Bundesamt
für Sicherheit in der
Informationstechnik

Die Lage der IT-Sicherheit in Deutschland 2016

Vorwort

Der Lagebericht des BSI 2016 beschreibt verlässlich und fundiert die aktuellen Entwicklungen in der IT-Sicherheit. Er skizziert die Gefährdungslage in Deutschland, bewertet Schwachstellen in IT-Systemen und illustriert Angriffsmittel und -methoden. Der Lagebericht gibt schließlich Auskunft über Strukturen und Rahmenbedingungen der IT-Sicherheit in Deutschland.

Der Berichtszeitraum war geprägt von einer weiter ansteigenden Professionalisierung der Angreifer und ihrer Angriffsmethoden. Die Zahl bekannter Schadprogrammvarianten ist 2016 weiter gestiegen und lag im August 2016 bei mehr als 560 Millionen. Gleichzeitig verlieren klassische bisherige Abwehrmaßnahmen weiter an Wirksamkeit. Dies betrifft alle Nutzer: Private, Unternehmen, Staat und Verwaltung.

Vor allem die Bedrohung durch sogenannte „Ransomware“ hat sich in Deutschland seit Ende 2015 deutlich verschärft. Wenn informationstechnische Systeme von Krankenhäusern, Unternehmen oder der Verwaltung lahmgelegt werden, um „Lösegeld“ zu erpressen, ist das eine ernst zu nehmende Entwicklung, die ein entschiedenes Handeln erfordert.

Das gilt auch für die Angriffe auf IT-Systeme des Deutschen Bundestages oder auf die im Bundestag vertretenen Parteien. Indem sie gezielt Einrichtungen der demokratischen Willensbildung ins Visier nehmen, stehen solche Cyber-Angriffe für eine neue Dimension an Bedrohung. Haben sie Erfolg, sehe ich langfristig Gefahren für die freiheitliche Gesellschaft und unsere Demokratie.

Natürlich ist IT immer dynamisch, die Anforderungen an ihre Sicherheit wachsen ebenso schnell. Doch so rasant die technischen Entwicklungen auch sein mögen: IT-Sicherheit muss immer von Anfang an mitgedacht werden.

Für die Bundesregierung bildet die neue Cyber-Sicherheitsstrategie den strategischen Rahmen, wenn es um mehr Sicherheit im Cyber-Raum geht. Wir wollen ein sicheres und selbstbestimmtes Handeln in einer digitalisierten Welt ermöglichen. Nur so können wir die enormen Chancen, die die Digitalisierung bietet, uneingeschränkt nutzen. Dafür müssen Staat und Wirtschaft besser zusammenarbeiten und Deutschland auch weiterhin eine aktive Rolle in der europäischen und internationalen Cyber-Sicherheitspolitik einnehmen.

Das Berichtsjahr verdeutlicht: Schwachstellen in Soft- und Hardware können von Angreifern leicht ausgenutzt werden und werden es auch. Um dies zu verhindern, braucht es mehr Prävention, Detektion und Reaktion. Alle Akteure müssen hierauf die nötige Aufmerksamkeit verwenden und ihren Beitrag zu mehr digitaler Sicherheit leisten. Der vorliegende Lagebericht des BSI unterlegt diese Notwendigkeit eindrucksvoll.

Dr. Thomas de Maizière, MdB
Bundesminister des Innern

Vorwort

Die Digitalisierung ist zu einer wichtigen Grundlage für technologischen Fortschritt sowie wirtschaftlichen und gesellschaftlichen Wohlstand in Deutschland geworden. Als die nationale Cyber-Sicherheitsbehörde gestaltet das Bundesamt für Sicherheit in der Informationstechnik die Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft.

In den 25 Jahren seines Bestehens hat das BSI sich von der Verschlüsselung von Informationen über den Schutz des Regierungsnetzes zur nationalen Cyber-Sicherheitsbehörde entwickelt, die die Informationssicherheit in der Digitalisierung gestaltet. Das BSI bietet Lösungen an, mit denen IT-Anwender der aktuellen, kritischen IT-Gefährdungslage besser begegnen und Risiken minimieren können, und fördert Möglichkeiten zum Informations- und Erfahrungsaustausch. Dazu gehören die etablierten Kooperationsplattformen Allianz für Cyber-Sicherheit mit derzeit rund 2.000 Teilnehmern oder der UP KRITIS, welcher seit dem offiziellen Start im Jahr 2007 einen wesentlichen Beitrag zur verlässlichen Bereitstellung kritischer Dienstleistungen für die Menschen in Deutschland leistet.

Die Komplexität der IT sowie die zunehmende Digitalisierung und Vernetzung bieten Cyber-Angreifern weitreichende Möglichkeiten, Informationen auszuspähen, Geschäfts- und Verwaltungsprozesse zu sabotieren oder sich anderweitig auf Kosten Dritter kriminell zu bereichern. Im Fokus der Angriffe stehen dabei Unternehmen und Kritische Infrastrukturen ebenso wie Verwaltung, Forschungseinrichtungen und Bürger.

Wir überantworten mehr und mehr sensible Prozesse vernetzten IT-Systemen – bis hin zu autonomen Fahrzeugen und lebenswichtigen Einrichtungen der öffentlichen Daseinsvorsorge. Eine Digitalisierung ohne ausreichende Cyber-Sicherheit wird nicht erfolgreich sein.

Das BSI arbeitet mit verschiedensten Akteuren aus Staat, Wirtschaft und Gesellschaft gemeinsam daran, den bestehenden Risiken wirksame und umsetzbare Sicherheitsmaßnahmen entgegenzusetzen. Im vorliegenden Bericht zur Lage der IT-Sicherheit in Deutschland finden Sie daher neben den wesentlichen Gefährdungen auch Lösungsansätze, mit denen das BSI einen Beitrag zur Förderung der Cyber-Sicherheit leistet.

Das BSI erfüllt die in uns gesetzten Erwartungen durch unabhängige und vom Stand der Technik geleitete Wahrnehmung unserer Aufgaben. Gleichzeitig können staatliche Unterstützungsleistungen aber nicht allein für die Sicherheit in der Digitalisierung sorgen – hier sind alle Akteure in Staat, Wirtschaft und Gesellschaft aufgefordert, gemeinsam Verantwortung zu übernehmen und die notwendigen Maßnahmen zu treffen. Das BSI gestaltet diesen kooperativen Prozess.

