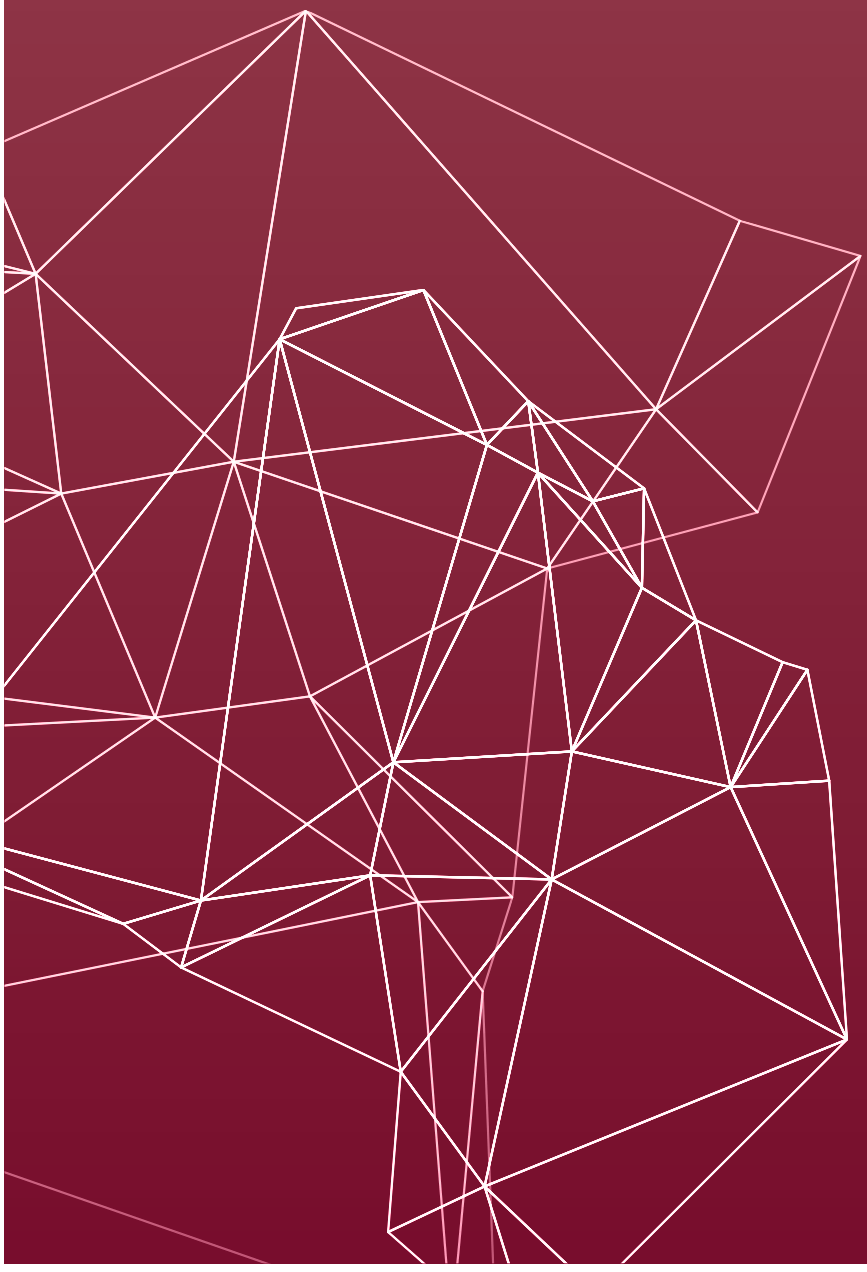
Gegenwärtig scheint Necurs lediglich mit weniger als 30 Prozent seiner Kapazität für den Versand von Werbung für Binär-Optionen-Handel verwendet zu werden. Wie das BSI verifizieren konnte, verfügen die aktuellen Versionen von Necurs zudem seit September 2016 über eine DDoS-Komponente, die bislang jedoch nicht prominent genutzt wurde. Sollten die Betreiber keine „Infrastruktur-Auslastung" mit Spam-Versand erreichen, ist es denkbar, dass die DDoS-Funktionalität monetarisiert wird.

Kleine Malware-Spam-Kampagnen laufen weiter

Unabhängig vom Necurs-Netzwerk werden weiterhin deutlich kleinere Malware-Spam-Kampagnen beobachtet. Hervorzuheben sind die wiederkehrenden Spam-Wellen, die den Adressaten persönlich in deutscher Sprache ansprechen und seine vollständige Adresse und Telefonnummer enthalten. Die Themen variieren stark. Verwendet werden angebliche Rechnungen, Paketzustellungsversuche, Gutschriften etc. Ziel der Versender war meist die Installation von Schadsoftware, vor allem der Krypto-ransomware Cerber. Nach dem BSI vorliegenden Indizien stammen die Daten aus dem eBay-Hack von Anfang 2014.

Noch aufwendiger vorbereitet wurde der Versand angeblicher Bewerbungen an Unternehmen. Hier wurden persönliche Kontaktdaten von Mitarbeitern der Personalabteilungen recherchiert und für persönliche Anrede sowohl in der E-Mail, als auch im angehängten Dokument verwendet (siehe Infokasten auf S. 28). Das Dokument enthielt nur teilweise lesbare Bewerbungsunterlagen mit einem Foto. Der unlesbare / kryptische Teil sollte den Empfänger dazu verleiten Makros im Dokument zuzulassen. Nach Aktivierung von Makros wurde das die Krypto-Ransomware Petya / Mischa oder deren Variante Goldeneye gestartet.

2 Maßnahmen des BSI



2 Maßnahmen des BSI

Wie begegnet das BSI den genannten Gefährdungen, welche Maßnahmen können den Risiken entgegengesetzt werden? Im folgenden Kapitel werden anhand ausgewählter Themen und immer bezogen auf die aktuelle Gefährdungslage der IT-Sicherheit 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 Aufgaben und Aufbau des BSI

Das BSI als die nationale Cyber-Sicherheitsbehörde gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft. Das BSI hat dafür einen klaren gesetzlichen Auftrag, der 2015 durch das IT-Sicherheitsgesetz noch einmal deutlich im Bereich der Kritischen Infrastrukturen und 2017 mit der Umsetzung der NIS-Richtlinie im Bereich der Anbieter digitaler Dienste erweitert wurde. Als das Kompetenzzentrum für Fragen der IT- und Cyber-Sicherheit gehören IT-Sicherheitsanalysen, die Erarbeitung von technischen Richtlinien, die Lösung praktischer IT-Sicherheitsprobleme und der fachliche Diskurs mit Experten aus Industrie, Fachorganisationen und Verbänden zu den wesentlichen Handlungsfeldern des BSI. Von der Kryptografie, über beispielsweise Netzwerk-, System oder Chipsicherheit sind alle notwendigen Kompetenzen zur Bewältigung hochkomplexer Fragestellungen im BSI vereint. Diese Bündelung und Vernetzung aller für Cyber-Sicherheit erforderlichen Kompetenzen in einer Behörde gibt dem BSI seine in Deutschland einzigartige Schlagkraft.

Mit der Zuweisung von 180 neuen Stellen allein für das Jahr 2017 wurde die Rolle des BSI als die nationale Cyber-Sicherheitsbehörde weiter gestärkt. Die Behörde wächst damit auf ca. 840 Mitarbeiter an. Um die 180 neuen Stellen besetzen zu können, hat das BSI eine Personalmarketingkampagne gestartet. Trotz des hart umkämpften Arbeitsmarktes für IT-Fachkräfte konnte das BSI als Top-Arbeitgeber für IT-Absolventen (trendence Graduate Barometer) im ersten Halbjahr 2017 bereits 60 Prozent dieser Stellen besetzen (Stand: Juni 2017).

Auch durch eine organisatorische Neuordnung trägt das BSI den veränderten Anforderungen Rechnung. Der veränderte Aufbau der Behörde mit seinen vier Fachabteilungen, die von der Zentralabteilung unterstützt werden, ist damit gleichzeitig ein Spiegel des Leitsatzes des BSI.

- In der Fachabteilung CK „Cyber-Sicherheit und Kritische Infrastrukturen“ werden alle Themen der Cyber-Sicherheit gebündelt und federführend gestaltet.
- In der Fachabteilung B „Beratung für Staat, Wirtschaft und Gesellschaft“ werden im Rahmen der Prävention alle Beratungsaufgaben gebündelt.
- Die Fachabteilung KT „Krypto-Technologie und IT-Management für erhöhten Sicherheitsbedarf“ bündelt einerseits alle Aufgaben im Bereich der Vorgaben und Zulassungen von Krypto-Systemen, und ist andererseits für deren Evaluierung und Betrieb zuständig.
- Die Cyber-Sicherheit in der Digitalisierung ist ein wachsender Arbeitsschwerpunkt der Fachabteilung D „Cyber-Sicherheit in der Digitalisierung, Zertifizierung und Standardisierung“.
- Die Zentralabteilung Z „Zentrale Aufgaben“ unterstützt durch interne Services die vorgenannten Fachabteilungen.

2.2 Zielgruppe Staat / Verwaltung

2.2.1 Das Cyber-Abwehrzentrum

Das Nationale Cyber-Abwehrzentrum (Cyber-AZ) wird unter Federführung des BSI auf Basis von Verwaltungsvereinbarungen der beteiligten Behörden betrieben. Das BSI stellt den Leiter, die Geschäftsstelle samt Personal und die Räumlichkeiten. Durch die Ansiedlung beim BSI kann das Cyber-AZ eng und auf kurzen Wegen mit dem Nationalen IT-Lagezentrum / IT-Krisenreaktionszentrum, dem CERT-Bund sowie mit den mobilen Einsatzteams (MIRT) des BSI zusammenarbeiten. Die anderen beteiligten Behörden sind über Verbindungsbeamte dieser Behörden angebunden.

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. Ein Großteil der Fallbearbeitung wird dabei von den beteiligten Behörden wie dem Bundesamt für Verfassungsschutz, dem Bundeskriminalamt, dem Bundesnachrichtendienst,

Das BSI – vernetzte Kompetenz in der Cyber-Sicherheit

Das Beispiel Vorfallsbearbeitung als eine integrierte Wertschöpfungskette

Detektion

Erkennen der Schwachstelle

Das BSI führt Tests der Hard- und Software durch und deckt dabei Sicherheitslücken und Schwachstellen auf. Diese Schwachstellen werden evaluiert sowie einer Sicherheitsanalyse unterzogen.

Erkennen des Angriffs

Das BSI detektiert Anomalien in IT-Netzen und Systemen und identifiziert so konkrete Cyber-Angriffe.

Abteilung B

Beratung für Staat, Wirtschaft und Gesellschaft

Abteilung D

Cyber-Sicherheit in der Digitalisierung, Zertifizierung und Standardisierung

Reaktion

Koordination der Cyber-Abwehr

Das BSI als nationales IT-Krisenreaktionszentrum koordiniert das Vorgehen mit Herstellern, Providern, Betroffenen, IT-Sicherheitswirtschaft, Kritischen Infrastrukturen und anderen Behörden.

Bewältigen des Cyber-Angriffs

Das BSI unterstützt die betroffenen Einrichtungen bei der Abwehr des konkreten Angriffs und hilft bei der Wiederherstellung des Regelbetriebes. Staat, Wirtschaft und Gesellschaft und internationale Partner werden über alle notwendigen Maßnahmen informiert.

Bewerten des Cyber-Angriffs

Das BSI erstellt in Zusammenarbeit mit allen Fachbereichen eine Lagedarstellung und gibt eine Bewertung zum Vorfall, der Schwachstelle und der Ausnutzbarkeit dieser. Diese Ausnutzbarkeit wird nochmal anhand von Einsatzszenarien für Staat, Wirtschaft und Gesellschaft aufgeschlüsselt dargestellt.

der Bundeswehr oder dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 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 auf die personellen Ressourcen aller beteiligten Behörden zugreifen. Sie werden gegenwärtig bei allen Cyber-AZ-Behörden verstärkt.

Das Cyber-AZ ist als Kooperationsplattform angelegt. Der Leiter des Cyber-AZ besitzt keine unmittelbaren Weisungsbefugnisse gegenüber den am Cyber-AZ beteiligten Behörden beziehungsweise deren Mitarbeitern. Derzeit erarbeitet das federführende Bundesinnenministerium mit den beteiligten Behörden ein Konzept, mit dem das Cyber-AZ weiterentwickelt werden soll.

2.2.2 Bund-Länder-Kooperation und Verbindungswesen

Die Digitalisierung ist eine gesamtgesellschaftliche Herausforderung. Bund und Länder stimmen sich intensiv zur digitalen Transformation in den Bundes- und Landesbehörden ab.

Gemeinsam für mehr Cyber-Sicherheit in Deutschland

Nach Maßgabe des BSI-Gesetzes berät das BSI die Länder auf deren Ersuchen hin und entwickelt zusammen mit ihnen in den Gremien des IT-Planungsrates gemeinsame IT-Sicherheitsstandards. Die Kooperations- und Unterstützungsangebote des BSI für die Länder sind vielfältig. Sie reichen von der Bereitstellung bedarfsgerechter Informationen und der übergreifenden Beratungs- und Gremienarbeit bis hin zur Einbindung der Länder in die Informations- und Warnkanäle des BSI. Weitere Aktionspunkte und Pfeiler der Zusammenarbeit sind

- die Bereitstellung von etablierten Sicherheitslösungen des BSI zur Nutzung durch die Länder,
- die Weitergabe von Erfahrungen beim Aufbau und Betrieb eines Managementsystems für Informationssicherheit (ISMS) sowie von technischen Schutzmechanismen,
- die Bereitstellung angepasster Arbeitshilfen im Portal der Sicherheitsberatung,
- die Inanspruchnahme vertrauenswürdiger, durch das BSI zertifizierter IT-Sicherheitsdienstleiter,
- die Unterstützung der Länder bei IT-Sicherheitsvorfällen durch mobile Einsatzteams (MIRT) des BSI,
- Beratung und Unterstützung zur IT-Sicherheit im Rahmen von Landtagswahlen.

Zentrale Anlaufstelle

Die Informationssicherheitsberatung des BSI ist die zentrale Anlaufstelle primär für die Informationssicherheitsbeauftragten der Bundesverwaltung zu allen Belangen der Informationssicherheit. Gemeinsam mit den Fachreferaten des BSI bietet die Sicherheitsberatung sowohl begleitende Unterstützung als auch individuelle Beratung zu konkreten Herausforderungen an. Ziel und Motivation ist es, dem Kunden Wissen zu Informationssicherheit zu vermitteln und gemeinsam praxisgerechte Lösungen zu finden. Um Arbeitsabläufe und Informationskanäle effizient zu gestalten, wird dabei das bewährte Point-of-Contact-Prinzip zwischen der BSI-Sicherheitsberatung und dem ISMS-Team der Behörde angewendet. Die Sicherheitsberatung stellt jeder Bundesbehörde einen zentralen BSI-Ansprechpartner bereit. Neben der zentralen E-Mail-Adresse Sicherheitsberatung@bsi.bund.de und der Möglichkeit einer direkten Kontaktaufnahme zum Berater werden auch eine persönliche Beratung und Vor-Ort-Termine bei der Behörde durch die Informationssicherheitsberatung angeboten. Oftmals geschieht dies in Form von Vorträgen, bei denen auch themenspezifisch die Fachspezialisten des BSI eingebunden werden. Die begleitende Gremienarbeit, bei der die Informationssicherheitsberatung Aspekte der Informationssicherheit einbringt und moderierend unterstützt, gehört ebenfalls zum Aufgabenspektrum.

Dreh- und Angelpunkt der Zusammenarbeit zwischen BSI und den Ländern ist die AG Informationssicherheit, kurz AG InfoSic, des IT-Planungsrates. In dieser Arbeitsgruppe wird die Zusammenarbeit zwischen Bund und Ländern in der Informationssicherheit koordiniert. Jedes Land ist dort durch einen Landes-IT-Sicherheitsbeauftragten (CISO) vertreten. Landkreistag und Städtetag sind dort ebenfalls vertreten. In der AG InfoSic werden grundsätzlich alle Fragen der Informationssicherheit behandelt, die Bund und Länder betreffen. Eines der wichtigsten Themen ist der Aufbau von ISMS-Strukturen in Ländern und Kommunen. Das BSI hat 2016 begonnen, das Dienstleistungsangebot für Länder weiter auszubauen.