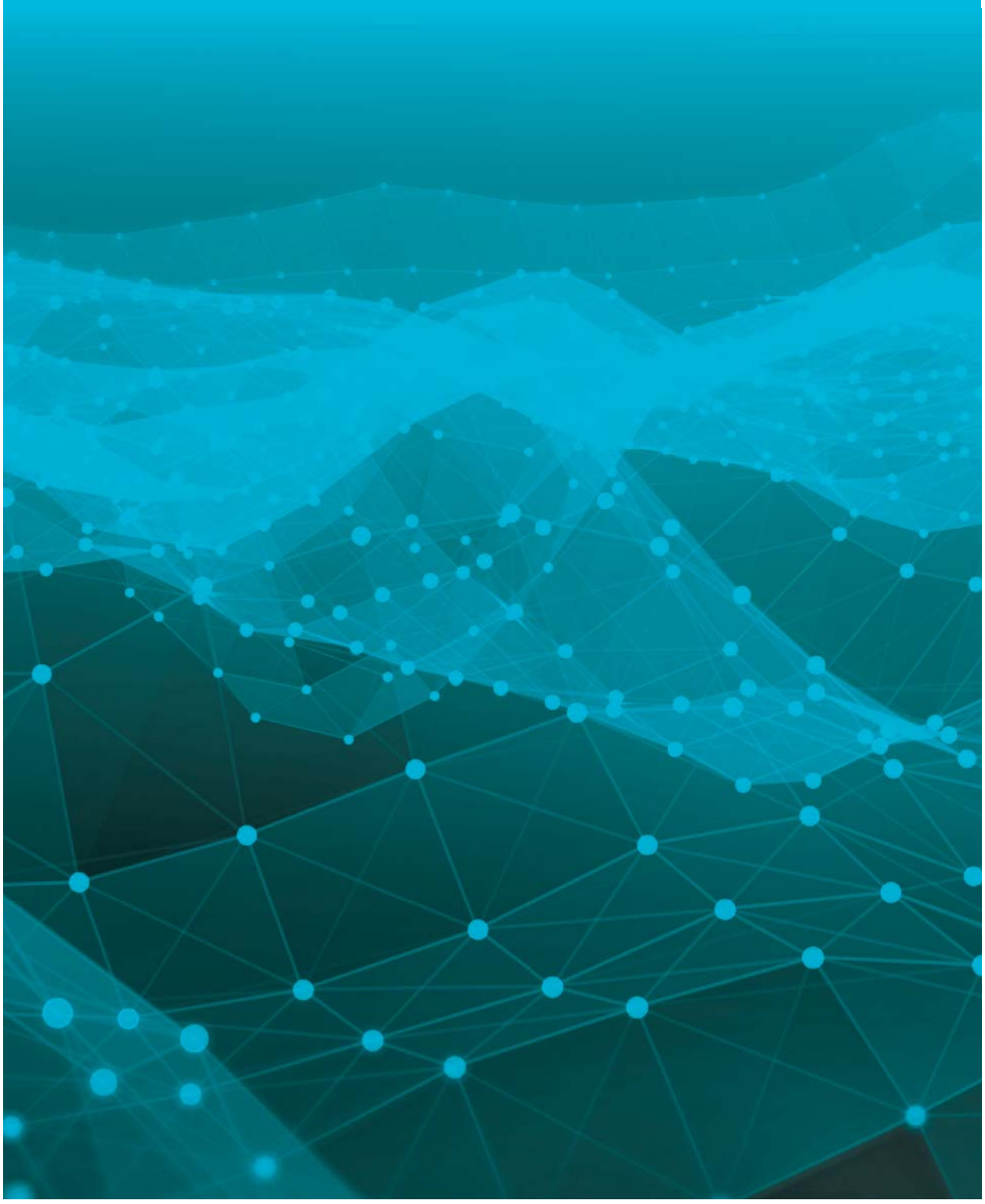
Mit dem vorliegenden Lagebericht 2016 informiert das BSI über die aktuellen Gefahren für die IT-Sicherheit in Deutschland sowie die Gegenmaßnahmen. Im Einzelnen finden Sie in Kapitel 1 die Beschreibung der aktuellen Gefährdungslage. Kapitel 2 widmet sich der Gefährdungslage der Bundesverwaltung, Kapitel 3 legt den Schwerpunkt auf die Gefährdungslage Kritischer Infrastrukturen. Kapitel 4 zeigt anhand ausgewählter Kernthemen die Lösungsansätze und Angebote des BSI auf. Abschließend wird in Kapitel 5 nach einer Zusammenfassung der wesentlichen Ergebnisse aus dem Bericht ein Ausblick auf die künftigen Entwicklungen gegeben.

Ich wünsche Ihnen eine interessante Lektüre und freue mich auf Ihre Anmerkungen.

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

Inhaltsverzeichnis

1 Gefährdungslage



1 Gefährdungslage

Das folgende Kapitel beschreibt die Gefährdungslage in Deutschland, die durch Methoden und Möglichkeiten der Angreifer, aber auch durch bestimmte Rahmenbedingungen geprägt wird.

1.1 Ursachen und Rahmenbedingungen

1.1.1 Cloud Computing

Einleitung

Das BSI hat zur Einschätzung der Sicherheitslage im Bereich Cloud Computing im Zeitraum von September 2015 bis Februar 2016 verschiedene öffentliche Quellen ausgewertet, beispielsweise einschlägige Informationsportale oder Selbstauskünfte der Cloud-Anbieter. Die aufgenommenen Vorfälle wurden in das Cloud-Schichtenmodell der IETF (Internet Engineering Task Force) eingeordnet, nach Risiken wie Manipulation, Informationsabfluss, Diensteausfall oder Rechteausweitung klassifiziert und grob nach Schwere eingeteilt.

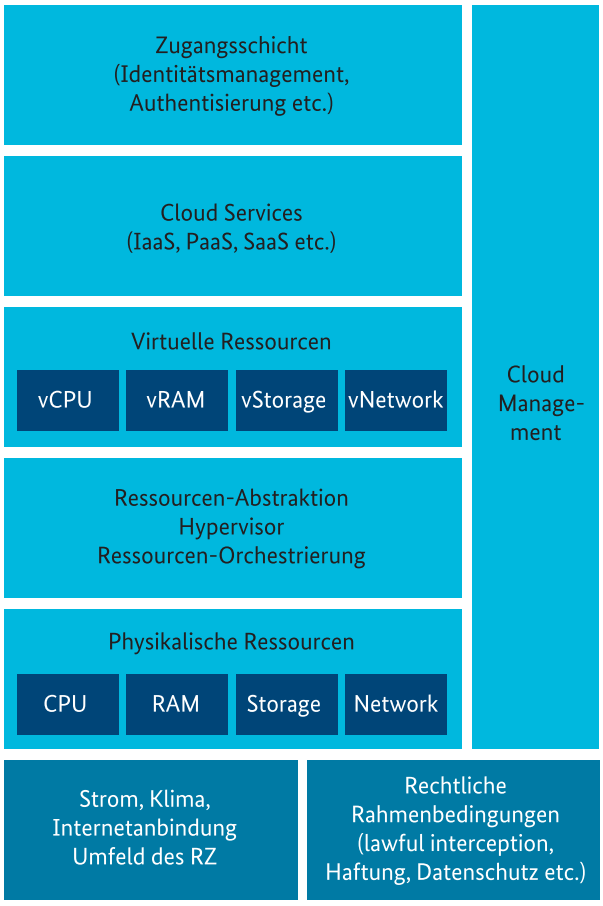


Abbildung 1: Cloud-Schichtenmodell der IETF

Lage

Im Untersuchungszeitraum wurden 404 Vorfälle aufgenommen, 98 Prozent davon betrafen die Verfügbarkeit von Cloud Services. Dieser hohe Anteil ist dadurch zu erklären, dass sich Selbstauskünfte der Cloud-Anbieter fast immer auf die Verfügbarkeit beziehen. Die Schlussfolgerung, dass nur sehr wenig Informationsabflüsse oder Manipulationen passieren, kann daraus nicht gezogen werden. Die Serviceausfälle lassen sich zu 78 Prozent (317 Vorfälle) direkt in der Serviceschicht der Cloud verorten. Ausfälle in dieser Schicht sind meist auf Fehler in der Software oder Probleme bei Updates zurückzuführen. Von den 317 Ausfällen in dieser Schicht sind 92 auf technisches, 13 auf menschliches Versagen und zwei auf vorsätzliche Handlungen zurückzuführen – zum Rest wurden keine Angaben gemacht. An zweiter Stelle der Ursache für Ausfälle liegt die virtuelle Ressourcenschicht mit 12 Prozent (46 Vorfälle). Ausfälle in dieser Schicht bedeuten, dass der Software des Dienstes nicht genügend virtualisierte Ressourcen (Rechenleistung, Arbeitsspeicher, Festplattenspeicher und Netzwerkdienste) zur Verfügung gestellt wurden. Jeweils sechs Fälle betrafen technisches und menschliches Versagen, bei 34 Fällen ist die Ursache nicht bekannt. Die restlichen 10 Prozent der Vorfälle zur Verfügbarkeit betrafen das Cloud Management und die physischen Ressourcen.

Der Großteil der Ausfälle (377) wurde innerhalb einer Stunde, weitere zwölf Ausfälle innerhalb von vier Stunden behoben. Bemerkenswert ist, dass 91 von 92 Ausfällen in der Cloud-Serviceschicht, die auf technisches Versagen zurückgehen, binnen einer Stunde behoben waren.

Bewertung

Aus den Zahlen geht hervor, dass die hier untersuchten Cloud-Anbieter im Wesentlichen eine Verfügbarkeit von ca. 99,9 Prozent (bis zu 9 Stunden Ausfall pro Jahr) erreichen. Cloud-Anbieter scheinen durch Cyber-Angriffe nur unwesentlich in der Verfügbarkeit ihres Dienstes eingeschränkt zu sein, da sie über ausreichend starke Gegenmaßnahmen verfügen. Angriffe auf die Verfügbarkeit eines Cloud-Dienstes sind zudem vermutlich nicht so lukrativ wie das Stehlen von Kundendaten. Diese sind bei Cloud-Anbietern stark kumuliert und deshalb ein attraktives Ziel für Datendiebe, sodass sich auch komplexe Angriffe mit hohem Aufwand für Angreifer lohnen könnten. Um dieser Gefahr zu begegnen und Schaden abzuwenden, sind gemeinsame Anstrengungen bei Prävention und Detektion von Cyber-Angriffen sowie bei der Reaktion der Cloud-Anbieter darauf nötig.

Begrüßenswert ist, dass große Cloud-Anbieter wie Amazon Web Services, Google, Microsoft und SAP Informationsplattformen bereitstellen, auf denen detailliert über den aktuellen Sicherheitsstatus verschiedener Teile der Cloud berichtet wird. Dies ist ein Schritt hin zu mehr Transparenz für Kunden und dient als Quelle für Lageeinschätzungen zur IT-Sicherheit.

1.1.2 Software-Schwachstellen

Einleitung

Softwareprodukte sind zunehmend komplexe Gebilde, bei deren Entwicklung Fehler unterlaufen können, die dazu führen, dass die Software Schwachstellen beinhaltet. Für die IT-Sicherheitslage relevant sind dabei insbesondere gängige Softwareprodukte, die weltweit von Millionen von Anwendern genutzt werden. Aufgrund ihrer weiten Verbreitung kann die Ausnutzung von Sicherheitslücken in diesen Produkten potenziell schwerwiegende und flächendeckende IT-Sicherheitsvorfälle nach sich ziehen.

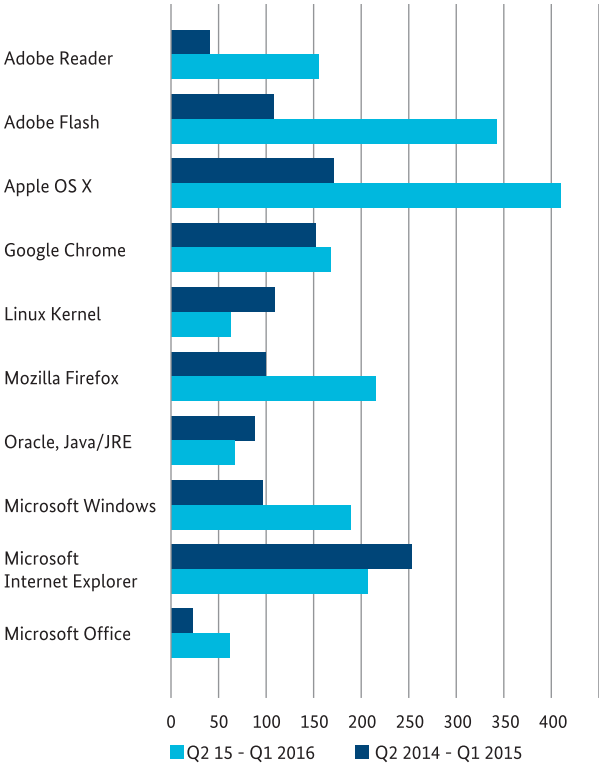


Abbildung 2: Schwachstellenaufkommen von Q2/2014-Q1/2015 zu Q2/2015-Q1/2016

Lage

- Die Anzahl der Schwachstellen der Hälfte der betrachteten Softwareprodukte bewegt sich im Vergleich zum Vorjahreszeitraum in einem eher vernachlässigbaren Schwankungsbereich (Abb. 2). Von den verbleibenden Softwareprodukten waren Adobe Reader und Flash Player sowie Apple OS X im vergangenen Jahr verstärkt im Fokus von Sicherheitsforschern, die insbesondere durch automatisiertes Ausprobieren (Fuzzing) eine große Anzahl gefundener Schwachstellen an die Hersteller gemeldet hatten. Durch eine strikte Veröffentlichungsrichtlinie der Sicherheitsforscher werden die Hersteller unter Druck gesetzt, die Schwachstellen schnell zu schließen und dieses auch öffentlich durch einen CVE-Eintrag zu dokumentieren.

- Für die zehn verbreitetsten in der BSI-Schwachstellenampel erfassten Softwareprodukte (Abb. 3) wurden im Jahr 2016 bis Ende September 717 kritische Schwachstellen bekannt. Eine große Anzahl gefundener Schwachstellen allein ist dabei zunächst nicht unbedingt problematisch. Kritisch zu bewerten ist jedoch, wenn durch Fuzzing mit nur geringem Aufwand auch potenziell kritische Schwachstellen gefunden werden, da auch Angreifer diese Techniken zum Finden von Schwachstellen aktiv einsetzen. Durch vergleichsweise leicht ausnutzbare Schwachstellen und eine hohe Verbreitung ist daher besonders Adobe Flash in den Fokus von Angreifern gerückt. So wurden einige Schwachstellen zuerst bzw. auch von Angreifern gefunden und ausgenutzt. Microsoft Windows und Office stehen seit jeher im Fokus von Sicherheitsforschern. Durch die komplexen Dateiformate können durch Fuzzing insbesondere auch immer wieder viele Schwachstellen in Office gefunden werden.

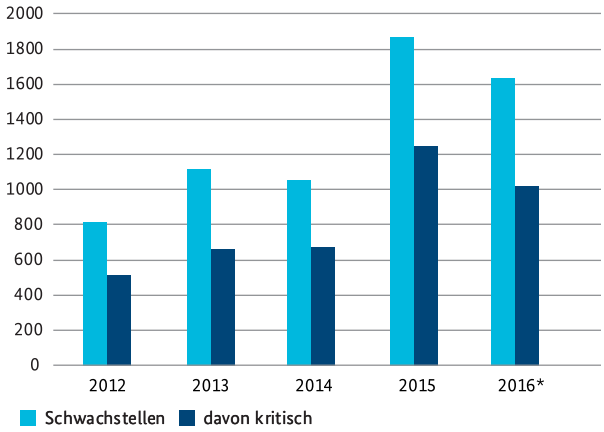


Abbildung 3: Anzahl aller Schwachstellen der zehn verbreitetsten in der BSI-Schwachstellenampel erfassten Softwareprodukte
* Zahlen für 2016 sind aus den bis Ende September 2016 entdeckten Schwachstellen hochgerechnet

Die CVE-Liste und ihre Aussagekraft

Die einzige weltweit anerkannte Quelle für die Veröffentlichung neuer Schwachstellen ist die Datenbank „Common Vulnerabilities and Exposures“ (CVE) der MITRE Corporation. In der CVE-Liste werden Schwachstellen nach einem standardisierten Verfahren katalogisiert. Derzeit enthält die Liste mehr als 76.000 Einträge. In der IT-Sicherheitsbranche werden CVE-Nummern in Verbindung mit Schwachstellen häufig referenziert; oft als einzige Quelle. Aussagen über die Sicherheit eines Softwareproduktes werden teilweise mit der Häufigkeit der Eintragungen in der Liste begründet. Trotz der allgemeinen Anerkennung der Liste, der häufigen Referenzierung und des Informationsgehalts stellen sich folgende Fragen:

» **Was bedeuten die CVE-Einträge für ein bestimmtes Softwareprodukt?**
Jeder Hersteller entscheidet selbst, ob eine Schwachstelle in die Liste eingetragen wird oder nicht. Es kann auch vorkommen, dass in einem Eintrag der CVE-Liste mehrere unabhängige Schwachstellen zusammengefasst werden. Die Zahl an Einträgen zu einem Produkt hat somit wenig Aussagekraft, zudem kann der CVE-Eintrag unter Umständen nicht einer spezifischen Schwachstelle zugeordnet werden.

» **Bekommt jede gefundene Schwachstelle auch einen CVE-Eintrag?**
Einige Hersteller erhalten einen CVE-Nummernpool, über den sie eigene Einträge erstellen können. Die übrigen Hersteller sowie unabhängige Sicherheitsforscher melden gefundene Schwachstellen an MITRE, die diese dann nach Prüfung ggf. in einen Listeneintrag überführt. Einige Hersteller melden hingegen keinerlei Schwachstellen.

» **Wie hoch ist die Betroffenheit?**
Der Schweregrad sowie der Grad der Ausnutzbarkeit sind in der NVD-Datenbank (National Vulnerability Database) aufgeführt, die weiterführende Informationen zu den CVE-Einträgen enthält. Es gibt keine Aussage über die Verbreitung der betroffenen Software. Eine Sicherheitslücke in einem speziellen Gerätetreiber hat zum Beispiel eine andere Betroffenheit als eine Kernel-Schwachstelle, die sämtliche Versionen eines Betriebssystems betrifft.