Darüber hinaus fordert die Cyber-Sicherheitsstrategie für Deutschland 2016 eine noch engere Zusammenarbeit zwischen Bund und Ländern im Bereich der Cyber-Sicherheit. Hiermit verbunden sind zusätzliche Aufgaben für das BSI insbesondere bei der Länderunterstützung, denen das BSI unter anderem durch den im

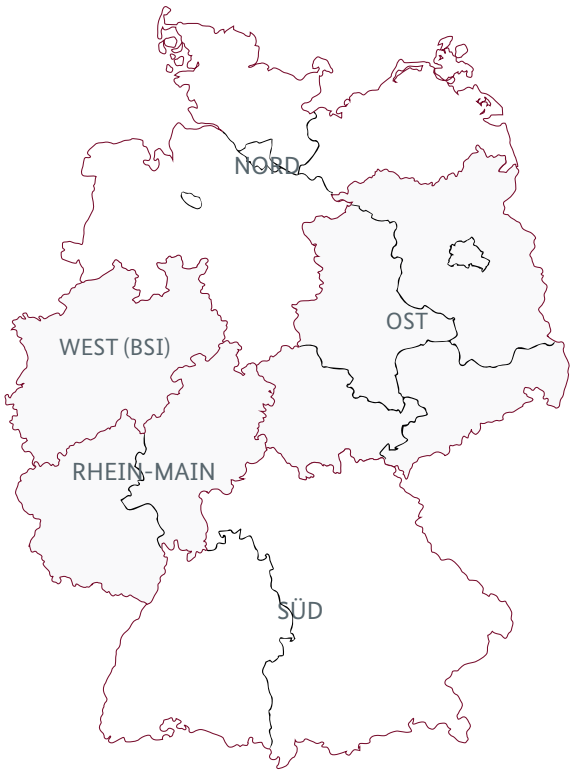


Abbildung 14 Geplante Umsetzung des nationalen Verbindungswesens des BSI

Rahmen eines Pilotverfahrens gestarteten Ausbau des Verbindungswesens nachkommt. Durch die Entsendung von Verbindungspersonen an verschiedene nationale und internationale Standorte wird das BSI für Länder, Bundesbehörden, internationale Organisationen und die Wirtschaft in Schlüsselregionen besser erreichbar. Die Verbindungsbeamten informieren vor Ort über die Produkte und Dienstleistungen des BSI, um besser auf die Bedürfnisse der Anwender aus den Bereichen Staat, Wirtschaft und Gesellschaft einzugehen. Beim Ausbau des Verbindungswesens stehen die regionalen Standorte im Rhein-Main-Gebiet, Berlin und Brüssel im Vordergrund. Repräsentanzen des BSI in Süd- und Norddeutschland sollen folgen.

2.2.3 Lauschabwehr

Das BSI stellt abhörgefährdeten Bundesbehörden 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.

Außerdem bietet das BSI Konfigurationsprüfungen von Telekommunikations-Anlagen (TK-Anlagen) an. Dabei werden die Systemeinstellungen der TK-Anlagen mithilfe eines vom BSI entwickelten Prüfwerkzeuges analysiert. Anschließend berät das BSI die jeweilige Behörde, welche Maßnahmen erforderlich sind, um ihre TK-Anlagen abzusichern.

Darüber hinaus werden aber auch Konferenzen wie das G20-Außenministertreffen im April 2017 in Bonn sowie der G20-Gipfel im Juli in Hamburg und bilaterale Treffen auf höherer Ebene betreut, bei denen die Vertraulichkeit der Gespräche eine besondere Relevanz hat. Dabei stellen die Lauschabwehr-Prüftrupps des BSI sicher, dass keine Abhörgeräte vorhanden sind und dass auch auf anderen Wegen, beispielsweise über manipulierte oder versehentlich aktivierte Mobiltelefone, keine Gesprächsinformationen an Unbefugte gelangen.

2.2.4 Sichere Mobilkommunikation

Zur Verarbeitung und Übertragung von Verschlusssachen stellt das BSI für die Bundesverwaltung verschiedene mobile Lösungen bereit. Bereits seit mehreren Jahren etabliert ist die Lösung SecuSUITE des Herstellers Secusmart. Im aktuellen Berichtszeitraum haben sich die Nutzerzahlen dieser Lösung weiter erhöht, sodass nun etwa 15.000 mobile Geräte in der Bundesverwaltung im Einsatz sind.

App-Testing

Die für die Bundesverwaltung entwickelten mobilen Lösungen werden vom BSI sicherheitstechnisch mit Ziel einer Zulassung für die Verarbeitung und Übertragung von Verschlusssachen evaluiert. Dabei werden auch die verwendeten Apps hinsichtlich ihrer Sicherheit geprüft. Das BSI hat Kriterien zur Bewertung der App-Sicherheit definiert, nach denen spezialisierte Anbieter die Apps verschiedenen Prüfverfahren unterziehen. Seit 2014 hat das BSI rund 300 Apps für die Betriebssysteme Android, Apple iOS und BlackBerry OS anhand verschiedener Kriterien wie Zugriff auf Kalender und Adressbücher, Standortdaten und die Nutzung von Tracking-Mechanismen prüfen lassen. Die Bandbreite der dabei aufgedeckten Sicherheitsmängel ist groß. Während einige Apps nur wenige Kriterien verletzen, sind bei anderen Apps erhebliche Mängel festzustellen, etwa im Umgang mit Nutzerdaten. Um ein differenzierteres Risikomanagement zu ermöglichen, unterzieht das BSI die Prüfberichte einer Nachbearbeitung, bei der die verschiedenen Kriterien je nach Anwendungsfall gegeneinander gewichtet werden. Die Prüfberichte werden den jeweiligen IT-Verantwortlichen der Bundesverwaltung zur Verfügung gestellt, die auf dieser Basis eine fundierte Entscheidung über den Einsatz der jeweiligen App in ihrem jeweiligen Verantwortungsbereich treffen können.

iOS-Systemlösung

Die iOS-Systemlösung ist eine vom BSI konzipierte Lösung, um eingestufte Daten auf iPhones und iPads des Herstellers Apple verarbeiten zu können. Hauptelement der Lösung ist die App „SecurePIM Government SDS“ des Herstellers Virtual Solution AG. Diese App kombiniert E-Mail, Adressbuch, Notizen, Aufgaben und Kalender und ermöglicht die Synchronisation dieser Daten mit dem behördeninternen Netzwerk. Zusätzlich können Dokumente und weitere Inhalte aus dem Intranet auf die mobilen Geräte geladen werden. Die Lösung verwendet als Sicherheitsanker für SecurePIM Government SDS eine Chipkarte, die über spezielle Smartcard-Reader an die iOS-Geräte gekoppelt wird. Außerdem kommt ein IPsec-VPN für die Kommunikationsverbindung zum Behördennetz sowie ein Mobile Device Management (MDM) zum Einsatz. Im Berichtszeitraum wurde das System im Rahmen eines Pilotprojekts in über 20 Behörden in Betrieb genommen und vom BSI nach einer Sicherheitsevaluierung zugelassen.

SecuTABLET

Die mobile Lösung SecuTABLET des Herstellers Secusmart nutzt Android-Tablets von Samsung für die sichere Bearbeitung von dienstlichen Daten und deren Synchronisation mit dem behördeninternen Netzwerk. Dabei werden Sicherheitstechnologien wie Samsung Knox und Secusmarts Wrapping-Technologie miteinander verknüpft, um die Sicherheit der Daten zu gewährleisten. Die mobile Lösung verwendet eine Chipkarte als Sicherheitsanker in den Endgeräten, nutzt ein IPsec-VPN für die Kommunikationsverbindung zum Behördennetz und verwaltet Applikationen und Geräte über den stationären Mobile-Application-Management (MAM) Server. Dadurch werden dienstliche und persönliche Applikationen auf den Endgeräten separiert. Im Backend des Behördennetzwerkes können verschiedene PIM-Daten-Server kontaktiert werden. Im Berichtszeitraum wurde die Lösung nach einer vorläufigen Zulassung des BSI erstmals an behördliche Nutzer ausgeliefert.

2.2.5 Entwicklung von IT-Systemen für die Verarbeitung von Verschlusssachen

IT-Systeme, mit denen im öffentlichen Interesse geheimhaltungsbedürftige Informationen (Verschlusssachen, VS) verarbeitet oder übertragen werden, müssen vom BSI zugelassen werden. Die hierfür relevante Allgemeine Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VSA) regelt unter anderem, wann zugelassene IT-Systeme eingesetzt werden müssen und wie diese korrekt zu handhaben sind. Die VSA enthält auch Vorgaben zu der Sicherheitsfunktionalität, über die IT-Systeme verfügen müssen, damit sie für einen bestimmten Geheimhaltungsgrad zugelassen werden können. So fordert die VSA beispielsweise, dass bei der Verarbeitung von Verschlusssachen mit dem Geheimhaltungsgrad VS-VERTRAULICH oder höher technische oder organisatorische Maßnahmen ergriffen werden müssen, damit Unbefugte nicht über das Abhören kompromittierender Abstrahlung an Geheimnisse gelangen können.

5G potenziert die IT-Sicherheitsrisiken

Die Mobilfunktechnologie der fünften Generation (5G) ermöglicht zahlreiche innovative Anwendungen und kombiniert bisher voneinander unabhängige Bereiche. Ein durchschnittlicher Haushalt wird mit einer Vielzahl von miteinander kommunizierenden Geräten ausgestattet sein, Autos werden untereinander sowie mit Einrichtungen der Verkehrsinfrastruktur verschiedene Arten von Daten austauschen. Auch die Bürokommunikation sowie Produktionsprozesse werden von 5G-Technik durchzogen.

Die Risiken der IT-Sicherheit werden im Zeitalter von 5G aber nicht einfach proportional mit der Anzahl der kommunizierenden Geräte und Komponenten zunehmen. Der Faktor der allgemeinen Vernetzung, die weiter zunehmende Komplexität der Gesamtsysteme sowie die schrittweise Übergabe von kritischen Aufgaben an die 5G-Technik führen vielmehr zu einer Potenzierung der Sicherheitsrisiken.

Die Chancen der Digitalisierung können nur dann genutzt werden, wenn die Risiken beherrschbar werden. In diesem Sinne sollten die Belange der IT-Sicherheit von Anfang an ausreichend berücksichtigt werden in der Standardisierung, in der Produktion und im Betrieb. Die Sicherheit ist unabdingbare Voraussetzung für den Erfolg der gesamten 5G-Technologie. Aufgabe des BSI ist es, dieses Kernthema der Digitalisierung mit seiner anspruchsvollen Sicherheitsproblematik in seinen Chancen und Risiken auszugestalten. Durch seine fachlich wissenschaftliche Kompetenz und den hohen Grad von Vernetzung in alle Bereiche des Staates, der Wirtschaft und der Gesellschaft ist das BSI für diese neue Herausforderung gut gerüstet.

Herausforderungen durch globalisierte Produktionsprozesse

Eine Leitlinie der von der Bundesregierung beschlossenen Cyber-Sicherheitsstrategie für Deutschland besagt, dass die Handlungsfähigkeit und Souveränität Deutschlands auch im Zeitalter der Digitalisierung gewahrt sein muss. Jedoch werden heutzutage die meisten IT-Produkte beziehungsweise deren Teilkomponenten nicht mehr in Deutschland oder der EU hergestellt. Hat man über den Herstellungsprozess oder die Lieferketten keine Kontrolle, können beispielsweise Manipulationen am fertigen IT-System nicht ausgeschlossen werden. Dass dies kein abstraktes Bedrohungsszenario ist, zeigen mehrere aktuelle Fälle, in denen auf großen Produktionsmengen von AndroidNGeräten ab Werk installierte Schadsoftware gefunden wurde.

Auf diese Herausforderung reagiert das BSI mit verschiedenen Maßnahmen, um vertrauenswürdige Herstellungsprozesse zu ermöglichen und zu fördern. So werden beispielsweise Kooperationsvereinbarungen mit Herstellern geschlossen, um Einsicht in den genauen Aufbau oder den Quellcode von IT-Produkten zu erhalten. Eine weitere Möglichkeit besteht darin, dass das BSI eine Eigenentwicklung des benötigten Produktes beziehungsweise von Teilkomponenten durchführt. Dies erfolgt im Rahmen von Ausschreibungen, auf die sich Unternehmen bewerben können, die bereit sind, die Aufforderungen des BSI hinsichtlich größtmöglicher Transparenz der Entwicklungs-, Fertigungs- und Auslieferungsprozesse zu erfüllen. Gibt es keine Alternative für den Einsatz von nicht vertrauenswürdigen Teilkomponenten in einem VS-IT-System, besteht noch die Möglichkeit, das verbleibende Risiko durch eine geeignete Konzeption des Gesamtsystems auf ein akzeptables Maß zu reduzieren. Dies kann beispielsweise dadurch erreicht werden, dass die nicht vertrauenswürdigen Bestandteile so stark vom übrigen System isoliert werden, dass sie keinen Schaden anrichten können.

Als Rechtsnorm kann die VSA jedoch nicht jede erdenkliche Situation konkret beschreiben oder zeitnah neuartige Technologien oder Bedrohungen abbilden. Es liegt daher in der Verantwortung des BSI, konkrete Sicherheitsanforderungen für VS-IT-Systeme zu formulieren. Zum einen ist hierfür eine Interpretation der VSA erforderlich, um aus abstrakten Rechtsnormen konkrete Anforderungen für den Einzelfall abzuleiten. Zum anderen muss das BSI die Sicherheitsanforderungen an VS-IT-Systeme permanent überprüfen und anpassen, um dem technologischen Fortschritt sowie neu bekannt gewordenen Bedrohungen gerecht zu werden. Auch der Spagat zwischen Sicherheitsfunktionalität und Benutzerakzeptanz muss überwunden werden, denn die Abnehmer aus dem Behördenumfeld und der Wirtschaft erwarten auch für die Verarbeitung von Verschlusssachen moderne, wirtschaftliche, mobile sowie leicht bedienbare Lösungen.

Bereits in der Konzeptionsphase von VS-IT-Systemen arbeitet das BSI eng mit Herstellern und Bedarfsträgern zusammen, um die Sicherheitsanforderungen zu definieren und im sogenannten Security Target festzuhalten. Während des Entwicklungsprozesses überprüft das BSI dann im Rahmen der entwicklungsbegleitenden Evaluierung, ob der Hersteller die Anforderungen aus dem Security Target wirksam und korrekt im Produkt umgesetzt hat. Gegebenenfalls werden auch technische und organisatorische Einsatzhinweise formuliert, die von den Bedarfsträgern zu beachten sind. Wenn alle Anforderungen erfüllt sind, spricht das BSI eine nationale Zulassung für das VS-IT-System aus. Um den Einsatz des Produktes auch im internationalen Kontext (EU, NATO etc.) zu ermöglichen und somit die Marktchancen des Produktes deutlich zu steigern, müssen neben den nationalen Anforderungen auch internationale Vorgaben berücksichtigt werden.

2.2.6 IT-Konsolidierung des Bundes

Die Bundesregierung hat am 20.05.2015 beschlossen, die IT der Bundesverwaltung zu konsolidieren. Dies umfasst,

- IT-Betrieb der unmittelbaren Bundesverwaltung bis 2022 stufenweise auf ein bis zwei Dienstleister an wenigen Standorten zu konzentrieren (Betriebskonsolidierung),
- die Entwicklung von häufig im Bund benötigten Anwendungen zusammenzufassen und eine „Bundes-Cloud“ aufzubauen (Anwendungskonsolidierung) sowie
- die IT-Beschaffung an wenigen Stellen der Bundesverwaltung zusammenzuführen (Beschaffungsbündelung).

Hierzu hat die Bundesregierung ein ressortübergreifendes, aus sechs Teilprojekten bestehendes Projekt eingerichtet. Es wird vom Bundesbeauftragten für IT (BfIT) im Bundesministerium des Innern geleitet.

Eines der Projektziele der IT-Konsolidierung ist, das IT-Sicherheitsniveau der Bundesverwaltung zu erhalten. Das BSI berät die Bundesregierung zu Sicherheitsaspekten bei der Umsetzung der Betriebskonsolidierung und der Anwendungskonsolidierung.

Die Betriebs- und Anwendungskonsolidierung kann einen Gewinn an IT-Sicherheit bringen, wenn von vornherein auf IT-Sicherheit Wert gelegt wird. Auch die nachhaltige Aufrechterhaltung des IT-Sicherheitsniveaus bedarf der Planung und Umsetzung geeigneter Sicherheitsmaßnahmen. Im Rahmen seiner Beratungstätigkeit weist das BSI die verschiedenen Stakeholder daher regelmäßig auf erforderliche Sicherheitsanforderungen hin. Passende Sicherheitskonzepte für die gemeinsamen IT-Systeme zu erarbeiten, liegt dabei in der Hoheit der IT-Dienstleister im Leistungsverbund.

Begleitend zur IT-Konsolidierung hat der Haushaltsausschuss des Deutschen Bundestags das BSI beauftragt, alle Rechenzentren des Bundes auf ihre IT-Sicherheit hin zu untersuchen. Das BSI kommt diesem Auftrag nach, indem es sukzessive alle Rechenzentren des Bundes auf Basis des Standards HV-Benchmark kompakt untersucht und dem Haushaltsausschuss berichtet.

2.2.7 Sonstige Maßnahmen für den Staat

Bund-Länder-Portal der Informationssicherheitsberatung

Die Informationssicherheitsberatung des BSI erfolgt überwiegend durch den unmittelbaren Kontakt zwischen Beratern und Fachexperten des BSI und dem ISMS-Team einer Institution (siehe 2.1.2). Ergänzend zum persönlichen Kontakt werden alle wesentlichen Informationen jederzeit abrufbar auf der Webseite des BSI und im Webportal der Informationssicherheitsberatung des BSI bereitgestellt. Das Webportal stellt dabei die allgemeinen Informationen des BSI in einem offenen Bereich zur Verfügung. Darüber hinaus werden in einem internen Bereich auch zielgruppengerechte Informationen zur Verfügung gestellt.

- Im offenen Bereich sind beispielsweise Arbeitshilfen wie das Konzeptions- und Auswertungstool für Erhebungen (KATE) und Informationen zu Penetrationstests und IS-Revisionen eingestellt, ebenso wie Termine und Veranstaltungen zu Schulungen sowie die Liste der zugelassenen IT-Sicherheitsprodukte und -systeme.

- Im internen Bereich „Bund“ sind die Produkte, Dienstleistungen und Publikationen des BSI für die Zielgruppe Bundesverwaltung eingestellt. Unter anderem gibt es dort IT-Sicherheitswarnungen, Sicherheitshinweise, BSI-Schriften und Lageberichte. Dienstliche Informationen, Orientierungspapiere zu aktuellen Themen wie Rahmenverträge, Notfallmanagement und Sensibilisierung runden das Angebot ab.

- Im internen Bereich „Land / Kommune“ sind die Produkte, Dienstleistungen und Publikationen des BSI für die Zielgruppe der Länder und kommunalen Institutionen eingestellt. Unter anderem finden sich dort Blaupausen zum Aufbau eines Informationssicherheitsmanagementsystems (ISMS), das Umsetzungsrahmenwerk Notfallmanagement (UMRA) sowie die Technischen Richtlinien des BSI (BSI-TR) und Technische Leitlinien zur VSA (BSI-TL).

Mindeststandards

Das BSI erstellt nach § 8 BSIG Mindeststandards für die Einrichtungen des Bundes und gibt damit ein gezieltes Mindestniveau für die Informationstechnik des Bundes vor. Bereits der erste veröffentlichte Standard über den Einsatz des SSL / TLS-Protokolls durch Bundesbehörden wurde durch das BMI im Einvernehmen mit dem IT-Rat als Allgemeine Verwaltungsvorschrift erlassen. Damit ist die Bundesverwaltung verpflichtet, sämtlichen Datenverkehr über ungeschützte Netzwerke mit SSL / TLS zu verschlüsseln. Im Laufe des letzten Jahres wurden zudem die Mindeststandards Sichere Web-Browser, Schnittstellenkontrolle, Nutzung von externen Cloud-Diensten, Mobile Device Management und Anwendung des HV-Benchmark kompakt veröffentlicht. Weitere Mindeststandards aus den Themenbereichen Netzsicherheit und Detektion werden derzeit erarbeitet.

Untersuchung Samsung Knox

Mobilgeräte mit dem Betriebssystem Android finden auch im Bereich der Bundesverwaltung starken Anklang. Im professionellen Umfeld sind die Anforderungen an die Sicherheit und die Möglichkeiten, Endgeräte und Applikationen zu verwalten, jedoch höher als beim privaten Nutzer. Mit der Lösung Samsung Knox adressiert der Mobilgeräte-Hersteller Samsung diesen Bereich und stellt erweiterte Sicherheitsfunktionalitäten bereit, die über die von Android hinausgehen. Neben der Prüfung der Systemintegrität und einer zusätzlichen Datenseparierung mittels der sogenannten Knox-Container auf den Endgeräten bietet Samsung Knox auch zusätzliche Möglichkeiten des Endgeräte-Managements.

Das BSI hat diese Lösung im Jahr 2016 untersucht und die Erkenntnisse in die Bewertung von Android-basierten mobilen Lösungen für die Bundesverwaltung (wie zum Beispiel SecuTABLET, siehe Kapitel 2.2.4) einfließen lassen. Für Administratoren in Verwaltung und Wirtschaft, die Samsung Knox bereits einsetzen oder den Einsatz planen, hat das BSI auf seiner Webseite Konfigurationsempfehlungen veröffentlicht. Darin werden mögliche Ansätze aufgezeigt, mobile Lösungen auf Android-Basis mittels der Knox-Funktionen abzusichern und zu konfigurieren. Zudem gibt das BSI

konkrete sicherheitstechnische Empfehlungen für die Vielzahl der Konfigurationsmöglichkeiten. Anhand von zwei beispielhaft gewählten Mobile-Device-Management-Systemen (MDM) werden aus Sicherheitssicht sinnvolle Konfigurationsparameter für Knox-Geräte aufgezeigt.

Wie die meisten komplexen IT-Systeme ist auch Samsung Knox nicht frei von Sicherheitsschwachstellen. Neben den Android-Schwachstellen, die Google regelmäßig veröffentlicht und mit Sicherheitsaktualisierungen schließt, wurde im Berichtszeitraum von Sicherheitsforschern zweimal auf Schwachstellen hingewiesen, die unmittelbare Angriffe auf Sicherheitsfunktionalitäten von Samsung Knox ermöglichten. Beide Veröffentlichungen zeigen Wege auf, wie der Echtzeit-Schutz für den Betriebssystem-Kernel ausgehebelt werden kann. Im Sinne einer Responsible Disclosure wurden diese Schwachstellen dem Hersteller vor ihrer Veröffentlichung gemeldet und von Samsung in einigen Modellen behoben. Es zeigt sich jedoch auch hier, dass aus dem Android-Umfeld bekannte Problem, dass Schwachstellen nicht auf allen Geräten kurzfristig und auf manchen Geräten gar nicht behoben werden.

Zulassung

Das BSI ist gesetzlich befugt, IT-Sicherheitsprodukte zu prüfen und eine verbindliche Aussage zum Sicherheitswert zu treffen. Insbesondere IT-Sicherheitsprodukte, die für die Verarbeitung, Übertragung und Speicherung von amtlich geheim gehaltenen Informationen (Verschlusssachen, VS) im Bereich des Bundes und der Länder oder bei Unternehmen im Rahmen von Aufträgen des Bundes oder der Länder eingesetzt werden, bedürfen einer solchen Evaluierung und Zulassung durch das BSI. Hauptsächlich sind von dem Verfahren IT-Sicherheitsprodukte betroffen, die kryptografische Anteile enthalten und daher als Kryptosysteme bezeichnet werden. Der Antrag auf Zulassung eines IT-Sicherheitsproduktes kann grundsätzlich nur von einem behördlichen Anwender gestellt werden.

Nach § 37 der Verschlusssachenanweisung (VSA) des Bundesinnenministeriums 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. Im Berichtszeitraum Juli 2016 bis Juni 2017 hat das BSI hierzu 59 Zulassungen ausgesprochen beziehungsweise verlängert. 46 Zulassungen wurden zurückgezogen beziehungsweise durch Zulassungen neuerer Versionen ersetzt. Eine tagesaktuelle Auflistung der zugelassenen IT-Sicherheitsprodukte enthält die BSI-Schrift 7164, die auf der Webseite des BSI zur Verfügung steht.

Optimierung des Zulassungsprozesses

Gegenwärtig betreut das BSI mehr als 60 laufende Verfahren mit dem Ziel einer Zulassung. Um den auch weiterhin stark wachsenden Bedarf der (Bundes-)Verwaltung nach zugelassenen Produkten und sicheren IT-Lösungen decken zu können, wird das BSI den Zulassungsprozess optimieren und die Entwicklung und Bereitstellung von VS-Anforderungsprofilen (VS-AP) deutlich erhöhen. VS-Anforderungsprofile beschreiben IT-Sicherheitsanforderungen für bestimmte Produktklassen und -typen. Sie richten sich zum einen an Anwender und Betreiber, wie beispielsweise Behörden, die Produkte beim Umgang mit eingestuften Dokumenten verwenden wollen und hierfür die grundsätzlichen Anforderungen benötigen, denen geeignete Produkte genügen müssen. Zum anderen richten sich VS-APs an die Hersteller solcher Produkte, um ihnen eine generelle technische Leitlinie zur Umsetzung geltender relevanter IT-Sicherheitsanforderungen zu geben.

Bei der Optimierung des Zulassungsprozesses werden folgende Ziele verfolgt:

I. Vorausschauende Gestaltung informationssichernder Systeme und Komponenten für den VS-Bereich durch das BSI

II. Harmonisierung von IT-Sicherheitsanforderungen bestimmter Produktklassen und -typen

III. Bedarfsgerechte Festlegung von Anforderungen durch unmittelbare Beteiligung von Anwendern, Betreibern und Produktherstellern an der Gestaltung entsprechender VS-APs

IV. Effizienzsteigerung der Zulassungsverfahren im BSI durch frühzeitige Bereitstellung einschlägiger VS-APs

Das BSI hat derzeit drei VS-Anforderungsprofile publiziert. Weitere acht VS-APs werden momentan bearbeitet. Damit deckt das BSI bereits die unterschiedlichsten Produktklassen für den Schutz und die Verarbeitung von eingestuften Informationen ab. Parallel dazu wird eine Vielzahl an VS-APs und nationalen Protection Profiles (nPP) für den Einsatz im VS-Bereich für die Standardisierung weiterer IT-Sicherheitsprodukte vorbereitet. Die Entscheidung, Produkthersteller, Anwender und Betreiber schon frühzeitig in die Gestaltung derartiger IT-Sicherheitsanforderungen zu involvieren, führte im Berichtszeitraum zu einer durchweg positiven Resonanz sowie regen Beteiligung am beschriebenen Vorgehen.

Veraltete Cloud-Software

Sachverhalt
Im Februar 2017 wurde dem BSI bekannt, dass mehrere Zehntausend der in Deutschland betriebenen Private-Cloud-Systeme auf Basis der weit verbreiteten Software ownCloud und Nextcloud mit veralteten Versionen laufen, die nicht mehr von den Herstellern unterstützt werden und teils kritische Sicherheitslücken aufweisen. Unter den Betreibern dieser verwundbaren Cloud-Systeme befanden sich neben Privatnutzern unter anderem viele große und mittelständische Unternehmen, öffentliche und kommunale Einrichtungen, Energieversorger, Krankenhäuser, Ärzte und Rechtsanwälte.

Ursache und Schadenswirkung
Von den Herstellern der Cloud-Software bereitgestellte Updates, welche die Sicherheitslücken schließen, wurden von den Betreibern nicht eingespielt. Dies ermöglichte Angreifern, bekannte Sicherheitslücken in veralteten Versionen der Cloud-Software auszunutzen, um gegebenenfalls sensible in den Clouds gespeicherte Informationen wie zum Beispiel Kundendaten von Unternehmen oder persönliche Dokumente auszuspähen und diese anschließend im Internet zu veröffentlichen oder für kriminelle Zwecke wie Erpressungen zu verwenden. Andere Sicherheitslücken ermöglichen Angreifern die Ausführung beliebiger Programmcodes auf dem Cloud-Server. Dies kann gegebenenfalls zu einer vollständigen Kompromittierung des Systems und dessen Missbrauch für weitere kriminelle Aktivitäten führen.

Reaktion
Das CERT-Bund des BSI informiert deutsche Netzbetreiber regelmäßig über dem BSI bekannte verwundbare Cloud-Systeme in Deutschland. Provider werden gebeten, ihre betroffenen Kunden entsprechend zu informieren und aufzufordern, die Schwachstellen zu schließen.

Empfehlung
Das BSI rät Cloud-Betreibern, den Versionsstand der von ihnen eingesetzten Cloud-Software regelmäßig zu überprüfen und von den Herstellern bereitgestellte Updates schnellstmöglich zu installieren. Die Hersteller der weit verbreiteten Cloud-Software ownCloud und Nextcloud stellen unter https://scan.owncloud.com beziehungsweise https://scan.nextcloud.com einen kostenfreien Dienst zur Verfügung, mit dem Betreiber den Sicherheitsstatus von Clouds auf Basis dieser Software überprüfen können.

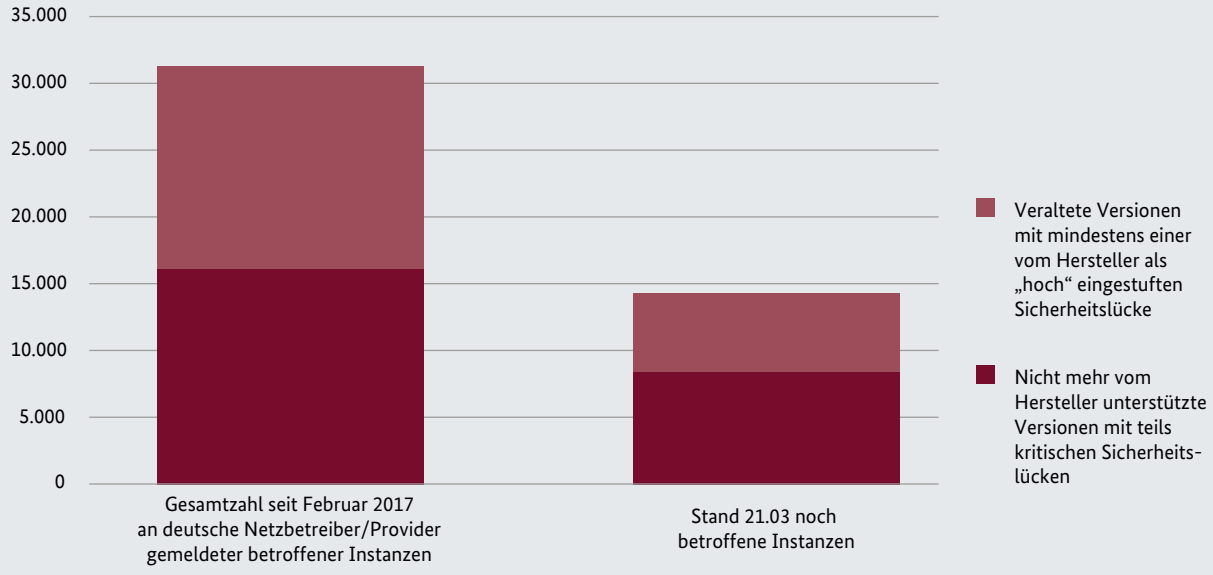


Abbildung 15 Bekannte verwundbare ownCloud / Nextclloud-Instanzen in Deutschland.

Zusammenarbeit mit dem Bundesamt für Wirtschaft und 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 EG-Dual-Use-Verordnung. Ihr Schwerpunkt liegt auf dem Gebiet der Krypto-Exportkontrolle und gliedert sich wie folgt:

I. Unterstützung der deutschen Kryptoindustrie,

II. Schutz zugelassener IT-Sicherheitsprodukte und Komponenten wie zum Beispiel Smartcards und Technologie vor Re-Engineering, Manipulation etc.

Die Bearbeitung dieser Anträge ist eine Querschnittsaufgabe, die eine enge Zusammenarbeit mit externen Behörden, den Antragstellern und Herstellern sowie den zuständigen Fachabteilungen/-referaten erfordert. Um die Zahl der BSI-relevanten Anträge zu reduzieren, wurde mit dem BAFA vereinbart, die Bearbeitung der Anträge auf Ausfuhr-/Verbringungsgenehmigung auf zugelassene IT-Sicherheitsprodukte zu konzentrieren (siehe Abbildung 16). Dies wird seit Mai 2016 umgesetzt.

Zudem wurden 2016 folgende Themen im Kontext der Ausfuhrkontrolle bearbeitet:

- Mitarbeit bei der Überarbeitung der EG-Dual-Use-Verordnung
- Bewertung von Voranfragen (Anträgen) für schutzbedürftige Information, wie zum Beispiel Prüfberichte aus dem CC-Umfeld und Technologie
- Beteiligung bei Firmenverkäufen und -übernahmen im Bereich der Informationssicherheit im Rahmen der Erlassbearbeitung
- Bearbeitung von Exportanfragen im Zusammenhang mit der Verschlüsselungssoftware Chiasmus sowie Unterstützung des BSI-Vertriebs bei der Antragstellung für die Ausfuhr von Chiasmus
- Unterstützung des BAFA bei der Auskunft zur Güterliste (AzG) zur Feststellung der Exportgenehmigungspflicht eines Produktes
- Sicherstellung abgeschlossener MoAs für den Export von zugelassenen IT-Sicherheitsprodukten (ab der Einstufung VS-VERTRAULICH).

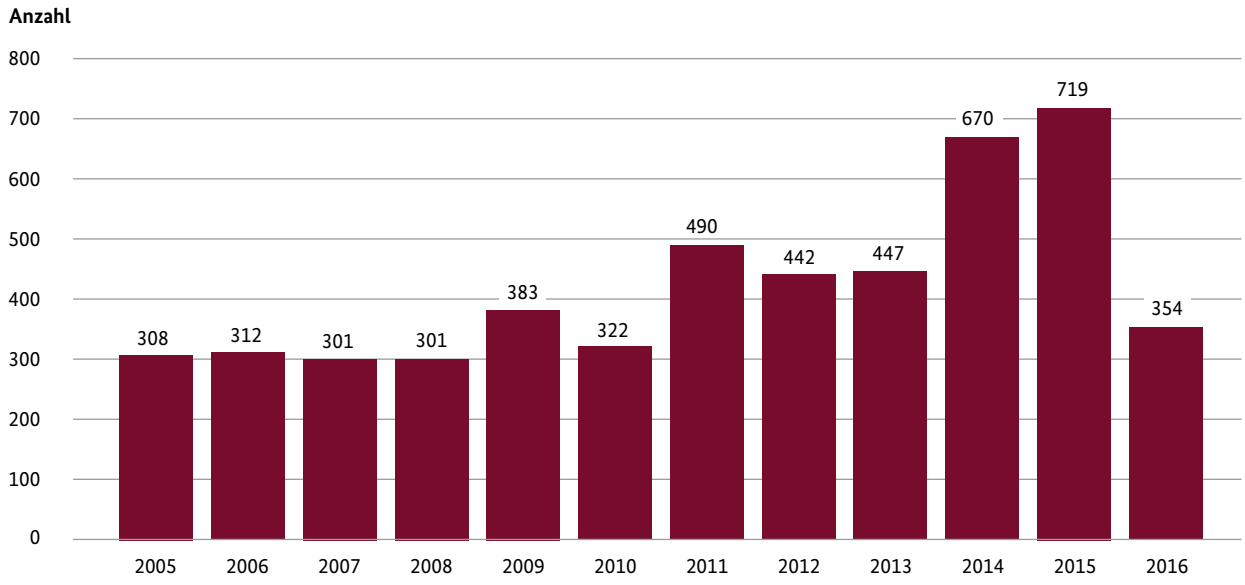


Abbildung 16 Darstellung der Anzahl der im BSI bearbeiteten BAFA-Anträge von 2005 bis 2016

2.3 Zielgruppe Wirtschaft

2.3.1 CERT-Bund und nationales IT-Lagezentrum

Bei der Bewältigung von IT-Sicherheitsvorfällen kommt es darauf an, schnell und angemessen zu reagieren, um den Abfluss von Daten, eine Gefährdung Dritter oder ein weiteres Ausbreiten eines Angreifers im eigenen Netz zu verhindern. Um Betroffene, deren IT-Sicherheitsbeauftragte und Administratoren zu unterstützen, werden Computer-Notfall-Teams eingesetzt (Computer Emergency Response Teams – CERTs; auch bezeichnet als Computer Security Incident Response Teams – CSIRTs). Das BSI verfügt seit 1994 über ein derartiges Team. Es ist seit 2001 als eigenständiges Referat organisiert. 2016 feierte das Referat „CERT-Bund“ somit sein 15-jähriges Bestehen.