Die CVE-Datenbank allein sollte somit nicht zur Bewertung der Sicherheit eines Softwareproduktes herangezogen werden. Die Aussagekraft ist begrenzt durch:

» unterschiedliches Melden von Schwachstellen in Softwareprodukten
» fehlende Bewertung des Schweregrads der Schwachstelle (dazu liefert nur der verlinkte NVD-Eintrag mehr Informationen)
» fehlende Aussage über die Verbreitung der Software und damit über die Betroffenheit.

Neben der CVE-Datenbank wertet das BSI daher auch die zugehörigen NVD-Einträge aus, um eine Zuordnung der dort aufgeführten Schwachstellen zu Softwareprodukten zu ermöglichen. Die oben beschriebenen Einschränkungen der Aussagekraft bezogen auf die CVE-Datenbank spiegeln sich daher auch in der Bewertung von Schwachstellen in den Softwareprodukten wider: Allein aufgrund der Anzahl geschlossener Schwachstellen in einem Softwareprodukt kann keine Aussage über dessen Sicherheit getroffen werden. Selbst bei öffentlich bekannt gewordenen Schwachstellen besteht zwar grundsätzlich eine Gefährdung für den Nutzer, jedoch ist auch hier der einfache Rückschluss auf die Unsicherheit der Software nicht ohne Weiteres möglich. Bei häufigem Bekanntwerden von Schwachstellen ist allerdings der Schluss in diese Richtung naheliegend. Eine Analyse der nicht geschlossenen Schwachstellen in Softwareprodukten ist auf der Basis der CVE- und NVD-Datenbank nicht möglich, da die Einträge nahezu ausschließlich erst nach der Veröffentlichung eines Updates erstellt werden. Da es hierfür kein allgemein akzeptiertes Verfahren gibt, beschränken sich die meisten Analysen zu Schwachstellen darauf, anhand der geschlossenen Schwachstellen Rückschlüsse auf die Produktsicherheit einer Software zu ziehen.

Bewertung

Schwachstellen in Softwareprodukten stellen nach wie vor eine relevante Bedrohung für die Sicherheit von IT-Systemen dar. Um ein Eindringen von Schadsoftware in die eigenen Systeme zu verhindern und Angreifern keine Möglichkeit zur Ausnutzung dieser Schwachstellen zu bieten, ist es daher wichtig, stets die aktuellsten Software- oder Sicherheitsupdates zu installieren.

Die saisonalen Veränderungen der Anzahl der gefundenen Schwachstellen spiegeln wider, welche Softwareprodukte momentan mehrheitlich im Fokus von Sicherheitsforschern sind, sei es aufgrund großer Verbreitung, schlechter Softwarequalität oder einer Kombination von beidem. Erst das über mehrere Jahre nachhaltige Absinken der Anzahl und/oder Schwere der gefundenen Schwachstellen eines Softwareprodukts bei gleichbleibender oder höherer Marktrelevanz lässt Rückschlüsse auf Verbesserungen der Softwarequalität zu.

Einige Hersteller schließen Schwachstellen in ihren Produkten nach wie vor nur bei anhaltendem öffentlichem Druck. Die verschiedenen Initiativen der Softwareindustrie zur Qualitätsverbesserung stecken noch in den Kinderschuhen und werden u.a. aus Kostengründen nicht konsequent umgesetzt. Signifikante globale Veränderungen der Softwarequalität sind momentan nicht erkennbar, da punktuelle Verbesserungen durch Verschlechterungen an anderer Stelle im Allgemeinen kompensiert werden. Eine signifikante Verbesserung würde sich bereits ergeben, wenn alle Hersteller zumindest für neue Produkte den Stand der Technik aus der Sicherheitsforschung direkt umsetzen und für etablierte Produkte schrittweise nachrüsten würden. Der Nachholbedarf ist an dieser Stelle immens.

1.1.3 Hardware: Schwachstellen in Sicherheitselementen

Einleitung

Das Kerckhoffs'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 ein Brechen des Verfahrens die Lösung eines als schwer angenommenen mathematischen Problems erfordert. Jedoch ist die sichere Speicherung und unbeobachtbare Verarbeitung des Schlüssels selbst ein Problem. Hierzu kommen oft Hardware-Sicherheitselemente zum Einsatz, welche sich zwangsweise für die Geheimhaltung der gespeicherten Schlüssel des eigentlich umstrittenen Prinzips der Sicherheit durch Obskurität bedienen – zum Beispiel Verschleiern der ausgeführten Operationen per Software, durch kryptografisches Blinding, durch physikalisch implementierte Maßnahmen wie eine ausgefeilte Sensorik, die die Betriebsbedingungen ständig überprüft und Angriffe erkennt, oder auch durch die bei heutigen Chips vorherrschende geringe Strukturgröße selbst. All diese Maßnahmen können Ziel eines Angriffs sein.

Lage

Neben fehlerhafter Software können auch Schwachstellen in Hardware potenzielle Einfallstore für Angriffe sein. Hardware-Manipulationen können zum Beispiel durch Modifikationen durch zusätzliche Baugruppen, Änderungen bestehender Schaltungen, Manipulationen auf Chipebene oder Softwaremodifikationen auf Firmware-Ebene vorgenommen werden. In Bezug zu den genannten Angriffsmöglichkeiten ist die Gefährdungslage gegenüber dem Vorjahr unverändert.

Um die Digitalisierung abzusichern, kommen Sicherheitselemente in verschiedensten Formen und Ausprägungen zum Einsatz: Smartcards in Form einer Kredit- oder EC-Karte, Signaturkarten, Personalausweis oder Reisepass, FIDO-Token (Token zur Zweifaktor-Authentifizierung nach Maßgabe der Fast IDentity Online Alliance) oder im Bereich von Pay-TV Trusted-Platform-Module auf dem PC, in Verbindung mit einem Trusted Execution Environment auf dem Mobiltelefon, oder zukünftig im Bereich von Industrie 4.0, dem Internet der Dinge und in intelligenten Verkehrsinfrastrukturen.

Angriffe auf Sicherheitselemente lassen sich in zwei Klassen unterteilen:

1. **Invasive** Angriffe, bei denen physische Manipulationen am Chip vorgenommen werden, beispielsweise Fehlerinduktionsangriffe durch Laserbeschuss bis hin zur Modifikation der Schaltkreise.

2. **Nicht invasive Angriffe**, bei denen ein Seitenkanal ausgenutzt wird, zum Beispiel die elektromagnetische Abstrahlung des Chips während der Schlüsselverarbeitung.

Zunächst müssen Schwachstellen identifiziert werden, die dann in einem zweiten Schritt für die praktische Durchführung von Angriffen ausgenutzt werden. Gerade bei hardwarebasierten Sicherheitselementen ist die Identifikationsphase oft aufwendig. Bis vor wenigen Jahren waren

aufgrund der Strukturgrößen der Halbleiter und der geringen Verfügbarkeit der notwendigen Laborausstattung beide Angriffsformen mit sehr hohem finanziellem Aufwand verbunden. Die Preise für Equipment für invasive und nicht invasive Angriffe – Focused Ion Beam, Rasterelektronen- oder Atomic-Force-Mikroskope und Oszilloskope – sind jedoch derart gefallen, dass vermehrt mit neuen Angriffstechniken gerechnet werden muss.

Bewertung

Auch wenn der notwendige Aufwand für das erfolgreiche Brechen eines zertifizierten Hardware-Sicherheitselements hoch ist, sind derartige Angriffe oft attraktiv für Angreifer. Einerseits sind die hohen Kosten für spezialisierte Analysewerkzeuge eine einmalige Investition, andererseits ist das Ziel der Angriffe oft lukrativ. So lassen sich beispielsweise durch den Verkauf von kopierten Pay-TV-Karten oder gefälschten Ausweisdokumenten hohe Gewinne erzielen. Durch die steigende Verwendung von Sicherheitselementen im Zuge der fortschreitenden Digitalisierung ergeben sich somit ständig neue Angriffsziele, die mit großem finanziellem Nutzen für die Angreifer einhergehen. Ist ein konkreter Angriffspfad auf ein Sicherheitselement einmal identifiziert, ist das Ausnutzen der gefundenen Schwachstelle oft relativ einfach möglich, zum Beispiel durch Template-Attacken. Zwar könnte die praktische Ausnutzbarkeit von Schwachstellen der Hardware zum Teil durch zusätzliche Maßnahmen auf der Ebene der Firmware des Sicherheitselements stark erschwert werden. Jedoch sind Softwareupdates, die im Bereich herkömmlicher Computersysteme verbreitet sind, bei Sicherheitselementen üblicherweise nicht vorgesehen. Schwachstellen in Sicherheitselementen stellen daher eine starke Bedrohung dar. Bei Geräten mit eingebetteten Sicherheitselementen ist ein Austausch nicht vorgesehen, sodass das gesamte Gerät ausgetauscht werden muss. Jedoch ist der Ad-hoc-Austausch einer Vielzahl von bereits in Verwendung befindlichen Chipkarten aus organisatorischen Gründen praktisch nicht durchführbar.

Serverausfall im Krankenhausrechenzentrum

Sachverhalt: Drei Kliniken in Deutschland, die IT-Services über ein zentrales Rechenzentrum beziehen, mussten infolge eines Serverausfalls ohne elektronische Dokumentation arbeiten.

Ursache: Der Ausfall einer Festplatte führte zu einem kompletten Serverausfall. Die eigentlich vorgesehene Redundanzlösung funktionierte nicht ordnungsgemäß.

Schadenswirkung: Die Störung dauerte ca. 19 Stunden. In dieser Zeit konnten keine Rechner der Verwaltung genutzt werden. In den Kliniken fiel unter anderem das System zur Dokumentation der Patientenversorgung aus. Die Dokumentation musste daher manuell durchgeführt und nach Beseitigung der Störung im System nachgetragen werden. Die Patientenversorgung war nicht gefährdet, da die Medizingeräte unabhängig im „Stand Alone"-Modus betrieben werden konnten.

Zielgruppen: Störungen dieser Art können grundsätzlich in jedem zentralisierten IT-Netzwerk auftreten. Wichtig ist es daher, dass sich die Betreiber darauf entsprechend vorbereiten, Redundanzmechanismen einrichten und diese auch testen.

1.1.4 Hardware: Schwachstelle Breitband-Router

Einleitung

In Deutschland gibt es derzeit rund 30 Millionen Breitbandanschlüsse. Der Netzabschluss dieser Anschlüsse erfolgt überwiegend durch Router, die häufig die einzige wesentliche Sicherheitskomponente zum Schutz des internen Netzes der Anwender bilden. Der Absicherung des Routers kommt daher eine herausragende Bedeutung zu. Wird der Router durch einen Angreifer manipuliert oder übernommen, kann dieser zum Beispiel Kommunikationsdaten des Anwenders ausspähen oder manipulieren, die Infrastruktur des Anwenders zum Teil eines Botnetzes werden lassen oder auf Kosten des Anwenders hochpreisige Gespräche führen.

Lage

Die Anzahl der bekannten kritischen Schwachstellen in Routern ist in den letzten Jahren gestiegen. Abbildung 4 zeigt zum einen die Entwicklung von kritischen Schwachstellen seit 2013. Demnach wurden in den Jahren 2013 und 2014 insgesamt acht kritische Schwachstellen in Routern gemeldet, 2015 bis Mitte 2016 hat sich diese Anzahl annähernd verdoppelt. Zum anderen verdeutlicht das Diagramm den Zeitraum von der Bekanntgabe der Schwachstelle bis zur Bereitstellung des Updates durch den Hersteller. Beispielsweise dauerte es 804 Tage, bis ein Update für die 4. kritische Schwachstelle bereitgestellt wurde. Andere Hersteller hingegen veröffentlichten mit der Bekanntgabe einer Schwachstelle das dazugehörige Update, sodass dieser Zeitraum 0 Tage beträgt. Tatsächlich dürfte auch hier die Schwachstelle einige Zeit für Angriffe offen gewesen sein.

Vor dem Hintergrund dieser Bedrohungslage sowie der besonderen Bedeutung eines Routers hat das BSI ein Testkonzept für Breitband-Router veröffentlicht, das sich vornehmlich an die Internet Service Provider und die Router-Hersteller richtet. Ziel ist es, die Sicherheit von Breitband-Routern messbar zu machen und ein einheitliches Sicherheitsniveau der Geräte zu erreichen. Das Testkonzept ermöglicht die Überprüfung relevanter Sicherheitseigenschaften von Routern. Dabei werden grundlegende sicherheitsrelevante Funktionen sowie die Unterstützung und Einhaltung etablierter Sicherheitsstandards betrachtet. Darüber hinaus behandelt das Testkonzept exemplarisch bekannte Sicherheitsrisiken und Angriffsszenarien. Das Testkonzept wurde in Zusammenarbeit mit den Internet Service Providern, Herstellern von Breitband-Routern und weiteren Interessierten entwickelt.

Bewertung

Mit der Abschaffung des Routerzwangs im August 2016 haben Internetnutzer mehr Möglichkeiten bei der Auswahl ihres Routers. Sie sollten diese Möglichkeiten nutzen, indem sie auch die Sicherheit zum wichtigen Entscheidungskriterium beim Kauf eines Routers machen. Die Implementierung der Sicherheitsfunktionen können die Hersteller mithilfe des im Testkonzept beschriebenen Standards umsetzen und den Nutzern darlegen.

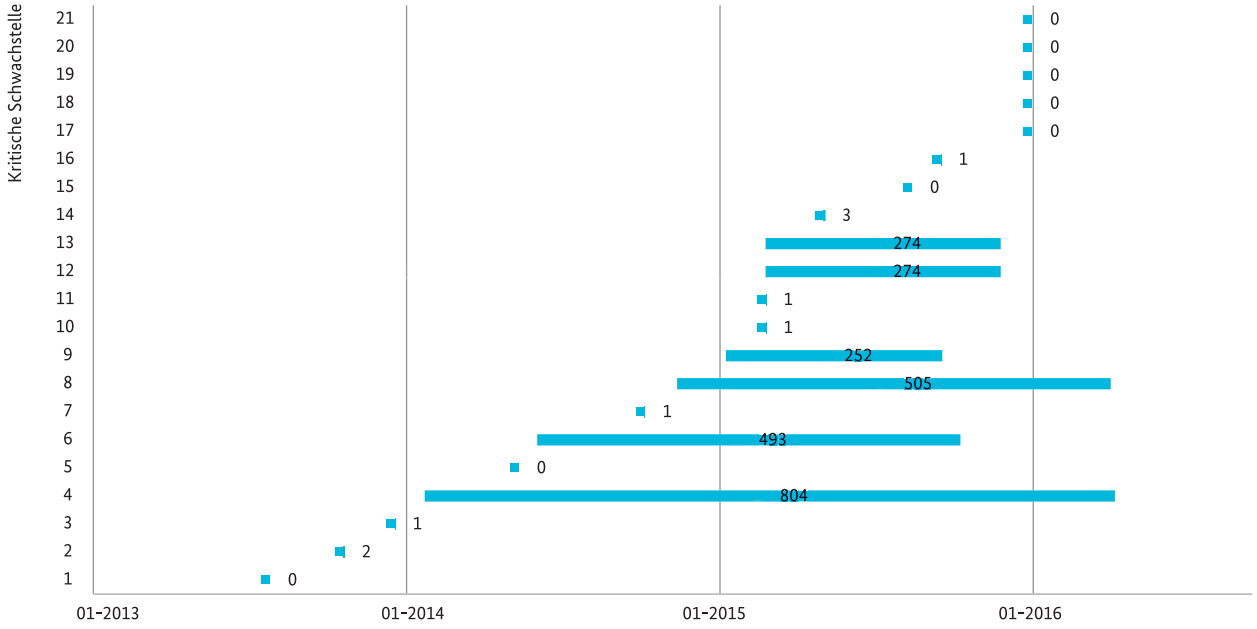


Abbildung 4: Kritische Router-Schwachstellen, Quelle: CVE Details, Stand: Juni 2016

Router-Besitzer sollten in regelmäßigen Abständen Sicherheitsupdates für ihre Geräte installieren oder die automatische Update-Funktion nutzen. Darüber hinaus muss der Zugriff auf die Weboberfläche und auf das WLAN des Routers jeweils mit einem individuellen komplexen Schlüssel abgesichert werden, um Angriffen vorzubeugen.