Zusätzlich zu Erkenntnissen aus eigenen Analysen erhält CERT-Bund in seiner Rolle als nationales CERT von Partnern und weiteren vertrauenswürdigen externen Quellen Informationen zu Sicherheitsvorfällen in Bezug auf IT-Systeme in Deutschland. Dies umfasst unter anderem Informationen zu Schadprogramm-Infektionen, unzureichend abgesicherten Serverdiensten sowie kompromittierten Systemen beziehungsweise 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. Falls es sich bei dem Netzbetreiber um einen Provider handelt, wird dieser gebeten, seine betroffenen Kunden entsprechend zu informieren.

Das Nationale IT-Lagezentrum des BSI führt eine kontinuierliche Lagebeobachtung der IT-Sicherheit durch. Hierzu wird täglich eine Vielzahl von öffentlichen und nicht öffentlichen Quellen ausgewertet, von Fachmedien über Analysten-Blogs bis hin zu Informationen von IT-Herstellern. Dies gewährleistet die zeitnahe Reaktion auf neu entdeckte Schwachstellen oder bekannt gewordene IT-Sicherheitsvorfälle. Ergänzt werden diese Erkenntnisse durch die Auswertung der Informationen unterschiedlicher Sensoren unter anderem in den Regierungsnetzen sowie weiterführender Analysen.

Im IT-Lagezentrum ist zudem die zentrale Meldestelle des BSI verortet. Hier laufen Vorfallsmeldungen unter anderem von Bundesbehörden im Rahmen der Meldepflichten aus dem Umsetzungsplan Bund (UP Bund) sowie von den Betreibern Kritischer Infrastrukturen aufgrund des IT-Sicherheitsgesetzes zusammen. Hinzu kommen freiwillige Meldungen, zum Beispiel aus der Allianz für Cyber-Sicherheit und dem UP KRITIS. Alle diese Vorfallsmeldungen werden in der Meldestelle erfasst und es wird das weitere Vorgehen koordiniert. Durch die Gesamtsicht der Meldestelle auf alle Vorfallsmeldungen ist es möglich, sowohl die Analyse als auch die Unterstützung der Betroffenen in einem größeren Kontext zu betrachten und kurzfristig Angriffswellen oder neue Angriffsmethoden zu adressieren. Das BSI nutzt die Informationen insbesondere auch zur Information seiner Zielgruppen in Form von Lageberichten, Warnungen und Empfehlungen.

2.3.2 Mobile Incident Response Teams (MIRT)

Mit der Cyber-Sicherheitsstrategie 2016 der Bundesregierung wurde der Fokus des CERT-Einsatzes verstärkt auf die Unterstützung vor Ort gelegt. Das BSI baut daher mobile Einsatzteams – Mobile Incident Response Teams (MIRT) – auf, die bei IT-Sicherheitsvorfällen bei Betroffenen vor Ort tätig werden können. Der Schwerpunkt liegt dabei auf Einrichtungen der Bundesverwaltung und Betreibern Kritischer Infrastrukturen. In herausragenden Einzelfällen können MIRTs auch bei anderen Unternehmen zum Einsatz kommen. Parallel dazu werden die existierenden Strukturen von CERT-Bund sowie auch anderen zuständigen Fachreferaten des BSI ausgebaut.

Hauptaufgabe der MIRTs ist es, bei IT-Sicherheitsvorfällen oder Cyber-Angriffen die Funktionsfähigkeit der betroffenen informationstechnischen Systeme kurzfristig wiederherzustellen. Dies geschieht in enger Abstimmung mit der betroffenen Einrichtung.

Typische Elemente eines MIRT-Einsatzes sind:

- Telefonische Erstunterstützung und Klärung der notwendigen Voraussetzungen für einen Vor-Ort-Einsatz: Welche Sofortmaßnahmen sind möglich? Welche Unterstützung wird benötigt? Wie kann diese Unterstützung möglichst schnell und wirksam geleistet werden?

- Vor-Ort-Einsatz zur Identifikation des wesentlichen Problems: Was ist konkret geschehen? Wie ist es aufgefallen?

- Eingrenzen der Ausbreitung des Problems: Wie weit hat sich ein Angreifer im System ausgebreitet? Welche Systeme sind betroffen? Wie kann eine weitere Ausbreitung verhindert werden?

- Bereinigen der Systeme mit gegebenenfalls vorheriger forensischer Sicherung für eine Auswertung im Labor beziehungsweise für Strafverfolgungsbehörden: Welche Hilfsmittel oder Exploits hat der Angreifer eingesetzt? Wie kann die Erkennung der betroffenen Systeme verbessert werden? Ist eine Bereinigung auch ohne Neuinstallation möglich?

- Wiederanlauf der Systeme: Welche Reihenfolge ist sinnvoll? Welche Systeme könnten gegebenenfalls wieder befallen werden? Welche Ad-hoc-Maßnahmen können einen vorübergehenden Schutz bieten?

Der zeitliche Rahmen für einen MIRT-Einsatz sollte in der Regel zwei Wochen nicht überschreiten. Sollten die Möglichkeiten des BSI zur Unterstützung bei der Bewältigung des Vorfalls nicht ausreichen, können auch Dritte eingeschaltet werden, beispielsweise vom BSI zertifizierte IT-Sicherheitsdienstleister. Das Umsetzungsgesetz zur NIS-Richtlinie hat dafür mit der Ergänzung des §5a des BSI-Gesetzes die entsprechende gesetzliche Grundlage geschaffen.

2.3.3 Gütesiegel

Die Cyber-Sicherheitsstrategie 2016 der Bundesregierung sieht zur Stärkung des sicheren und selbstbestimmten Handelns in einer digitalisierten Umgebung ein Gütesiegel für IT-Sicherheit vor. Es wird ergänzt durch ein Basis-Sicherheitszertifikat, um damit die Testierbereitschaft der Hersteller von IT-Verbraucherprodukten zu fördern und die IT-Sicherheit in diesem Produktbereich nachhaltig zu stärken. Hierbei wird auch die internationale Anerkennung im Europäischen Umfeld berücksichtigt werden.

Das BSI erarbeitet derzeit in enger Kooperation mit den zuständigen Ministerien in der exemplarischen Produktkategorie Netzwerk-Router die notwendigen Voraussetzungen, um ein Gütesiegel zu vergeben. Hierbei werden Hersteller und Verbände sowie Interessenvertreter einbezogen. Das Ergebnis soll dann mit geringem Aufwand auf weitere Produktkategorien übertragen werden, um so die Grundlage für ein breitflächig einsetzbares, vertrauenswürdiges Gütesiegel für IT-Sicherheit zu schaffen.

2.3.4 Allianz für Cyber-Sicherheit

Mit der 2012 gegründeten Allianz für Cyber-Sicherheit betreibt das BSI eine Plattform zum offenen Austausch von Cyber-Sicherheitsinformationen zwischen Behörden, Unternehmen und sonstigen Institutionen. Ziel der Allianz für Cyber-Sicherheit ist es, die Cyber-Sicherheit in Deutschland zu erhöhen und die Widerstandsfähigkeit des Standortes Deutschland gegenüber Cyber-Angriffen zu stärken. Die Allianz verfolgt dabei einen kooperativen Ansatz, um aktuelle Informationen zu Cyber-Bedrohungen zu verteilen, kommende Herausforderungen zu diskutieren und Good Practices zum sicheren Umgang mit diesen zu erarbeiten.

Das durch die Zusammenarbeit mit anderen erlangte Know-how soll den teilnehmenden Institutionen dazu dienen, ihr Cyber-Sicherheitsniveau nachhaltig zu verbessern und die Gefahr zu minimieren, Opfer eines Cyber-Angriffs zu werden. Als Informationsplattform betreibt das BSI die Webseite *www.allianz-fuer-cybersicherheit.de*. Das digitale Angebot wird ergänzt durch offene und geschlossene Veranstaltungen wie Cyber-Sicherheits-Tage, Erfahrungs- und Expertenkreise. Im Rahmen der Allianz für Cyber-Sicherheit stellen die Partner – in der Regel Unternehmen mit besonderer Expertise in Cyber-Sicherheitsthemen – kostenlose Inhalte in Form von Whitepapern oder Seminaren bereit.

Mit der Allianz für Cyber-Sicherheit trägt das BSI der immer weiter steigenden Vernetzung Rechnung. Angesichts der zunehmenden Bedrohung durch Cyber-Angriffe und immer neuer Methoden der Täter gilt es, den Austausch über präventive und reaktive Maßnahmen bei Cyber-Vorfällen voranzutreiben, um vom gegenseitigen Wissenstransfer zu profitieren. Dieses Vorhaben stößt bei den deutschen Institutionen auf reges Interesse: Bis Juni 2017 hatten sich mehr als 2.270 Organisationen für die Teilnahme an der Allianz für Cyber-Sicherheit registriert – ca. 30 Prozent mehr als zum gleichen Zeitpunkt im Vorjahr. Von diesen Mitgliedern stellen mehr als 100 regelmäßig Inhalte für die übrigen Teilnehmer zur Verfügung, ca. 50 verteilen die Informationen als Partner / Multiplikatoren in der Fläche.

Großer Zuspruch

Sowohl das Engagement der Partner als auch das Interesse der Teilnehmer ist beachtlich: Im vergangenen Jahr haben die Partner der Allianz für Cyber-Sicherheit durchschnittlich eine kostenlose Veranstaltung pro Woche irgendwo in Deutschland angeboten. Das BSI kann inzwischen etwa 130 Empfehlungen zu verschiedenen Cyber-Sicherheitsthemen vorweisen, die auf der Internetseite der Allianz für Cyber-Sicherheit veröffentlicht werden. Vom BSI angebotene Veranstaltungen erfreuen sich ebenfalls großer Beliebtheit: Zum ausgebuchten 16. Cyber-Sicherheits-Tag am 21. Februar in Hamburg erschienen über 200 Teilnehmer, bei der hauseigenen Schulung „Übungszentrum Netzverteidigung“ ist das Platzkontingent nach Start der Anmeldungen jeweils innerhalb von wenigen Stunden mehrfach überbucht.

UP KRITIS verhindert Schadcode-Ausbreitung

Sachverhalt
Ein Unternehmen in der Mineralöl-Branche (KRITIS-Sektor Energie) beobachtete einen zugestellten Schadcode als Mailanhang, den die eingesetzten Systeme nicht erkennen konnten. Es meldete den Vorfall zum einen gemäß seiner gesetzlichen Pflicht nach § 8b BSIG an das BSI. Und es informierte zum anderen die über den UP KRITIS und den Branchenarbeitskreis Mineralöl bestehenden Branchenkontakte in einer schnell angesetzten Telefonkonferenz.

Ursache und Schadenswirkung
Der Versand von Schadcode ist ein alltägliches Phänomen, das im Normalfall keinen Anlass zu einer Warnung bietet. Da in der Telefonkonferenz aber klar wurde, dass auch andere Unternehmen in der Branche einen ähnlichen Sachverhalt bei sich festgestellt hatten, änderte sich die Ausgangslage. Da mehrere Unternehmen betroffen waren, gab es einen Anlass für eine allgemeine Warnung.

Reaktion
Das BSI sendete eine entsprechende Warnung an die UP-KRITIS-Teilnehmer und die gemäß BSIG registrierten KRITIS-Betreiber. In der Folge erhielt das BSI Samples zum Schadcode von anderen gewarnten UP-KRITIS-Teilnehmern und konnte diese analysieren. Dies führte zu einem Update der Warnung und zu einer passenderen und zielgenaueren Empfehlung von Maßnahmen und der erforderlichen Sensibilisierung.

Empfehlung
Diese Reaktion zeigt, wie bei akuten Vorfällen ein langfristig aufgebautes, gut funktionierendes Netzwerk des Vertrauens wie im UP KRITIS genutzt werden kann, um Erkenntnisse zu einem Vorfall auszutauschen und die Betroffenheit anderer KRITIS-Betreiber zu ermitteln. Erst die Vernetzung und der Austausch im UP KRITIS gaben dem BSI die Möglichkeit, den Sachverhalt schnell zu analysieren und eine passgenaue Warnung auszusprechen sowie die Rückmeldung aus der Branche zu bekommen.

Aufgrund des Zuspruchs der beteiligten Institutionen wird das BSI die Aktivitäten der Allianz im kommenden Jahr weiter ausbauen. So laufen bereits Planungen, neue branchenspezifische Erfahrungskreise einzurichten. Zudem wird das Informationsangebot um weitere Themenbereiche ergänzt.

2.3.5 UP KRITIS und IT-Sicherheitsgesetz

Im Jahr 2017 feiert der UP KRITIS, die öffentlich-private Partnerschaft zum Schutz Kritischer Infrastrukturen (KRITIS) in Deutschland, sein zehnjähriges Bestehen. 2007 mit ca. 30 Organisationen gestartet, ist die Teilnehmerzahl im UP KRITIS inzwischen auf fast 500 Organisationen angewachsen. Die Teilnehmer (KRITIS-Betreiber, Verbände und Behörden) arbeiten gemeinsam daran, die Versorgung von Wirtschaft, Staat und Gesellschaft mit (lebens-)wichtigen Gütern und Dienstleistungen auch im IT-Zeitalter möglichst störungsfrei aufrechtzuerhalten.

Der kooperative Ansatz von Staat und Wirtschaft beim Schutz Kritischer Infrastrukturen wird auch mit dem Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz, IT-SiG; Umsetzungsgesetz zu NIS-Richtlinie) weiterverfolgt. Die Umsetzung der gesetzlichen Anforderungen sowie die Identifizierung, wer konkret unter die Neuregelungen des Gesetzes fällt, wurde und wird von den KRITIS-Betreibern im UP KRITIS aktiv begleitet.

Anfang Mai 2016 ist der erste Teil der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV) in Kraft getreten. Er regelt in den Sektoren Energie, Wasser, Ernährung sowie Informationstechnik und Telekommunikation, welche Anlagen zu den Kritischen Infrastrukturen im Sinne des IT-SiG gehören. Deren Betreiber müssen die Anforderungen aus dem BSI-Gesetz umsetzen. Dies ist zum einen die Pflicht, dem BSI eine Kontaktstelle zu benennen, über die erhebliche IT-Störungen an das BSI gemeldet werden müssen und über die die Betreiber im Gegenzug Informationen des BSI wie Lagebilder oder Cyber-Sicherheitswarnungen bekommen (§ 8b BSIG). Zum anderen müssen die Betreiber ihre informationstechnischen Systeme, Prozesse und Komponenten, die

für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind, gemäß dem Stand der Technik gegen Störungen absichern (§ 8a BSIG).

Für die Umsetzung dieser Anforderungen gelten entsprechende Fristen, die seit Inkrafttreten der Verordnung laufen. Für die Benennung einer Kontaktstelle sind dies sechs Monate, die für die betroffenen Betreiber im November 2016 abgelaufen sind. Diese Frist wurde vom Großteil der Betreiber der vorher abgeschätzten Kritischen Infrastrukturen eingehalten, so dass für den ersten Teil der Verordnung 205 Betreiber ca. 550 Anlagen beim BSI registrieren ließen.

Zweiter Korb der Verordnung verabschiedet

Der zweite Teil der Verordnung, der die noch verbleibenden Sektoren Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr regelt, ist am 30. Juni 2017 in Kraft getreten. Hier rechnet das BSI bis zum Ablauf der Frist zum 30. Dezember 2017 mit weiteren 800 bis 1.000 zu registrierenden Anlagen. Seitens des BSI sind die erforderlichen Prozesse für die Entgegennahme von Registrierungen und Vorfallsmeldungen etabliert worden, erste Meldungen sind bereits eingegangen. Auch die Betreiber profitieren bereits von den Regelungen des IT-Sicherheitsgesetzes, beispielsweise durch Cyber-Sicherheitswarnungen oder aktuelle Lageinformationen, die das BSI-Lagezentrum mehrmals pro Woche verschickt.

Zur Umsetzung von § 8a BSIG werden in verschiedenen Branchenarbeitskreisen des UP KRITIS branchenspezifische Sicherheitsstandards (B3S) entwickelt. Das BSI begleitet die Erstellung der Standards und hat mehrere Orientierungshilfen als Maßstab herausgegeben. Auch diese wurden in Zusammenarbeit mit den Betreibern Kritischer Infrastrukturen im UP KRITIS erarbeitet. Auf Antrag stellt das BSI die Eignung branchenspezifischer Sicherheitsstandards fest. Der erste branchenspezifische Sicherheitsstandard, der die Anforderungen des BSI erfüllt, ist der B3S Wasser / Abwasser.

2.3.6 Sonstige Maßnahmen für die Wirtschaft

Modernisierung des IT-Grundschutzes

Der IT-Grundschutz ist der meistgenutzte Standard für Informationssicherheit in Deutschland. Die Modernisierung der bewährten BSI-Methodik zum Aufbau eines soliden Informationssicherheitsmanagements nach IT-Grundschutz befindet sich auf der Zielgeraden. Ziel der Modernisierung ist es, besonders kleinen und mittelständischen Unternehmen einen einfachen Einstieg in ein eigenes Sicherheitsmanagement zu ermöglichen. Grundlegende Vorhaben konnten erfolgreich auf den Weg gebracht werden: Auf der CeBIT 2017 wurde der neue Standard 200-2 zur IT-Grundschutz-Methodik als Community Draft vorgestellt, auf der Hannover Messe Industrie 2017 dann der BSI-Standard 200-1 zu den Grundlagen des Informationssicherheitsmanagements. Der Standard 200-3 zum Thema Risikomanagement wurde bereits im Rahmen der IT-Security-Messe it-sa im Oktober 2016 präsentiert. Die drei Standards ersetzen die Vorgänger 100-1 bis 100-3.

Zur diesjährigen Messe it-sa im Oktober 2017 wird der modernisierte IT-Grundschutz in finalisierter Fassung veröffentlicht. Er umfasst die BSI-Standards 200-1, 2, 3 sowie das neue IT-Grundschutz-Kompendium mit rund 80 essenziellen Bausteinen zu verschiedenen Aspekten der Informationssicherheit. Nach der umfangreichen Überarbeitung ist der IT-Grundschutz nun schlanker, praxisnaher und flexibler umsetzbar. Dies gilt besonders für die neuen Bausteine im IT-Grundschutz, die nun auf rund zehn Seiten alle wichtigen Informationen enthalten. Die Anwender sparen dadurch Zeit und Ressourcen.

Anforderungskatalog Cloud Computing (C5)

Im Februar 2016 stellte das BSI einen Anforderungskatalog Cloud Computing vor, den Cloud Computing Compliance Controls Catalogue (C5). Er besteht im Wesentlichen aus drei Teilen, die sich mit den Anforderungen an die Sicherheit, an die Transparenz und an die Prüfung von Cloud-Diensten befassen. Die in 17 verschiedene Bereiche eingeteilten 114 Sicherheitsanforderungen stellen die Mindestanforderungen dar, die professionelle Cloud Services für geschäftsrelevante Daten und Prozesse erfüllen müssen. Zum größten Teil stammen sie aus anderen Standards wie der ISO / IEC 27001 oder der Cloud Controls Matrix der Cloud Security Alliance, da inzwischen hoher informeller Konsens innerhalb der Cloud Security Community erreicht wurde.

Manche Bereiche werden vom C5 stärker betont, wie zum Beispiel Notfallmanagement und Kryptografie. In den Transparenzanforderungen hilft der C5 bei der Entscheidung, ob die Randbedingungen des Cloud-Dienstes den Anforderungen der Cloud-Kunden genügen. Der Nachweis, ob die Anforderungen des C5 erfüllt werden, wird durch Wirtschaftsprüfer erbracht. Angelehnt an die internationalen Normen ISAE 3000, ISAE 3402 und SOC 2 nimmt der C5 einige Konkretisierungen vor. Ziel ist es, Prüfung und Report aussagekräftig zu machen, damit der Cloud-Kunde einen validen Inhalt für sein eigenes Risikomanagement hat.

Abbildung 17 Arne Schönbohm bei „BSI im Dialog mit der Politik“

Durch die Nutzung von bewährten Standards, die neu kombiniert durch die Expertise des BSI ergänzt werden, entstand mit dem C5 ein Standard, der sofort auch internationale Beachtung erhielt. Bis zum Zeitpunkt der Veröffentlichung dieses Lageberichts waren mit Amazon Web Services, Fabasoft und Box bereits drei Cloud-Anbieter testiert, weitere werden erwartet.

European Secure Cloud (ESCloud)

Die European Secure Cloud (ESCloud) ist eine Initiative des BSI und der französischen Partnerorganisation Agence nationale de la sécurité des systèmes d'information (ANSSI). Beide Behörden haben gemeinsame Kriterien an die Cloud-Sicherheit definiert. Cloud-Anbieter, die diese Kriterien durch ein Testat nach C5 oder eine Zertifizierung der ANSSI (SecNumCloud) nachweisen und ihre Dienste in Europa erbringen, erhalten das ESCloud-Label als Gütemerkmal. Die ersten Label sollen im Jahr 2017 vergeben werden, wenn der zugehörige Prozess etabliert ist. Zudem soll noch bei weiteren europäischen Ländern um eine Mitarbeit geworben werden.

Für Cloud-Anwender stellt das Cloud Label eine Erleichterung in der Auswahl eines geeigneten Cloud-Anbieters dar. Die Anbieter können durch die Nutzung des Labels deutlich machen, dass ihre Cloud-Dienste die grundlegenden Sicherheitsanforderungen erfüllen, die entweder durch den deutschen C5-Katalog oder die französische SecNumCloud definiert werden.

2.4 Zielgruppe Gesellschaft

2.4.1 Schutz vor Beeinflussung der Bundestagswahl

Am 24. September 2017 findet die Wahl zum 19. Deutschen Bundestag statt. Zwar geben die Bürgerinnen und Bürger ihre Stimmen in den Wahlbüros mit Stift und Papier ab, dennoch spielt die Digitalisierung auch bei der Bundestagswahl eine große Rolle. Elektronische Kommunikation und Informationsverarbeitung wird unter anderem bei der Organisation der Wahl und bei der Ermittlung des vorläufigen Wahlergebnisses genutzt. Hinzu kommt, dass der vorausgehende Wahlkampf auch in digitalen Medien stattfindet, etwa in Sozialen Netzwerken, in Blogs und anderen Webangeboten. Twitter und Facebook sind heute wichtige Quellen, in denen sich die Bürgerinnen und Bürger über Kandidaten und Parteien informieren.

Vor dem Hintergrund der Berichte aus den USA und Frankreich über Cyber-Angriffe im Zusammenhang mit den dortigen Präsidentschaftswahlen (siehe Infokasten auf S. 66) besteht auch in Deutschland die Sorge, dass Täter auf digitalem Wege versuchen könnten, die Bundestagswahl 2017 zu beeinflussen.

Zwar liegen dem BSI keine konkreten Hinweise über geplante Cyber-Angriffe auf die Bundestagswahl vor, dennoch muss Deutschland auf dieses Szenario vorbereitet sein. Mögliche Ziele für Cyber-Angriffe im Kontext von Wahlen sind insbesondere Organe wie Parlamente, Abgeordnete und Behörden, Parteien (Parteizentralen, Geschäftsstellen,

Wahlbeeinflussung – Sicherheitsvorfälle im Kontext politischer Wahlen

Sachverhalt
In der jüngeren Vergangenheit wurde über eine Vielzahl von gezielten Cyber-Angriffen im politischen Umfeld insbesondere von Wahlen berichtet. So wurden im Vorfeld der US-Präsidentschaftswahlen Computer des Democratic National Committee (DNC) kompromittiert. Die Angreifer erbeuteten eine Vielzahl von Dokumenten. US-Geheimdienste kommen in einem Untersuchungsbericht zu dem Schluss, dass diese Angriffe von zwei russischen Hackergruppen gesteuert wurden, die gleichzeitig im Netzwerk der Demokraten aktiv waren.

Medien berichteten zudem im Juni 2017 über die Veröffentlichung eines angeblichen Top-Secret-Berichts der NSA über Spear-Phishing-Angriffe auf US-Wahlbehörden sowie auf US-Dienstleistungsunternehmen, die in diesem Bereich tätig sind.

Im März 2017 wurden am Tag der Parlamentswahlen in den Niederlanden mehrere tausend Twitter-Konten kompromittiert. Die Angreifer veröffentlichten auf den betroffenen Twitter-Konten Meldungen, die für das vom türkischen Staatschef Erdoğan angestrebte Referendum warben und zugleich Deutschland und die Niederlande anfeindeten. Außerdem wurde eine Vielzahl von Defacement-Angriffen verzeichnet, bei denen beispielsweise Inhalte von Webseiten etablierter Institutionen manipuliert und für propagandistische Zwecke missbraucht wurden.

Im Kontext der französischen Präsidentschaftswahlen im Mai 2017 war die Partei „La République en Marche“ mit ihrem Präsidentschaftskandidaten Emmanuel Macron von Cyber-Angriffen betroffen. Die Täter haben interne Dokumente erbeutet und veröffentlicht.

Ursache und Schadenswirkung
Mithilfe betrügerischer E-Mails und Phishing-Mails haben Hacker ausgesuchte Empfänger mit Schadsoftware infiziert, um so an die Passwörter der Betroffenen zu gelangen. Auf diesem Wege sind sie in den Besitz einer Vielzahl von Dokumenten und umfangreicher E-Mail-Korrespondenz gelangt. Dies ermöglichte einige kompromittierende Veröffentlichungen. Der Missbrauch der Twitter-Konten in den Niederlanden erfolgte über die Webanwendung beziehungsweise „App“ twittercounter.com, mit der Nutzer ihre Twitter-Konten verwalten und unter anderem Nutzerstatistiken und Reports generieren können. Twitter-Nutzer müssen Apps wie twittercounter.com den Zugriff auf das eigene Twitter-Konto explizit erlauben, damit die App Tweets über das jeweilige Konto posten kann. Durch die Kompromittierung der App twittercounter.com konnten Angreifer Inhalte auf Twitter-Konten veröffentlichen.

Reaktion
Die Bundestagswahl 2017 ist Schwerpunkt der kontinuierlichen Lagebeobachtung des BSI, auch im Austausch mit anderen europäischen Ländern wie Frankreich und den Niederlanden, in denen Wahlen stattgefunden haben. Das BSI unterstützt den Bundeswahlleiter und berät diesen etwa bei der Auswahl und Umsetzung von Sicherheitsmaßnahmen, insbesondere zur Härtung von IT-Systemen und IT-Netzen.

Im Rahmen seiner Beratungstätigkeiten zu Fragen der IT-Sicherheit hat das BSI auch Parteien und parteinahe Stiftungen über die Möglichkeit von Cyber-Angriffen informiert und auf Wunsch an besonders kritischen Stellen Penetrationstests durchgeführt. Darüber hinaus hat das BSI Maßnahmen zum digitalen Persönlichkeitsschutz empfohlen. 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, bei der das BSI zahlreiche Abgeordnete und Kandidaten auf deren Wunsch hin unterstützt hat.

Empfehlung
Einerseits zeigt sich die Notwendigkeit, Berichte und Meldungen im Internet und insbesondere in Sozialen Netzwerken kritisch zu hinterfragen. Andererseits müssen Parteien, Politiker und Institutionen im politischen Umfeld sich zunehmend auf gezielte Cyber-Angriffe einstellen und frühzeitig geeignete Sicherheitsmaßnahmen umsetzen. Twitter-Nutzer sollten zum Beispiel regelmäßig überprüfen, welche Apps Zugriff auf das jeweilige Twitter-Konto haben.

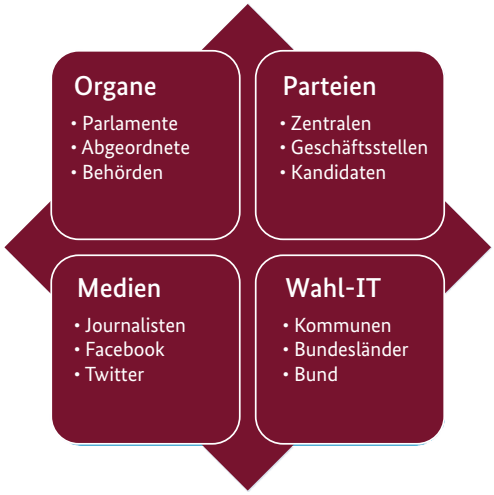


Abbildung 18 Mögliche Ziele von Cyber-Angriffen

Kandidaten), Medien (Journalisten, Redaktionen, Verlage, Online-Plattformen wie Facebook und Twitter) und für die Bundestagswahl genutzte IT auf allen föderalen Ebenen.

Im Rahmen seines gesetzlichen Auftrags stellt das BSI umfangreiche Informations- und Dienstleistungsangebote zum Schutz der Bundestagswahl 2017 bereit. Als Erstes ist hier die Beratung und Unterstützung des Bundeswahlleiters zu nennen, der auf Bundesebene für die Vorbereitung und Durchführung der Bundestagswahl verantwortlich ist (siehe *https://www.bundeswahlleiter.de*). Das BSI berät den Bundeswahlleiter in organisatorischen und technischen Fragen der Informationssicherheit und gibt Empfehlungen zur Konzeption und Umsetzung von Sicherheitsmaßnahmen. Auf Wunsch hat das BSI an besonders kritischen Stellen auch Penetrationstests durchgeführt. Darüber hinaus hat das BSI in Abstimmung mit dem Bundeswahlleiter ein Informationspaket mit Hinweisen und Empfehlungen für die Landeswahlleiter erstellt.

Informationssicherheit kann aber nicht allein durch Maßnahmen der Betreiber und Administratoren erreicht werden, sondern erfordert immer auch die Mitwirkung der Nutzer. Dies betrifft beispielsweise den sicheren Umgang mit sozialen Netzwerken, mobilen IT-Systemen und E-Mail. Im Rahmen mehrerer Informationsveranstaltungen hat das BSI deshalb auch Abgeordnete für Cyber-Sicherheitsrisiken im Kontext Wahlen in Bund und Ländern sensibilisiert und auf entsprechende Angebote mit Hinweisen und Empfehlungen aufmerksam gemacht. Hierzu gehören zwei Veranstaltungen der Reihe „BSI im Dialog“ mit Abgeordneten in Düsseldorf und Berlin.

Ebenso hat das BSI politischen Parteien speziell auf das Thema Wahlen zugeschnittene Informations-, Beratungs- und Unterstützungsleistungen angeboten. Dies ist auf große Resonanz gestoßen. Neben dem Schutz von Informations- und Kommunikationssystemen wurde regelmäßig auch die Gefahr einer Diskreditierung von Personen durch den Missbrauch digitaler Identitäten angesprochen. Insgesamt zeigt sich die Notwendigkeit, Berichte und Meldungen im Internet und insbesondere in Sozialen Netzwerken kritisch zu hinterfragen. Parteien, Politiker und Institutionen im politischen Umfeld müssen sich zunehmend auf gezielte Cyber-Angriffe einstellen.

Als Plattform für die Vorfallsbewältigung und für den Dialog mit Medienunternehmen zum Thema Informationssicherheit nutzt das BSI vor allem die Zusammenarbeit im UP KRITIS und dort insbesondere den Branchenarbeitskreis „Medien“. Auch die speziellen Sicherheitsaspekte der Bundestagswahl hat das BSI auf diesem Wege mit den Medienunternehmen erörtert. Zu Sicherheitsfragen steht das BSI zudem in direktem Austausch mit Social-Media-Anbietern.

Flankierend zu den Beratungs- und Unterstützungsangeboten hat das BSI die Bundestagswahl zu einem Schwerpunkt der Lagebeobachtung im Nationalen IT-Lagezentrum des BSI gemacht. Dies stellt sicher, dass auf relevante Ereignisse mit Bezug zur Bundestagswahl unverzüglich reagiert werden kann, etwa durch Warnmeldungen oder geeignete Schutzmaßnahmen.

2.4.2 Digitalisierungsprojekte in Deutschland

Die zunehmende Digitalisierung und Vernetzung in der Gesellschaft steigert die Effizienz, optimiert die Prozesse und führt zu mehr Komfort, indem Produktkomponenten sowie Systeme untereinander kommunikativ verknüpft werden. Auf der anderen Seite steigt das Bedrohungspotenzial deutlich an, da sich die Anzahl der Angriffspunkte erhöht, die Kommunikationsinfrastrukturen immer komplexer werden und die zu verarbeitenden Datenmengen sich vervielfachen. Die Wahrscheinlichkeit erfolgreicher Angriffe auf digitalisierte Infrastrukturen wird folglich zunehmend größer.

Eine erfolgreiche digitale Transformation kann daher nur gelingen, wenn allgemeinverbindliche Sicherheitsstandards frühzeitig entwickelt und bereitgestellt sowie Maßnahmen umgesetzt werden, um die Vertrauenswürdigkeit digitaler Infrastrukturen zu sichern („Privacy & Security by Design“). Darum sind nationale Referenzmärkte mit sicheren Produktkomponenten, Systemen und Kommunikationsinfrastrukturen entscheidend, um in zukünftigen digitalen Märkten eine führende Gestaltungsrolle einzunehmen und darauf aufbauend die internationale Standardisierung zu gestalten.