1.1.5 Kryptografie

Einleitung

Die von der Bundesregierung beschlossene „Digitale Agenda" ebenso wie die „Charta zur Stärkung vertrauenswürdiger Kommunikation" geben das Ziel aus, Deutschland zum „Verschlüsselungsstandort Nr. 1" zu machen, zum Schutz der Bürger, der Wirtschaft und der Verwaltung vor Ausspähung oder Manipulation ihrer Kommunikation. Auf dieses Ziel ist auch die Arbeit des BSI ausgerichtet. Kryptografie ist nach wie vor ein zentraler Baustein für die Wirksamkeit vieler IT-Sicherheitsmechanismen.

Lage

- Aktuelle kryptografische Mechanismen liefern grundsätzlich ausgezeichnete Sicherheitsgarantien. So können zum Beispiel zwei Parteien, die nur ihre lokalen Rechner zuverlässig kontrollieren und die kein Geheimnis miteinander teilen, 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 die für den Gegner verfügbare Rechenleistung in einem praktischen Rahmen weitgehend irrelevant.
- In diese Einschätzung fließen verschiedene Voraussetzungen ein, die erfüllt sein müssen, 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 auf dem Wege kompromittierender 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 hierbei keine exakte Übereinstimmung besteht zwischen angestrebten Sicherheitszielen und den Sicherheitsgarantien eines kryptografischen Protokolls, können Sicherheitslücken auftreten.
  - Der Gegner darf zwar über praktisch beliebig viel Rechenleistung verfügen, aber nicht über kryptoanalytische Fähigkeiten, die qualitativ über den Stand der öffentlichen Forschung weit hinausgehen.
- Im Bereich der Public-Key-Kryptografie gehen praktisch sämtliche Sicherheitsgarantien verloren, wenn der Gegner über einen skalierbaren universellen Quantencomputer verfügt.
- 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.

Bewertung

Bis auf wenige Ausnahmen können dem Stand des kryptografischen Wissens entsprechende Krypto-Algorithmen als sicher angesehen werden. Auch viele etwas ältere Verfahren bieten bei richtigem Einsatz noch ein hohes Maß an Sicherheit. Trotzdem versagen Krypto-Systeme auch heute noch gelegentlich in ihrer Sicherheitsfunktion.

Verschiedene Probleme können zu einem praktischen Versagen eines kryptografischen Systems führen: 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. Gerade Fehler in weitverbreiteten Implementierungen

Aktuelle Themen in der Kryptografie

Untersuchung kryptografischer Implementierungen
OpenSSL ist eine verbreitete kryptografische Open-Source-Bibliothek. Sie implementiert verschiedene kryptografische Funktionalitäten, in der Praxis ist die TLS-Implementierung am bedeutsamsten. Aufgrund der großen Bedeutung der Bibliothek hat das BSI eine Studie in Auftrag gegeben, um die Sicherheitseigenschaften von OpenSSL zu untersuchen. Hierbei wurde der Zufallsgenerator untersucht, eine Untersuchung auf Implementierungsschwachstellen durchgeführt sowie eine systematische Dokumentation der Bibliothek erstellt. Zudem wurden Hinweise erstellt, die eine Konfiguration entsprechend den Anforderungen der Technischen Richtlinie TR-02102 erleichtern sollen für Komponenten, die OpenSSL benutzen. Die Studie „Quellcode-basierte Untersuchung von kryptografisch relevanten Aspekten der OpenSSL-Bibliothek“ kann von der Webseite des BSI heruntergeladen werden.

Analyse des Linux-RNG
Grundvoraussetzung für die Gewährleistung von Informationssicherheit sind effektive und vertrauenswürdige Sicherheitsmechanismen auf technischer Ebene. Viele IT-Systeme setzen mittlerweile auf das Betriebssystem Linux, darunter neben PCs auch viele eingebettete Systeme wie Netzwerk-Router oder Load Balancer. Auf fast allen diesen Geräten spielt Kryptografie eine wichtige Rolle: Auf Desktop-PCs werden Schlüssel für die Verschlüsselungslösung GnuPG erzeugt, damit E-Mails verschlüsselt werden können; Load Balancer stellen TLS-gesicherte Verbindungen mit Webservern her, damit Daten verschlüsselt übertragen werden können. Für kryptografische Operationen wie diese werden sichere Schlüssel gebraucht, die ein Angreifer nicht vorhersagen und damit die Verschlüsselung brechen kann.
Basis für eine gute Verschlüsselung sind gute Zufallszahlen. Es muss also sichergestellt werden, dass der Zufallszahlengenerator (random number generator, RNG) von Linux auch wirklich zufällige und nicht vorhersagbare Daten liefert, damit die damit erzeugten kryptografischen Schlüssel sicher sind. Das BSI lässt derzeit über einen bestimmten Zeitraum hinweg den RNG für jede neu erscheinende Version von Linux untersuchen. Damit kann das BSI Sicherheitsaussagen über diesen RNG, aber insbesondere auch über kryptografische Systeme machen, die diesen RNG zur Erzeugung von Schlüsselmaterial verwenden. Ein Hauptaspekt der Untersuchung ist der Nachweis, dass der Linux-RNG konform zu einer vom BSI spezifizierten Funktionalitätsklasse ist. Wenn diese Konformität gegeben ist, erfüllt der Linux-RNG nachweislich bestimmte Eigenschaften bezüglich der Qualität der Zufallszahlen, des Entropiegehalts, der Sicherheit usw. Durch diesen Nachweis lässt sich zum einen die Vergleichbarkeit mit anderen RNGs herstellen, zum anderen kann diese Klassifizierung die Common-Criteria-Zertifizierung oder auch die Zulassung von Produkten erleichtern, wenn diese den Linux-RNG einsetzen. Der Untersuchungsbericht ist auf der BSI-Webseite verfügbar.

Technische Richtlinien der Serie 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 die Verbreitung von angemessenen IT-Sicherheitsstandards. Technische Richtlinien richten sich daher in der Regel 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 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 aus vier Dokumenten, die sich mit allgemeinen kryptografischen Empfehlungen wie Schlüssellängen oder kryptografischen Verfahren (Teil 1), mit Protokollen wie TLS und SSH und darauf bezogene konkrete Empfehlungen für den Einsatz dieser Protokolle (Teile 2 und 4) sowie Empfehlungen für IKEv2/IPsec (Teil 3) befassen. Die Technische Richtlinie BSI-TR-02102-2 (TLS) ist die Basis für den TLS-Mindeststandard, der diese Technische Richtlinie für die Bundesverwaltung verbindlich macht. Die Technischen Richtlinien werden mindestens einmal pro Jahr aktualisiert.

Sweet32
Sweet32 ist eine kryptografische Attacke, die die seit Langem bekannte Tatsache ausnutzt, dass jede Blockchiffre bei der Verschlüsselung sehr großer Mengen von teilweise bekanntem Klartext mit einem Schlüssel unsicher wird. Der Punkt, an dem die Unsicherheit einsetzt, hängt hier mit der Blockgröße der Chiffre und der gewählten Betriebsart zusammen. Sweet32 konzentriert sich auf die Anwendung der relevanten Beobachtungen auf (veraltete) Chiffren mit 64 Bit Blocklänge (z.B. Triple-DES, Blowfish) im CBC-Modus und insbesondere auf die Ausnutzung der entstehenden Schwächen gegen TLS-Verbindungen. Ähnlich wie bei anderen in jüngerer Vergangenheit diskutierten Angriffen gegen TLS (z.B. CRIME, BEAST) wird auch hier ein Man-in-the-Browser-Szenario eingesetzt. Das Opfer wird dabei von den Angreifern dazu gebracht, eine von ihnen kontrollierte Webseite aufzurufen, und diese bringt den Computer des Opfers dazu, immer wieder über den TLS-Kanal die gleiche Nachricht zu übermitteln. Nach einer Übertragung von etwa 232 Chiffratsblöcken gelingt dem Angreifer die Entschlüsselung eines Session Cookies.
Diese Angriffe sind kein Problem, wenn eine Blockchiffre mit einer Blocklänge von 128 Bit genutzt oder bei Verwendung einer Legacy-Chiffre mit 64 Bit Blocklänge ein Schlüsselwechsel rechtzeitig erzwungen wird (vergleiche hierzu auch BSI-TR-02102-1). Der Punkt, an dem die für Sweet32 bedeutsame Schwachstelle mit einiger Wahrscheinlichkeit relevant wird, lässt sich gut einschätzen, die Gegenmaßnahme eines rechtzeitigen Schlüsselwechsels ist also zuverlässig.

können die Sicherheit vieler Systeme gefährden. Die Tatsache, dass viele Systeme keine oder nur selten Softwareupdates erhalten oder nicht in Sicherheitsanalysen berücksichtigt werden, sorgt 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.