Gesundheitsvorsorge

Auch im Bereich der Gesundheitsversorgung ist die Digitalisierung (eHealth) gleichermaßen prägender Faktor und Chance. Das Beispiel der Telematikinfrastruktur zeigt, dass mit zunehmender Vernetzung von Leistungsträgern des Gesundheitssystems die Effizienz der Versorgung zunimmt und gleichzeitig die Sicherheit des Patienten gesteigert werden kann. Neue Anwendungen wie zum Beispiel das Notfalldatenmanagement oder der eMedikationsplan leisten hierzu zukünftig einen weiteren wertvollen Beitrag.

Der Einsatz von zertifizierte Komponenten in sicherheitskritischen Bereichen dieser Infrastruktur unterstützt hier das Ziel einer auch unter Datenschutzapekten sicheren, tragfähigen und flächendeckenden digitalen Weiterentwicklung der medizinischen Versorgung in Deutschland.

Aber auch bei der individuellen Ausstattung von Patienten mit elektronischen Hilfsmitteln (Gesundheitskarte) eröffnet die Digitalisierung neue bisher unerreichte Möglichkeiten, um eventuell vorhandene medizinisch bedingte persönliche Defizite zu kompensieren und so die Lebensqualität Betroffener zu erhöhen. Allerdings schaffen elektronische Zugänge zu den Geräten – wie zum Beispiel zur individuellen Anpassung / Einstellung oder zur (Fern-)Wartung – immer auch ein gewisses Risiko des ungewollten Datenabflusses oder der Manipulation. Auch hier spielen die zur Datensicherheit formulierten Ziele und Forderungen des BSI eine zentrale Rolle.

Sichere Identifizierung von Personen

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 Februar 2017 hat Deutschland die Notifizierung der Online-Ausweisfunktion des Personalausweises und elektronischen Aufenthaltstitels auf dem höchsten Vertrauensniveau gemäß eIDAS-Verordnung eingeleitet. Nach Abschluss der Notifizierung werden alle EU-Mitgliedstaaten ab September 2018 verpflichtet sein, ihre elektronischen Verwaltungsverfahren für die Online-Ausweisfunktion zu öffnen. Auch Unternehmen im EU-Ausland können den elektronischen Identitätsnachweis auf freiwilliger Basis anerkennen. Das BSI hat die technischen Vorarbeiten für die Notifizierung der Online-Ausweisfunktion geleistet und begleitet den gesamten Notifizierungsprozess aus technischer Sicht.

Daneben spielt auch die mobile Nutzung von eID-Technologien wie die Entwicklung und Zertifizierung der mobilen AusweisApp2 für den Personalausweis sowie Smartphones als Kartenleser eine wichtige Rolle. Hierzu engagiert sich das BSI in entsprechenden Standardisierungsgremien wie dem NFC-Forum und FIDO.

Identifizierungsverfahren (TR 03147)

In der Praxis haben sich für die Identitätsfeststellung aber sehr unterschiedliche Verfahren mit unterschiedlichen Sicherheitseigenschaften etabliert. Das BSI entwickelt daher in Abstimmung mit Bedarfsträgern Kriterien zur Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen und veröffentlicht diese in Technischen Richtlinien (vgl. BSI TR-03147). Hierdurch soll in Zukunft eine einheitliche Sicherheitsbewertung von Verfahren zur Identitätsfeststellung – wie etwa Verfahren mit persönlicher Anwesenheit oder von videobasierten Verfahren – erleichtert werden.

Smart Borders

Ein ganz anderer Einsatzbereich neuer Technologien findet sich im klassischen Grenzkontrollprozess. Während Reisende aus europäischen Ländern schon seit mehreren Jahren an den Schengen-Außengrenzen komfortabel mit dem EasyPASS-System der Bundespolizei die Grenzkontrolle im Self-Service durchführen können, wird in den nächsten Jahren mit der Einführung des europäischen Ein-/Ausreiseregisters die Digitalisierung des Grenzkontrollprozesses weiter vorangetrieben. Das System erlaubt dann die biometrische Erfassung und Suche von Drittstaatenangehörigen und dokumentiert die einzelnen Ein- und Ausreisen in den Schengen-Raum. Das BSI unterstützt die Bundespolizei in den Bereichen der sicheren Prüfung von hoheitlichen Reisedokumenten (optisch und elektronisch) und in der biometrischen Datenerfassung der Reisenden. Dadurch wird ein übergreifendes Werkzeug für das Identitätsmanagement im gemeinsamen Raum der Freizügigkeit geschaffen. Die Vorgaben und Zertifizierungen des BSI werden dabei für ein durchgehend hohes Sicherheitsniveau der Prozesse Sorge tragen.

Umsetzung der Energiewende

Das BSI entwickelt im Auftrag des Bundesministeriums für Wirtschaft und Energie Schutzprofile und Technische Richtlinien sowie Prüfverfahren für das Smart-Meter-Gateway als zentrale Kommunikationsplattform intelligenter Messsysteme. Zusammen mit den technischen Standards des BSI schafft das Gesetz zur Digitalisierung der Energiewende damit verbindliche Rahmenbedingungen für den sicheren und datenschutzkonformen Einsatz von Ladesäulen und zeigt bereits perspektivisch auf, wie die Mindestanforderungen gestaltet werden müssen, um die Ladesäuleninfrastruktur von Elektromobilen sicher in das intelligente Stromnetz zu integrieren. Deutschland ist damit in diesem Bereich Vorreiter in Europa.

Smart Home / Internet of Things (IoT)

Smart Services, Smart Home, Smart Building oder Smart City (Urbanisierung 2.0) sind Beispiele dafür, wie die voranschreitende Digitalisierung durch das Internet der Dinge Einzug in fast alle Lebensbereiche hält. Neben den damit einhergehenden Komfortverbesserungen entsteht aber gleichzeitig ein Einfallstor für Cyber-Angriffe. Gerade im Consumer-Marktsegment sind viele Geräte nicht oder nur unzureichend vor Cyber-Angriffen geschützt. Neben der persönlichen Bedrohung des Nutzers (zum Beispiel durch Zugriff auf oder Ausspähen von Eigentum) kann die schiere Menge der IoT-Geräte auch für DDoS-Angriffe missbraucht werden und enormen Schaden bei Dritten anrichten.

Die Gewährleistung von „security by design“ für IoT-Endgeräte ist ein hervorzuhebendes Ziel des BSI. Es soll erreicht werden, indem kompakte und modulare Sicherheitsstandards geschaffen und international verankert werden. Hier spielen Funktionalitäten zur sicheren Software-Aktualisierung über den vollständigen Lebenszyklus der Geräte, starke und aktualisierbare kryptografische Mechanismen und die Verwendung von eingebetteten Hardware-Sicherheitskomponenten für die Ausführung sicherheitskritischer Funktionen wichtige Rollen.

Vernetztes Fahren und Intelligente Verkehrssysteme

Auch im Straßenverkehr macht sich die Digitalisierung bemerkbar. Durch Intelligente Verkehrssysteme, in denen vernetzte Fahrzeuge und Infrastrukturkomponenten Daten austauschen, sollen zukünftig Unfälle und Verkehrsstörungen verhindert und das Fahren komfortabler gemacht werden. Derartige Systeme sind aber nur dann vertrauenswürdig, wenn zum Beispiel die Authentizität der dabei ausgetauschten Nachrichten gewährleistet ist. Das BSI wirkt in diesem Kontext an Sicherheitsrichtlinien für die notwendigen Public-Key-Infrastrukturen in der Fahrzeug-zu-Fahrzeug- und Fahrzeug-zu-Infrastruktur-Kommunikation mit.

Zahlreiche Fahrzeugmodelle bieten bereits heute Komfortfunktionen an, die auf einer mobilen Anbindung an das Internet basieren. Auch hier besteht die Gefahr von Cyber-Angriffen, wie bereits in den vergangenen Jahren für einzelne Fahrzeugmodelle demonstriert wurde. Gemeinsam mit dem Bundesministerium für Verkehr und Infrastruktur (BMVI) und weiteren Behörden diskutiert das BSI, welche Mindestanforderungen im Bereich der IT-Sicherheit zukünftig von vernetzten und automatisierten Fahrzeugen erfüllt sein müssen.

2.4.3 Plattform für Diskurs zur sicheren Informationsgesellschaft

Das BSI hat den bereits im Jahr 2016 intensivierten Kurs der Förderung des gesamtgesellschaftlichen Diskurses zu Themen der Cyber-Sicherheit fortgeführt. Im Rahmen des Projektes „Digitale Gesellschaft: smart & sicher“ (*https://www.bsi.bund.de/susi*) wurden die Aktivitäten gebündelt und der offene Interessenaustausch im Dialog mit Vertreterinnen und Vertretern aus Zivilgesellschaft, Kultur, Wissenschaft, Wirtschaft und Verwaltung weiter vorangetrieben.

Das BSI bietet mit der Veranstaltung „Denkwerkstatt sichere Informationsgesellschaft“ eine Plattform, um über Fragen der Cyber-Sicherheit in einer digitalisierten Gesellschaft mit einem breiten Spektrum an Akteuren zu diskutieren. Im Fokus der Veranstaltungen im Februar und Juni 2017 standen facettenreiche und konstruktive Debatten. Während bei der Veranstaltung im Februar 2017 die zentralen Fragestellungen um die Themen „Sicherheit und Technologie“, „Verantwortung“ und „Vertrauen“ mithilfe von Kleingruppendiskussionen in Form eines „World Cafés“ identifiziert wurden, stand im Juni 2017 die Reflexion der Ergebnisse der Empirie und die gemeinsame Erarbeitung eines Impulspapiers im Vordergrund. Auf Basis von Experteninterviews, einer repräsentativen Bevölkerungsumfrage und einer Befragung von 20 Bürgerinnen und Bürgern in einer Online-Community wurden gemeinschaftlich Impulse für eine sichere Informationsgesellschaft entwickelt.

Die Ergebnisse des Prozesses und das Impulspapier werden im September 2017 in Berlin der Öffentlichkeit präsentiert. Sie stellen die Grundlage für die weitere Arbeit des BSI in diesem Bereich dar. Der aufschlussreiche Diskurs hat das BSI motiviert, diesen Weg konsequent fortzusetzen, um auch weiterhin im gesamtgesellschaftlichen Austausch eine sichere Informationsgesellschaft zu gestalten.

2.4.4 Sonstige Maßnahmen für die Gesellschaft

Bürger-Services des BSI

Eine wichtige Aufgabe des BSI ist die Information und Sensibilisierung von Bürgerinnen und Bürgern für einen sicheren Umgang mit Informationstechnologie, mobilen Kommunikationsmitteln und Internet. Unter https://*www.bsi-fuer-buerger.de* wird ein speziell für Privatanwender zugeschnittenes Internetangebot bereitgestellt. Dabei behandelt das BSI die vielfältigen Themen und Informationen rund um das Thema IT- und Internet-Sicherheit so, dass sie auch für technische Laien verständlich sind. Neben der reinen Information bietet das BSI für Bürger konkrete und umsetzbare Handlungsempfehlungen an, beispielsweise zu Themen wie E-Mail-Verschlüsselung, Smartphone-Sicherheit, Online-Banking, Cloud Computing oder Soziale Netzwerke. Auf die Website wurde im Berichtszeitraum von durchschnittlich 243.000 Besuchern pro Monat zugegriffen. Gegenüber dem Vorjahr bedeutet dies einen Zuwachs von 40 Prozent.

In den Sozialen Medien bietet das BSI über die Facebook-Seite (*www.facebook.com/bsi.fuer.buerger*) und den seit März 2016 aktiven Twitter-Kanal (*www.twitter.com/BSI_Presse*) Internetnutzern die Möglichkeit, sich über IT-Sicherheit zu informieren und mit dem BSI in einen Dialog zu treten. Zum Stichtag 30. Juni 2017 taten dies 31.738 Fans (Facebook) und 7.483 Follower (Twitter). Beide Kommunikationskanäle werden vor allem auch genutzt, um bei IT-Sicherheitsvorfällen schnell und flächendeckend zu informieren. Resonanzen zeigen dabei, dass das BSI als fachkompetente Stelle für IT-Sicherheits-Informationen überaus geschätzt wird.

Auch telefonisch unter 0800 2741000 oder per E-Mail unter mail@bsi-fuer.buerger.de können sich Privatanwender mit ihren Fragen zu Themen der IT- und Internetsicherheit an das BSI wenden. Das Service-Center des BSI nimmt jeden Monat durchschnittlich rund 450 Anfragen von Privatanwendern entgegen.

Darüber hinaus bietet das BSI mit dem „Bürger-CERT“ einen kostenlosen Warn- und Informationsdienst, der Bürger und kleine Unternehmen schnell und kompetent über Schwachstellen, Sicherheitslücken und anderen Risiken informiert und konkrete Hilfestellungen gibt. Derzeit nutzen rund 105.000 Abonnenten dieses Informationsangebot, rund 3.000 Nutzer mehr als im Vorjahreszeitraum. Der vierzehntägige Bürger-CERT-Newsletter „Sicher • Informiert“ liefert einen Überblick der wichtigsten IT-Sicherheitsnachrichten. Im Jahr 2017 wurde das gesamte Bürger-CERT-Angebot auf der Webseite „BSI für Bürger“ integriert. Seitdem finden die Besucherinnen und Besucher des Onlineportals alle wichtigen Informationen von Warnungen bis zu grundlegendem IT-Wissen gebündelt an einem Ort.

Europäischer Monat der Cyber-Sicherheit (ECSM)

Im Oktober 2016 fand europaweit unter Federführung der European Network and Information Security Agency (ENISA) der Europäische Monat der Cyber-Sicherheit (ECSM) statt. Zu unterschiedlichen Themenschwerpunkten der Cyber-Sicherheit wurde die Öffentlichkeit informiert und sensibilisiert. Das BSI übernahm in Deutschland die Rolle der nationalen Koordinierungsstelle und beteiligte sich zudem mit eigenen Aktionen. Es konnten 73 Partner gewonnen werden, die sich mit über 120 Aktionen am ECSM beteiligten. Die Aktionen reichten dabei von Mitarbeitersensibilisierung in Unternehmen über Live-Hacking-Aktionen bis zu Webinaren und Informationsveranstaltungen. Eine Übersicht zu diesen Aktionen findet sich auf *www.bsi.bund.de/ecsm*.

Das BSI selbst informierte zu den Schwerpunktthemen „Sicher online bezahlen“, „Cyber-Gefahren (er)kennen“, „Fit in IT-Sicherheit“ und „Smartphone & Co – sicher mobil“. Hierzu erstellte es unter anderem eine Serie von animierten Erklärvideos. Auf Facebook wurde im gesamten Oktober ein Cyber-Sicherheits-ABC gepostet, in dem unterschiedliche Begrifflichkeiten erklärt wurden. Abgerundet wurden die Aktionen des BSI durch ein Online-Quiz au*f www.bsi-fuer-buerger.de*.

Im Vorfeld des ECSM standen Ende September 2016 Experten der Sicherheitsberatung im BSI bei einem Webinar von klicksafe.de den Fragen von Eltern und (Medien-)Pädagogen zum Thema Basisschutz Rede und Antwort. Gemeinsam mit der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK) befragte das BSI außerdem Bürger online, welche Schutzmaßnahmen sie nutzen, wo sie sich zum Thema IT-Sicherheit informieren und welche Erfahrungen sie mit Cyber-Kriminalität gemacht haben. An der Umfrage beteiligten sich insgesamt über 1.600 Bürgerinnen und Bürger.

Anlässlich des ECSM lud das BSI ferner am 5. Oktober 2016 Vertreter aus Zivilgesellschaft, Medien, Verwaltung und Think Tanks im Europäischen Haus in Berlin ein und diskutierte unter anderem die Frage, wie sich Cyber-Sicherheit für die Gesellschaft gestalten lässt. In der Diskussion erörterten die Teilnehmer unter anderem Aspekte der Erfolgsmessung von Sensibilisierungsmaßnahmen, der Integration von IT-Sicherheitsmaßnahmen in Produkten für Privatanwender sowie der Aufklärung in Schulen und Bildungseinrichtungen.

Kooperation mit der Verbraucherzentrale Nordrhein-Westfalen

Einen wichtigen Teil des kooperativen Gestaltungsansatzes des BSI stellt die vertrauensvolle Zusammenarbeit mit anerkannten Akteuren im Bereich Cyber-Sicherheit für die Gesellschaft dar. Das BSI hat bereits in mehreren Feldern erfolgreich und konstruktiv mit der Verbraucherzentrale NRW zusammengearbeitet. Diese Kooperation wurde nun mit der Unterzeichnung eines Memorandum of Understanding Anfang März 2017 gefestigt.

Durch die Kombination aus der technischen Expertise des BSI auf der einen und der verbraucherrechtlichen Perspektive und der Befugnisse der Verbraucherzentrale NRW auf der anderen Seite kann mit der gemeinsamen Arbeit die Informationssicherheit für die Bürger gesteigert werden. Ein Beispiel für die erfolgreiche Zusammenarbeit stellt das aktuell laufende Klageverfahren gegen einen Verkäufer eines Smartphones mit nicht mehr behebbaren Sicherheitslücken dar. Dieses Verfahren wurde nur auf Grundlage der technischen Prüfung des BSI möglich.