Eine klassische Kryptoanalyse ist bei modernen Verschlüsselungsverfahren kaum erfolgreich. Sie bleibt für die Praxis dennoch wichtig, weil die Aufdeckung theoretischer Schwächen in Kryptosystemen ein „Frühwarnsystem" vor der Möglichkeit des Auftretens praktischer Schwierigkeiten bietet. Zudem haben kryptoanalytische Fortschritte das Potenzial, die Sicherheitsgarantien eines Verfahrens flächendeckend zu entwerten. Es ist insgesamt jedoch als unwahrscheinlich anzusehen, dass kryptografische Systeme, 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.

Die Entwicklung universeller Quantencomputer würde praktisch alle heute eingesetzten Public-Key-Verfahren unsicher machen, da die zugrunde liegenden mathematischen Probleme (Faktorisierung und Diskreter Logarithmus) durch Shors Algorithmus auf einem Quantencomputer in polynomieller Zeit gelöst werden könnten. Ein Quantencomputer, der zur Ausführung von Shors Algorithmus für aktuell eingesetzte Schlüssellängen und Public-Key-Verfahren geeignet wäre, existiert nicht. Es sind jedoch in den letzten Jahren deutliche Fortschritte zumindest im Bereich der relevanten Grundlagenforschung erkennbar.

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. Das sind 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 sein, diese Aktivitäten aktiv zu begleiten. Ergänzend werden eigene Projekte zum Thema Quantencomputer und Post-Quanten-Kryptografie im BSI durchgeführt.

Neben quantencomputerresistenten kryptografischen Verfahren werden auch Verfahren aus dem Bereich der Quantenkryptografie als mögliche Lösung zur Etablierung sicherer Datenverbindungen in einer Welt mit Quantencomputern genannt. Hierbei handelt es sich um technische Systeme, die mittels physikalischer Effekte ein ähnliches Sicherheitsproblem lösen wie Public-Key-Kryptoverfahren 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.

Die Nutzung kryptografischer Verfahren für kriminelle Zwecke, etwa zur Verabredung gesetzwidriger Handlungen, lässt sich technisch kaum unterbinden. Eine Prävention mancher 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.

1.1.6 Mobilkommunikation

Einleitung

Kommunikation, Navigation, Fitnesstraining, soziale Netzwerke und Unterhaltung sind nur einige der Anwendungsmöglichkeiten moderner Smartphones und Tablets. Die immer intensivere App-Nutzung sorgt dafür, dass auch die Sensibilität der Daten zunimmt, die auf den Geräten verarbeitet werden. Adressbücher, Standort- und Zugangsdaten, E-Mails und andere Kommunikationsdaten sowie auf dem Smartphone ausgeführte sensible Anwendungen wie Home Banking machen die Mobilgeräte zu einem nach wie vor lohnenden Angriffsziel für Kriminelle.

Lage

- Trotz einiger Initiativen der Industrie, die Bereitstellung von Software-Aktualisierungen zur Beseitigung von Sicherheitslücken zu beschleunigen, kann von einer schnellen und flächendeckenden Bereitstellung von Sicherheitspatches in der Mobilkommunikation nach wie vor keine Rede sein. Aufgrund der großen Vielfalt von Gerätetypen ist eine flächendeckende Versorgung mit Sicherheitsupdates kein einfaches Vorhaben. Ob es gelingen wird, hängt nicht zuletzt davon ab, ob sich der Umgang der Anbieter mit Sicherheitspatches beim Verbraucher als Qualitätsmerkmal etablieren kann.

- 2015/2016 konnten einzelne Verbesserungen im Einsatz von Verschlüsselungstechnologien verzeichnet werden. So hat beispielsweise der populäre Whatsapp-Messenger eigenen Angaben zufolge eine Ende-zu-Ende-Verschlüsselung der Chat-Inhalte eingeführt. Diese punktuellen Verbesserungen beeinflussen die Gesamtsituation aber nur gering: Der Großteil der auf mobilen Geräten anfallenden persönlichen und sensiblen Informationen wird nicht oder nur unzureichend verschlüsselt.

- Die App-Stores der großen Anbieter wie Google, Apple und Microsoft bieten weltweit eine Vielzahl unterschiedlicher Apps an. Bei der Auswahl spielen Sicherheit und Datenschutz für den Anwender jedoch meist eine untergeordnete Rolle. Der Wettbewerb findet vielmehr über die „User Experience“ statt, über die Kombination von Nützlichkeit und Bequemlichkeit sowie über die Kosten einer App.

- Mobilgeräte können sich automatisch mit öffentlichen Hotspots verbinden. Diese sind oftmals offen, sodass Daten unverschlüsselt übertragen und von unbefugten Dritten mitgelesen werden können.

- Betreiber von Mobilfunknetzwerken, App-Anbieter, aber auch Cyber-Kriminelle 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 in bestimmten Fällen eine Ortung von Mobilfunkgeräten durch Dritte auch ohne Kontrolle über das Endgerät 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. In bestimmten Fällen sind auch 3G- und 4G-Telefonate abhörbar, beispielsweise wenn der Angreifer zunächst veranlasst, dass diese auf 2G-Standard umgeschaltet werden.

Bewertung

Die Gefährdungslage im Bereich der Mobilkommunikation hat sich im Vergleich zu 2015 nur wenig verändert. Punktuelle Verbesserungen im Bereich der Verschlüsselung sind zu verzeichnen, dennoch ist das Gefahrenpotenzial im Bereich der Mobilkommunikation aufgrund der zuvor beschriebenen Faktoren sowie der hohen Zahl an verfügbaren und teils schadhaften Apps nach wie vor hoch. Am Beispiel der Mobilkommunikation wird deutlich, dass der sorglose Umgang mit hochkomplexen Technologien seinen Preis hat. Auch die Auswirkungen unterschiedlicher Geschäftsmodelle der Anbieter spiegeln sich in der Informationssicherheit wider. Die Betreiber der App-Stores, aber auch die Anwender sind gefordert, mehr Augenmerk auf die Sicherheit zu legen. Während die Betreiber sicherstellen müssen, dass möglichst keine schadhaften Apps in den App-Stores angeboten werden, sollten sich die Nutzer sorgsam überlegen, welche App sie tatsächlich benötigen und welche Rechte man diesen Apps einräumt.

1.1.7 Standardsetzung

Einleitung

Die Digitalisierung kann ihr Potenzial nur entfalten, wenn alle notwendigen Bauteile aufeinander abgestimmt sind und zuverlässig funktionieren. Standards definieren alle relevanten Parameter für das Zusammenwirken unterschiedlicher IT-Komponenten, angefangen mit der Form und Größe von Steckern bis hin zur elektrischen Feldstärke oder Programmierschnittstellen. Dabei erfüllen Standards nicht nur ihren Zweck zur Sicherstellung der Interoperabilität, sondern sie legen auch Qualitätsanforderungen für IT-Produkte fest. So wird Informationstechnik im massenhaften Gebrauch hinsichtlich ihrer Sicherheitseigenschaften maßgeblich durch nationale und internationale Standardisierung gestaltet. Das BSI hat die Möglichkeit, direkt und verbindlich über Technische Richtlinien oder Prüfanforderungen nach den international anerkannten Common-Criteria (CC)-Standards zu etablieren, sofern dies durch deutsches bzw. europäisches Recht vorgeschrieben ist. Beispiele hierfür sind unter anderem intelligente Messsysteme, die elektronische Gesundheitskarte und der Personalausweis.

Lage

- Ob ein Standard international erfolgreich ist, hängt im Wesentlichen davon ab, ob die Hersteller ihre Produkte nach diesem Standard ausrichten und anbieten. Den größten Einfluss haben hier die jeweiligen Marktführer. Durch ihre Marktstellung sind die IT-Branchenführer oftmals nicht auf die

offiziellen Normungsgremien für die Standardsetzung angewiesen, sondern können De-facto-Standards setzen und ändern. Diese technologisch und wirtschaftlich treibenden IT-Unternehmen finden sich kaum noch in Deutschland oder Europa, sondern überwiegend in den USA oder Asien. Deutschlands Einfluss auf die IT-Standards ist daher bis auf einzelne Bereiche wie Smartcard-Anwendungen oder durch die internationale Spitzenstellung bei hochwertigen Prüfverfahren meist nur gering. Mangels wirtschaftlicher Interessen ist die Beteiligung der deutschen Industrie in IT-Standardisierungsgremien – anders als in anderen Branchen – daher verhältnismäßig schwach.