Kooperation mit der Polizeilichen Kriminalprävention der Länder und des Bundes

Risikobewusstsein schärfen, Selbstschutz ermöglichen und verhindern, dass Privatanwender Opfer von Cyber-Kriminalität oder gar unwissentlich zu Tätern werden: Diese Prämissen sind Teil der Präventionsarbeit des BSI und des Programms Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK). Anfang April 2017 unterzeichneten BSI-Präsident Arne Schönbohm und Gerhard Klotter als Vorsitzender der Projektleitung des ProPK in Stuttgart eine gemeinsame Vereinbarung zur strategischen Kooperation der beiden Organisationen.

Bereits in der Vergangenheit haben BSI und ProPK gemeinsam zu Themen der IT- und Internetsicherheit agiert: Mit der Online-Anwendung „Sicherheitskompass“ klären sie zu zehn häufigen Sicherheitsrisiken im Internet auf, das Medienpaket „Verklickt“ für den Schulunterricht vermittelt Jugendlichen sicherheitsbewusstes Verhalten im digitalen Alltag, unter anderem in Bezug auf Cyber-Mobbing, auf Soziale Netzwerke oder Persönlichkeitsrechte.

2.5 Kryptografie als Grundlage der IT-Sicherheit

2.5.1 Deutschland als Verschlüsselungsstandort Nr. 1

Die von der Bundesregierung beschlossene „Digitale Agenda“ ebenso wie die „Charta zur Stärkung der vertrauenswürdigen Kommunikation“ geben das Ziel aus, Deutschland zum „Verschlüsselungsstandort Nr. 1 auf der Welt“ zu machen, zum Schutz der Bürger, der Wirtschaft und der Verwaltung vor Ausspähung oder Manipulation ihrer Kommunikation.

Auf dieses Ziel ist die Arbeit des BSI ausgerichtet. Es setzt dabei ausnahmslos auf den Einsatz von starker Kryptografie als grundlegende Voraussetzung, um Authentizität, Integrität und Vertraulichkeit von digitalen Informationen gewährleisten zu können.

Zur Förderung dieses Ziels wurde die „Fokusgruppe Verschlüsselung“ als Initiative von Wirtschaft, Fachverbänden, Verbraucherorganisationen sowie Politik und Wissenschaft gegründet. Sie hat im Herbst 2015 eine „Charta zur Stärkung der vertrauenswürdigen Kommunikation“ (*www.krypto-charta.de*) aufgesetzt, die bereits von einer Vielzahl an Unternehmen und Vereinen unterzeichnet wurde. Das BSI unterstützt die Arbeit der Fokusgruppe aktiv, hat an der Formulierung der Charta mitgewirkt und ist neben dem BMI einer der ersten Unterzeichner.

Die Unterzeichner der Charta bekennen sich unter anderem zu

- Einfachheit,
- Technologieneutralität / Aktualität / Standardkonformität,
- Transparenz und Vertrauenswürdigkeit und
- Security made in Germany / Europe.

Damit sollen nutzerfreundliche, transparente, sichere Verschlüsselungslösungen gefördert und starke Algorithmen ohne Hintertüren garantiert werden, um das Vertrauen der Bürger sowie kleiner und mittelständischer Unternehmen in die Sicherheit und Integrität der digitalen Welt zu stärken.

Der inhaltliche Schwerpunkt der Aktivitäten der Fokusgruppe liegt dabei auf der Ende-zu-Ende-Verschlüsselung bei der E-Mail-Kommunikation. Diese ermöglicht den Nutzern, die Inhalte ihrer E-Mails durchgehend vom Sender zum Empfänger ohne Einsehbarkeit von vermittelnden Systemen vor unerwünschtem Mitlesen zu schützen.

Die Verschlüsselung von E-Mails auf dem Transportweg, also zwischen den Servern der großen E-Mail-Provider im Internet, ist heute bereits gut etabliert (Transportverschlüsselung) und geschieht normalerweise automatisch durch die Provider ohne Mitwirkung der Nutzer.

Die nutzerindividuelle Ende-zu-Ende-Verschlüsselung wird dagegen bis heute insbesondere in der E-Mail-Kommunikation aufgrund mangelnder Sensibilisierung und Angebote noch viel zu wenig genutzt und ist dort noch eine Nischenanwendung, im Gegensatz etwa zu den inzwischen etablierten verschlüsselnden Messengern. Hier sollen nutzerorientierte, technikneutrale und sichere Angebote geschaffen und gefördert werden. Unter anderem durch die Initiative „Volksverschlüsselung“ und die angebotenen Lösungen von 1&1, GMX und Web.de ist eine positive Entwicklung angestoßen worden.

Die Fokusgruppe Verschlüsselung versucht darüber hinaus zum Beispiel in einem organisierten Speed-Dating, Unternehmen zusammen zu bringen, die einen Beitrag zu Verschlüsselungslösungen liefern. Dabei sollen Synergieeffekte gefunden und diese effizient genutzt werden, um dadurch die Angebote für die Wirtschaft und Bürger zu optimieren. In letzter Zeit konnte bereits festgestellt werden, dass es immer mehr benutzerfreundliche Angebote auf dem Markt gibt, die den Einsatz von starker Verschlüsselung voranbringen sollen.

Auch im BSI gibt es mehrere Projekte rund um sichere E-Mail-Kommunikation (unter anderem auf Basis des freien Kryptografie-Systems GNU Privacy Guard / GnuPG). Außerdem müssen Diensteanbieter, die De-Mail-Dienste zur Verfügung stellen wollen, durch das BSI akkreditiert werden. Durch die Technischen Richtlinien des BSI werden zudem Vorgaben für den sicheren E-Mail-Transport, De-Mail sowie allgemein für den Einsatz von starker Kryptografie in IT-Sicherheitsprodukten gemacht.

2.5.2 Botan – Sichere Implementierung einer allgemeinen Krypto-Bibliothek

Kryptografische Bibliotheken werden häufig als Kernkomponenten in Sicherheitsanwendungen eingesetzt. Sie sind von zentraler Bedeutung, um die Sicherheitsziele zu erreichen. Das Angebot an verfügbaren Bibliotheken für diesen Anwendungsbereich ist groß und stetig wachsend. Allein im TLS-Umfeld gibt es zurzeit rund 15 quelloffene Bibliotheken wie zum Beispiel das bekannte und weit verbreitete OpenSSL. Aufgrund des oftmals großen Umfangs, der hohen Komplexität und der zum Teil jahrelang gewachsenen Struktur dieser Bibliotheken ist der konkrete Einsatz in Kryptoprodukten jedoch fehleranfällig und eine Evaluierung der verwendeten Kryptografie praktisch nicht vollständig möglich.

Aus diesen Gründen führt das BSI das Projekt „Sichere Implementierung einer allgemeinen Kryptobibliothek“ mit dem Auftragnehmer Rohde & Schwarz Cybersecurity GmbH durch. Ziel ist es, eine quelloffene, sichere, übersichtliche, kontrollierbare, gut dokumentierte und damit auch evaluierbare Kryptobibliothek bereitzustellen, die für möglichst viele Einsatzszenarien geeignet ist und auch in Anwendungen mit erhöhtem Sicherheitsbedarf eingesetzt werden kann.

Dazu wurde in einer ersten Analysephase aus allen gängigen Open-Source-Kryptobibliotheken die Bibliothek Botan als geeignete Grundlage für die weitere Entwicklung ausgewählt. In der daran anschließenden Entwicklungsphase wurde Botan tiefer gehend kryptografisch untersucht und bestehende Mängel wurden behoben. Fehlende Krypto-Primitive und -Standards wurden gemäß den Technischen Richtlinien des BSI nachimplementiert, die Testsuite wurde verbessert und eine Testspezifikation erstellt. Außerdem wurde die Resistenz gegen Seitenkanalangriffe durch geeignete Software-Gegenmaßnahmen verbessert und die Möglichkeit zur Einbindung von kryptografischer Spezialhardware geschaffen. Die Dokumentation von Botan wurde verbessert und erweitert.

Alle im Rahmen des Projekts an Botan durchgeführten Änderungen und Erweiterungen sind an das Originalprojekt zurückgeflossen. Dadurch entspricht die durch das BSI entwickelte Bibliothek im Wesentlichen der aktuellen, öffentlich verfügbaren Version von Botan (siehe https://botan.randombit.net/).

Um die Sicherheit und Aktualität der Kryptobibliothek auch für die Zukunft zu gewährleisten und auf neue wissenschaftliche Entwicklungen, Sicherheitsbedrohungen oder Einsatzszenarien angemessen reagieren zu können, wird die Bibliothek in der laufenden Wartungsphase des Projekts für die nächsten Jahre weiter gepflegt und nach Möglichkeit dabei regelmäßig mit dem offiziellen Botan-Stand synchronisiert.

2.5.3 BSI-Projekt: Studie „Bewertung gitterbasierter kryptografischer Verfahren“

Mit Hinblick auf die mögliche Entwicklung eines universellen Quantencomputers muss die heute gängige Public-Key-Kryptografie möglichst bald durch Verfahren ersetzt oder ergänzt werden, die auch gegen Angriffe mit ebensolchen Quantencomputern resistent sind. Heute schon gut verstanden und standardisiert sind Signaturverfahren, die Hashbäume verwenden („hashbasierte Signaturen“). Diese gelten als resistent gegen Quantencomputer. Es gibt allerdings keine hashbasierten Verfahren zur Schlüsseleini-

Virenschutz

Eine moderne Virenschutz-Software ist für die meisten IT-Nutzer immer noch unverzichtbar. Privatnutzer sollten unter Microsoft Windows in jedem Fall eine gut getestete, kostenlose Internet-Sicherheitssuite einsetzen. Sicherer sind kostenpflichtige Varianten, die einen größeren Funktionsumfang und besseren Support bieten und sich nicht durch Werbung oder Auswertung von Nutzerdaten finanzieren.

Professionelle IT-Nutzer sollten bei größeren Netzwerken nur ausgewiesene Enterprise-Produkte einsetzen, die gegenüber den Consumer-Produkten einen wesentlich erweiterten Funktionsumfang aufweisen (zum Beispiel zentrales Management, Applikationskontrolle, Schwachstellenscanner). Ein Enterprise-Schutz besteht aus einer Vielzahl unterschiedlicher Produkte, die sich zu einer komplexen IT-Sicherheitsinfrastruktur zusammenfügen. Die wichtigste Komponente ist der Endgeräteschutz (Endpoint-Protection), der über die meisten Erkennungsverfahren verfügt. Gateway-Produkte sind – ähnlich wie Spamfilter – unerlässlich, bieten aber alleine keinen ausreichenden Schutz.

Die reine Erkennungsleistung etablierter Schutzprogramme unterscheidet sich kaum. Die Detektionsraten bei unterschiedlichen Konfigurationen desselben Produkts können jedoch erheblich sein. Es kommt daher darauf an, das gewählte Produkt optimal zu konfigurieren, sicher zu beherrschen und auf erkannte Gefahren adäquat zu reagieren. Der Ressourceneinsatz bei Planung, Implementierung, Betrieb und Audit ist wesentlich höher als in früheren Zeiten. Eine Verbindung zur Cloud des Herstellers erhöht die Detektionsrate erheblich, birgt aber auch die Gefahr ungewollter Datenübertragungen. Das BSI fordert daher von den Herstellern, ihren Kunden die in die Cloud übertragenen Daten zu spezifizieren und die Art und Weise der Nutzung offenzulegen.

Um Schadsoftware zielgerichteter zu erkennen, sind die unterschiedlichen Sensoren heute vernetzt und nutzen zum Teil zentrale Analysekomponenten. Die Entscheidung für einen Hauptlieferanten von Schutztechnik kann daher Vorteile bieten. Dieses Portfolio lässt sich dann punktuell durch weitere Produkte anderer Hersteller ergänzen. Bei Schutzsoftware, die hauptsächlich mit bekannten Suchmustern (Signaturen) arbeitet (zum Beispiel am Gateway oder bei Datenträgerschleusen) ist dagegen weiterhin eine Multi-Vendor- beziehungsweise Multi-Engine-Strategie sinnvoll.

Moderne Schutzprogramme erkennen viele, aber nicht alle Angriffe. Gegen gezielte Angriffe oder neue Angriffstechniken bieten sie nur eingeschränkten Schutz. Neben Schutzprogrammen sollten daher immer die bekannten Basis-Sicherheitsmaßnahmen umgesetzt werden: eine sichere Netzwerk- und Systemarchitektur, regelmäßige Updates und eine sichere Authentisierung mit starken Passwörtern und Zweifaktor-Authentisierung.

Im Enterprise-Bereich werden zunehmend spezielle Analysesysteme und Virtualisierungstechniken eingesetzt. Dabei werden verdächtige Dateien automatisiert in einer gesicherten Umgebung ausgeführt und analysiert beziehungsweise Anwendungen so gekapselt, dass ein Schadprogramm keinen Zugriff auf wichtige Daten oder Programme nehmen kann.

gung oder Verschlüsselung. Kandidaten für solche Verfahren basieren auf

- der Schwierigkeit, allgemeine fehlerkorrigierende Codes effizient zu dekodieren („codebasierte Verfahren“),
- der Schwierigkeit, Isogenien zwischen elliptischen Kurven zu berechnen („isogeniebasierte Verfahren“) oder
- der Schwierigkeit von bestimmten Problemen in mathematischen Gittern („gitterbasierte Verfahren“).

Im Auftrag des BSI haben Forscher der Technischen Universität Darmstadt eine Studie zur „Bewertung gitterbasierter kryptografischer Verfahren“ erstellt. Ziel dieser Studie war es, eine Analyse der bisherigen Veröffentlichungen von gitterbasierten Public-Key-Verfahren (Schlüsseleinigung, Signatur und Verschlüsselung) zu erhalten. Dafür wurden im ersten Teil zunächst die theoretischen Grundlagen, also die verschiedenen Gitterprobleme und Reduktionen zwischen diesen, sowie die verschiedenen Ansätze zum Lösen von Gitterproblemen (beispielsweise Gitterbasisreduktion) zusammengetragen. Dies bildet die Grundlage, um die Sicherheit von gitterbasierten Verfahren zu bewerten. Der zweite Teil der Studie besteht aus einer Übersicht über diese Verfahren und einer Bewertung von ausgewählten Verfahren auf Basis der Ergebnisse des ersten Teils. Die Studie ist auf der Internetseite des BSI veröffentlicht.

2.5.4 Analyse der Zufallserzeugung in virtualisierten Umgebungen

In einer Studie des BSI wurde untersucht, wie Virtualisierungstechniken, die zum Beispiel bei Cloud-Diensten zum Einsatz kommen, die Entropie von Betriebssystem-Rauschquellen beeinflussen und was getan werden kann, um die Versorgung der virtuellen Maschinen (VM) mit genügend

Zufall sicherzustellen. Exemplarisch wurde dabei der quelloffene Zufallszahlengenerator von Linux in virtuellen Maschinen untersucht, die auf verschiedenen virtuellen Maschinenmonitoren (VMM) wie KVM, Oracle VirtualBox, Microsoft Hyper-V und VMware ESXi liefen.

Im Ergebnis war in allen Kombinationen bei entsprechender Konfiguration eine ausreichende Entropie-Versorgung der Linux-VMs möglich. Unterschiedliche Rauschquellen erfüllten ihre Aufgabe allerdings unterschiedlich gut, sodass sich je nach Einsatzszenario durchaus Probleme ergeben können, zum Beispiel für die Qualität der Zufallszahlen kurz nach dem Systemstart. Mit einem Fragenkatalog werden Anwender daher in die Lage versetzt, selbst zu analysieren, ob solche Probleme auf sie zukommen, sodass sie vorab die kritischen Informationen von ihrem Systemlieferanten einfordern können.

Prinzipiell müssen Anwender ihrem VMM (und dessen Betreiber) vertrauen und sollten sich nicht auf eine einzige Rauschquelle verlassen.

- Software-basierte Rauschquellen, die Hardware-Unterstützung für ihre Entropiegewinnung brauchen, können am ehesten problematisch sein und müssen daher am genauesten auf ihre Eignung für die Einsatzumgebung geprüft werden.

- Software-basierte Rauschquellen, die hochauflösende Zeitstempel zu Systemereignissen auswerten, funktionieren in virtuellen Umgebungen genauso gut und bisweilen sogar besser als in nicht virtualiserten Umgebungen.

- Hardware-Rauschquellen bleiben von der Virtualisierung meist unberührt. Bei einer geeigneten Kombination kann der VMM sein Gastsystem bei der Gewinnung von Entropie auch unterstützen.

2.5.5 Technische Richtlinie BSI-TR-02102 und ECC-Seitenkanal-Leitfaden

BSI-TR-02102

Eine wichtige Aufgabe des BSI ist es, der Bundesverwaltung, Unternehmen und Privatanwendern Empfehlungen für den sicheren Einsatz von IT-Systemen an die Hand zu geben, beispielsweise in Form von Technischen Richtlinien (TR). Das Ziel der Technischen Richtlinien ist es, geeignete IT-Sicherheits-Empfehlungen zu verbreiten. Sie richten sich daher vor allem an alle, die mit dem Aufbau oder der Absicherung von IT-Systemen zu tun haben. Sie ergänzen die technischen Prüfvorschriften des BSI und liefern Kriterien und Methoden für Konformitätsprüfungen sowohl hinsichtlich der Interoperabilität von IT-Sicherheitskomponenten als auch der umgesetzten IT-Sicherheitsanforderungen. Die Empfehlungen unterstützen beispielsweise Unternehmen dabei, Webserver sicher zu betreiben, oder Behörden der Bundesverwaltung, ein Datenaustauschverfahren so zu implementieren, dass die Daten nach dem aktuellen Stand der kryptografischen Technik geschützt übertragen werden können.

Zu diesem Zweck erstellt und pflegt das BSI unter anderem seit vielen Jahren die Technischen Richtlinien der Serie BSI-TR-02102. Die Serie besteht zurzeit aus vier Dokumenten, die allgemeine kryptografische Empfehlungen zu Schlüssellängen und kryptografischen Algorithmen (Teil 1) sowie konkrete Empfehlungen für den Einsatz der kryptografischen Protokolle TLS, IKE / IPsec und SSH (Teile 2 bis 4) enthalten.

Die Technische Richtlinie BSI-TR-02102-2 (TLS) ist die Basis für den TLS-Mindeststandard, der diese Technische Richtlinie für die Bundesverwaltung verbindlich macht. Alle Technischen Richtlinien werden turnusmäßig einmal pro Jahr und gegebenenfalls zusätzlich aus aktuellem Anlass aktualisiert.

Seit November 2016 sind alle vier Technischen Richtlinien auch in englischer Sprache auf der BSI-Webseite verfügbar. Eine der wichtigsten Neuerungen in den 2017er-Versionen ist die Ankündigung, dass das BSI das Sicherheitsniveau ab dem Jahr 2023 von 100 auf 120 Bit anheben wird.

ECC-Seitenkanalleitfaden

Im Rahmen der Common-Criteria-Zertifizierung (CC-Zertifizierung) unterstützt das BSI Hersteller, Evaluierer und Zertifizierer durch Herausgabe von Anwendungshinweisen und Interpretationen im Schema (den sogenannten AIS). Die AIS 46 „Informationen zur Evaluierung von kryptografischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren“ beinhaltet unter anderem einen Leitfaden mit Mindestanforderungen zur Seitenkanalanalyse von Implementierungen Elliptischer-Kurven-Kryptografie (ECC). Dieser enthält Hinweise zur seitenkanalresistenten Repräsentation von Kurven, Kurvenpunkten und zur Umsetzung der Arithmetik. Weiterhin wird auf seitenkanalresistente Aspekte verbreiteter Protokolle wie ECDH, ECDSA, ECIES und PACE eingegangen.

Dieser ursprünglich aus dem Jahre 2011 stammende Leitfaden wurde 2016 vom BSI in Zusammenarbeit mit der Wissenschaft, Herstellern, CC-Prüfstellen und CC-Zertifizierungsstellen unter Berücksichtigung neuerer Angriffsmethoden aktualisiert und wird auch in den nächsten Jahren weiterhin kontinuierlich aktualisiert werden.

3 Gesamtbewertung und Fazit

3 Gesamtbewertung und Fazit

Einfallstore für Cyber-Angriffe

Im Berichtszeitraum Juli 2016 bis Juni 2017 ist die Gefährdungslage weiterhin auf hohem Niveau angespannt. Die bekannten Einfallstore für Cyber-Angriffe bleiben unverändert kritisch bestehen:

- Die am häufigsten eingesetzten Soft- und teilweise auch Hardwareprodukte weisen Qualitätsmängel auf, denn sie enthalten Schwachstellen, die es Angreifern erlauben, Informationen abfließen zu lassen oder die Kontrolle über die Systeme zu erlangen (Kap. 1.4.1).

- Detektierte Sicherheitslücken werden zu langsam und unvollständig gemeldet, Hersteller stellen Updates verspätet zur Verfügung und Anwender setzen entsprechende Empfehlungen und Updates nicht unmittelbar und nur unvollständig um (Kap. 1.4.1).

- Organisiert aufgebaute und betriebene Botnetze sind nach wie vor eine erhebliche Bedrohung der IT-Sicherheit (Kap. 1.4.4). Sie werden genutzt, um Schadsoftware oder Spam-E-Mails massenhaft zu verteilen oder um die Verfügbarkeit von Diensten zu sabotieren. Aktuell sind Botnetze aus IoT-Geräten wie das Mirai-Botnetz (Kap. 1.4.4. und Seite 39) zu einer großen Bedrohung geworden.

- Die sprunghaft angestiegenen Fälle von Ransomware zeigen, dass vor allem Cyber-Kriminelle hier eine lukrative Möglichkeit gefunden haben, in großem Umfang Geld zu erpressen (Kap. 1.4.3). Anonyme Zahlungsmethoden wie beispielsweise Bitcoin erleichtern diese Vorgehensweise. Indem die Daten des Opfers und die digitale Identität bis zur Bezahlung blockiert oder ohne Bezahlung gelöscht werden, hat sich hier eine Form der „digitalen Geiselnahme“ entwickelt.

- Der „Faktor Mensch“ spielt immer dann eine entscheidende Rolle, wenn Angriffe über Social Engineering ausgeübt werden (Kap. 1.4.6). Gezielte Phishing-Angriffe, bei denen einzelne Unternehmen oder Mitarbeiter adressiert werden sind häufiger als in den vergangenen Jahren zu beobachten. Besonders viel Aufwand investieren Angreifer beim CEO-Betrug, einer Variante des Social Engineerings, bei der hohe Schadenssummen erreicht werden (Kap. 1.4.7).

Digitalisierung als Herausforderung

Gleichzeitig lässt sich im Berichtszeitraum erneut beobachten, dass die mit der rasanten Technologieentwicklung einhergehende Digitalisierung aller Lebensbereiche Staat, Wirtschaft und Gesellschaft vor große Herausforderungen stellt. Die zunehmende Digitalisierung und Vernetzung führen auf der einen Seite zu Effizienzsteigerungen durch vereinfachte Prozesse, zu mehr Transparenz durch verbesserte Kommunikationsmöglichkeiten und zu mehr Komfort im Alltag, da Komponenten und Systeme untereinander kommunikativ verknüpft werden. Auf der anderen Seite steigt das Bedrohungspotenzial deutlich an, da sich die Anzahl der Angriffspunkte erhöht, die Kommunikationsinfrastrukturen immer komplexer werden und die zu verarbeitenden Datenmengen sich vervielfachen. Die Wahrscheinlichkeit erfolgreicher Angriffe auf digitalisierte Infrastrukturen wird damit größer. Für Cyber-Angreifer bieten sich fast täglich neue Angriffsflächen und weitreichende Möglichkeiten, um Informationen und Know-how auszuspähen, Geschäfts- und Verwaltungsprozesse zu sabotieren oder sich auf Kosten Dritter kriminell zu bereichern:

- 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, weil deren IT-Sicherheit weder bei der Herstellung noch bei der Kaufentscheidung des Kunden eine ausreichende Rolle spielt (Kap. 1.3).

- Ausfälle oder Störungen industrieller Steuerungsanlagen – besonders im Bereich der Kritischen Infrastrukturen – haben in der Regel gravierende physische Auswirkungen, beispielsweise in Form von Stromausfällen oder Störungen von Logistik- oder Produktionsprozessen. Die Veränderungen der eingesetzten Technologien und der Infrastrukturen im Zuge von Industrie 4.0 nehmen weiterhin zu (Kap. 1.4.11).

- Ein relativ neues Phänomen ist die Einflussnahme auf politische Prozesse durch Cyber-Angriffe, in der Regel durch professionelle und vermutlich staatlich gelenkte Angreifergruppen. Dabei wird versucht, zum Beispiel durch Angriffe auf private E-Mail-Accounts, an Informationen zu gelangen, um diese zu einem späteren Zeitpunkt – etwa im Wahlkampf – zu veröffentlichen und so unter Umständen Einfluss auf die Reputation eines Kandidaten oder auf die Meinungsbildung der Wähler zu nehmen. Verschiedene Vorfälle im In- und Ausland haben gezeigt, dass neben demokratischen Institutionen zunehmend auch demokratische Verfahren wie Wahlen in den Fokus von Cyber-Angreifern geraten.

IT- und Cyber-Sicherheit als Voraussetzung

Die Informationssicherheit in den staatlichen Institutionen und Behörden, in Unternehmen und Organisationen, aber auch bei Privatanwendern muss durch die allumfassende Digitalisierung immer wieder neu und in hohem Tempo an die dynamischen Rahmenbedingungen angepasst werden.

Um im Kampf gegen Cyber-Angreifer jeglicher Herkunft nicht ins Hintertreffen zu geraten, muss die Sicherheit der eingesetzten Systeme von vornherein gewährleistet sein, ohne dass die Möglichkeiten der Digitalisierung dadurch nennenswert eingeschränkt werden. Damit jedoch die Paradigmen „Security-by-design“ und „Security-by-default“ umgesetzt werden, müssen IT- und Cyber-Sicherheit Chefsache sein. Nur wenn von Anfang an ein angemessenes Sicherheitsniveau gewährleistet wird, werden die großen Digitalisierungsprojekte zu einem Gewinn, von dem alle profitieren. Denn Cyber-Sicherheit ist keine Innovationsbremse, sondern ein Innovationsgarant.

Abwehr und Prävention aus einer Hand

Das BSI als die nationale Cyber-Sicherheitsbehörde gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft mit einem ausgeprägten kooperativen Ansatz und zahlreichen Partnern. Als Kompetenzzentrum für IT-Sicherheit in Deutschland, als Multiplikator und zentrale koordinierende Stelle sorgt es für eine ganzheitliche und konsistente Umsetzung seiner vielfältigen Aufgaben, wie zum Beispiel aus der Cyber-Sicherheitsstrategie, dem IT-Sicherheitsgesetz und dem NIS-Richtlinien-Umsetzungsgesetz. Dabei kommt dem BSI die enge Zusammenarbeit von Experten aus verschiedenen Spezialgebieten der Informationssicherheit in der Wahrnehmung seiner vielfältigen und unterschiedlichen Aufgabe zugute. Nur so konnte das BSI auf gravierende IT-Sicherheitsvorfälle wie WannaCry oder Petya mit kurzen Reaktionszeiten und hoher fachlicher Kompetenz reagieren. So können Erkenntnisse aus der operativen Cyber-Abwehr oder aus den permanenten Hard- und Softwareanalysen sowie aus der Grundlagenarbeit der Kryptografie ohne Zeitverzug in die Prävention, in die Standardisierung und Zertifizierung eingebracht werden. Das BSI gestaltet auf diese Weise Informationssicherheit aus einer Hand.

Dies gilt auch für die Zusammenarbeit von Staat und Wirtschaft bei der Gestaltung von mehr Cyber-Sicherheit, insbesondere im KRITIS-Bereich. Das IT-Sicherheitsgesetz hat dafür einen rechtsverbindlichen Rahmen geschaffen, der konsequent umgesetzt wird. Mit dem am 30. Juni 2017 in Kraft getretenen Gesetz zur Umsetzung der EU-Richtlinie zur Netzwerk- und Informationssicherheit werden die Aufsichts- und Durchsetzungsbefugnisse des BSI gegenüber den KRITIS-Betreibern noch weiter gestärkt und ergänzen so den seit zehn Jahren verfolgten kooperativen Ansatz des BSI. Die im Berichtszeitraum gemeldeten Vorfälle aus Kritischen Infrastrukturen (Kapitel 2.3.5) verdeutlichen die Notwendigkeit der neuen Meldepflicht.

Vernetzung der IT-Sicherheitsakteure

An zahlreichen Schnittstellen arbeitet das BSI als zentrale Kompetenzstelle mit externen Partnern zusammen, um IT-Sicherheit auf hohem Niveau zu gewährleisten. Ein derart ganzheitlicher Ansatz mit gebündelten Kompetenzen für Bund und Länder ermöglicht, die Chancen der Digitalisierung voll zu entfalten. Durch den Ausbau eines Verbindungswesens – in 2017 zunächst als Pilotprojekt begonnen – wird das BSI diesen Aspekt weiter in die Fläche tragen.

Parallel dazu wird die bilaterale und europäische Zusammenarbeit ausgebaut, in der Prävention, der Detektion und der Entwicklung einheitlicher Standards und Vorgehensweisen.

Schlussfolgerungen für die deutsche IT-Sicherheitslandschaft

Viele der bekannt gewordenen IT-Sicherheitsvorfälle in den Jahren 2016 und 2017 haben gezeigt, dass sich für eine erfolgreiche IT-Sicherheit alle Akteure ihrer Verantwortung bewusst sein müssen. WannaCry hat auch deshalb so großen Schaden erwirken können, weil Systeme nicht hinreichend gepatcht wurden. Das BSI setzt sich dafür ein, dass in diesem Bereich mehr Transparenz für Verbraucher und stärkere Verpflichtungen für Unternehmen geschaffen werden.

Um noch besser in der Lage zu sein, die Verfassungsorgane, die Bundesbehörden und die Betreiber Kritischer Infrastrukturen auf deren Ersuchen vor Ort schnell, flexibel und adressatengerecht zu unterstützen, wird das BSI den Aufbau von „Mobile Incident Response Teams“ (MIRTs) auch künftig weiter voran treiben – wie in der Umsetzung der Cyber-Sicherheitsstrategie und des NIS-Richtlinien-Umsetzungsgesetzes vorgesehen.

Um angesichts der skizzierten rasanten technologischen Entwicklung seine Aufgaben und Befugnisse nicht nur in der Reaktion, sondern auch in der Prävention und Detektion aktiv wahrnehmen zu können und „vor die Lage zu kommen“, muss die Prognosefähigkeit des BSI ausgebaut werden. Es muss einerseits Treiber im Bereich Kryptografie bleiben, und es muss zum anderen befähigt werden, im Sinne eines „Technologieradars“ alle für die IT-Sicherheit relevanten technologischen Trends durch das Screening neu aufkommender und das Monitoring

priorisierter Technologien frühzeitig zu erkennen und als „Thought Leader“ zu bewerten, um benötigtes Technologie-Know-how schnell zu entwickeln und zielgenau einsetzen zu können.

Der neue BSI-Lagebericht macht deutlich, dass Informationssicherheit die Voraussetzung für eine erfolgreiche Digitalisierung ist. Das BSI als die nationale Cyber-Sicherheitsbehörde nimmt sich auch weiterhin dieser Herausforderung an. Der Ansatz, Informationen zum Schutz der IT so weit wie möglich zu teilen („need to share“) ist dabei unser Grundverständnis. So kann durch gemeinsame gesellschaftliche Anstrengung das Niveau der Informationssicherheit in der Digitalisierung auch in Zukunft kontinuierlich erhöht 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 auf ein Netzwerk verschafft und diesen in der Folge auf weitere Systeme ausweitet. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten auf Seiten der Angreifer aus und sind in der Regel schwierig zu detektieren.

Angriffsvector
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.

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.

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.

Blinding
Blinding ist ein Verfahren, das meist zum Schutz gegen Seitenkanal-Angriffe in der Kryptografie verwendet wird. Blinding kann dabei helfen, den geheimen Schlüssel (oder Teile davon) während einer Verschlüsselungsoperation so zu verschleiern, dass keine Informationen über ihn abfließen können. Meist wird eine zufällige Zahl auf den geheimen Wert addiert, der die Krypto-Operation nicht beeinflusst, aber den echten Schlüssel schützt.

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.

CVE-Datenbank
Ziel der Common Vulnerabilities and Exposures (CVE) Datenbank ist Einführung einer einheitlichen Namenskonvention für Sicherheitslücken und andere Schwachstellen in Computersystemen. Jede gemeldete Schachstelle erhält darin eine laufende Nummer, um eine eindeutige Identifizierung der Schwachstelle zu gewährleisten. Die Datenbank wird von der Nonprofit-Organisation MITRE verwaltet und hat sich als Register öffentlicher Sicherheitslücken etabliert.

DANE
DNS-based Authentication of Named Entities (DANE) ist ein Protokoll, das es erlaubte 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.

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.

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

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

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

Nonce
Nonce steht für engl. number used only once und steht in der Kryptografie für eine Einmalzahl, das heißt eine Zahl, die in einem Kontext nur einmal benutzt wird. Häufig werden Nonces mit einem Zufallszahlengenerator erzeugt, dann zum Beispiel 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.

OpenSSL
OpenSSL ist eine freie Softwarebibliothek, die Verschlüsselungsprotokolle wie Transport Layer Security (TLS) und andere implementiert.

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

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

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

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

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

Root Zone
Die Root Zone ist die oberste Zone des hierarchisch aufgebauten Domain Name Systems (DNS):
. Root Zone
.de Top-Level Domain “de”
.bund.de Domain der Bundesverwaltung

RPKI
Die Ressource Public Key Infrastructure ist eine Zertifikatsinfrastruktur, die speziell der Absicherung des Internetroutings dient.

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

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

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

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.

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

Impressum

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik (BSI)

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

E-Mail
bsi@bsi.bund.de

Telefon
+49 (0) 22899 9582-0

Telefax
+49 (0) 22899 9582-5400

Stand
August 2017

Druck
Druck- und Verlagshaus Zarbock, Frankfurt am Main

Gestaltung
Fink & Fuchs AG

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

Bildnachweis
alle Bilder: iStock.com/jm1366

Grafiken
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Artikelnummer
BSI-LB17/506

www.bsi.bund.de