- Die vor allem im US-amerikanischen und asiatischen Raum angesiedelten IT-Hersteller und verschieden ausgeprägte Sicherheitspolitiken einzelner Staaten führen zu entgegengesetzten Interessenslagen bei den IT-Sicherheitsstandards: Während das BSI das Ziel verfolgt, kritische Komponenten möglichst genau auf ihre IT-Sicherheitseigenschaften bzw. mögliche Schwachstellen hin überprüfen zu können, werden derartige „High-Assurance-Prüfstandards“ im internationalen Umfeld eher zurückgedrängt. So wurde bereits 2014 das internationale Anerkennungsabkommen CCRA faktisch auf nur noch niedrige Prüftiefen abgesenkt – mit der Folge, dass die daran angelehnten ISO-Standards oder das europäische Anerkennungsabkommen SOGIS ebenfalls unter Druck geraten, sich auf niedrige Prüftiefen zu beschränken oder vereinheitlichte, fest definierte Testmethodiken statt offener Schwachstellenanalysen zu nutzen. Das BSI setzt sich daher international dafür ein, dass auch zukünftig hohe Prüfstandards für sensible Infrastrukturbereiche genutzt werden können.

Bewertung

Das BSI muss auch zukünftig in der Lage bleiben, IT-Sicherheitszertifikate mit hoher Prüftiefe für die Vermarktung von Produkten oder für die Erfüllung von spezialgesetzlichen Regulierungen herauszugeben. Dazu muss die hohe Anerkennungsstufe im SOGIS-Abkommen innerhalb von Europa erhalten bleiben. Die geringe Beteiligung der deutschen Industrie an der IT-Sicherheitsstandardisierung sollte in den relevanten Bereichen durch ein verstärktes öffentliches Engagement, etwa durch die Mitwirkung von Behörden, durch Mandate an Normungsorganen oder beauftragte Sachverständige ausgeglichen werden. Für kritische Bereiche werden verstärkt Empfehlungen für die Auswahl und die Anwendung von geeigneten Standards durch das BSI bereitgestellt, etwa durch die Veröffentlichung von BSI-Mindeststandards oder durch die Mitwirkung bei den Branchenstandards für KRITIS-Unternehmen nach dem IT-Sicherheitsgesetz.

1.1.8 Internet-Infrastruktur

Die Internet-Infrastruktur ist eine über Jahre gewachsene Struktur, die in vielen Bereichen sehr robust aufgebaut, gleichzeitig aber in vielen Teilen auch sehr fragil ist.

Robustes Internet

Ein robuster Dienst im Internet ist das Domain Name System (DNS). Über DNS erfolgt die Übersetzung von Namen in IP-Adressen – etwa von „*www.bsi.bund.de*“ in 77.87.229.76. Das DNS ist hierarchisch aufgebaut und in Zonen unterteilt, eine Namensauflösung erfolgt in der Regel in mehreren Schritten. Die Namensauflösung ist ein zentraler Dienst im Internet, für den es keine Alternative gibt. Viele andere Internetdienste sind auf eine funktionierende Namensauflösung angewiesen und verlassen sich auf Verfügbarkeit und Integrität des Dienstes. Die Betreiber großer Zonen – wie beispielsweise der root- oder der „.de“-Zone – sind sich dessen bewusst und sorgen in der Regel für die Ausfallsicherheit ihrer Systeme. Wie gut dies funktioniert, hat sich im November 2015 gezeigt, als es einen großen DDoS-Angriff auf die Nameserver der root-Zone gab. Während des Angriffs kam es zu ungewöhnlich großen Lasten – einige Instanzen haben mehr als das Hundertfache der sonst üblichen Anzahl an Anfragen erhalten. Auch wenn es durch den Angriff vereinzelt zu Verzögerungen und Timeouts gekommen ist, so waren die meisten Regionen und Nutzer von dem Vorfall nicht betroffen. Das DNS als Gesamtsystem hat weiterhin funktioniert.

Der Grund, warum auch ein solch großer Angriff aufgefangen werden konnte, ist eine massive Überprovisionierung. Zwar gibt es nur eine root-Zone, die jedoch von 13 Root-Nameservern bedient wird. Die meisten dieser Server haben wiederum mehrere Instanzen an verschiedenen Orten auf der Welt, die unter derselben IP-Adresse erreichbar sind. Dieses Verfahren namens Anycast sorgt dafür, dass die Anfrage an den nächstgelegenen Server weitergeleitet wird.

Fragiles Internet

Der Vorläufer des heutigen Internets war vergleichsweise überschaubar. Es gab nur wenige Akteure, die alle ein gemeinschaftliches Ziel verfolgten: den möglichst verlässlichen Austausch von Daten. Vertraulichkeit und Integrität der Kommunikation haben damals keine Rolle gespielt und wurden bei der Entwicklung von Protokollen nicht berücksichtigt. Inzwischen ist das Internet ein weltumspannendes Netz mit Milliarden Nutzern, die Protokolle von damals sind – von kleinen Änderungen abgesehen – jedoch nach wie vor im Einsatz. Inzwischen gibt es einen Bedarf an Sicherheit und man versucht, die alten Protokolle aufzurüsten oder zu ersetzen. Einige Beispiele:

- Es ist möglich, ganze Blöcke von IP-Adressen im Internet zu kapern. Dadurch können Kommunikationsinhalte zu unberechtigten Empfängern gelangen. Eine Gegenmaßnahme ist die Verwendung der Route Origin Authorisations (ROA) aus dem Rahmenwerk der Ressource Public Key Infrastructure (RPKI). Diese ermöglichen die Überprüfung, ob derjenige, der vorgibt, unter einer IP-Adresse erreichbar zu sein, auch dazu berechtigt ist.

- DNS ist zwar gegen Angriffe auf seine Verfügbarkeit gut geschützt, die im DNS gespeicherten Daten können jedoch gefälscht werden. Somit ist ein Missbrauch zum Beispiel zu Phishing-Zwecken möglich. Abhilfe schafft die Verwendung der sogenannten Domain Name System Security Extensions (DNSSEC). Mit der Sicherheitserweiterung DNSSEC lassen sich DNS-Einträge signieren, also kryptografisch absichern. Somit wird die Integrität dieser Einträge überprüfbar.

- Ist eine Domäne wie beispielsweise „bund.de“ mit DNSSEC signiert, so lassen sich weitere Einträge zur Verbesserung der Sicherheit im DNS hinterlegen. Diese werden häufig unter dem Schlagwort DANE (DNS-based Authentication of Named Entities) zusammengefasst. Beispiele für solche Einträge sind Zertifikate (TLSA) für kryptografisch geschützte Webseiten und Mail-Server oder PGP-Schlüssel (OPENPGPKEY).

Viele deutsche Betreiber von Internet-Infrastrukturen engagieren sich bei der Umsetzung dieser Maßnahmen und tragen aktiv zur Verbesserung der Sicherheit bei. So ist beispielsweise gut ein Drittel des Adressraums mittels RPKI gesichert. Damit steht Deutschland in der übergeordneten Region, für die die europäische Registrierungs- und Vergabestelle für IP-Adressen (RIPE NCC) zuständig ist, gut da. In der gesamten RIPE-Region sind etwa 12 Prozent des Adressraums mittels RPKI abgesichert. Die Absicherung des Adressraums mittels RPKI ist jedoch nur der erste Schritt. Die Validierung vor der Weiterleitung ist der zweite Schritt. Der De-CIX, einer der größten Internetknotenpunkte der Welt, plant, das Ergebnis einer solchen Validierung für andere einfach zugänglich zu machen.

Mit Unterstützung des BSI informieren die meisten deutschen Internet-Provider ihre Kunden, wenn sie davon Kenntnis erlangen, dass deren IT-Systeme mit Schadprogrammen infiziert oder andere Sicherheitsprobleme aufgetreten sind. So konnte beispielsweise die Anzahl von Servern verringert werden, die sich leicht für DDoS-Angriffe missbrauchen lassen.

Das BSI in seiner Zuständigkeit für den Schutz der Regierungsnetze hat alle verfügbaren Sicherheitsmaßnahmen getroffen: Für den Informationsverbund Berlin-Bonn wurde RPKI eingerichtet, die Domain „bund.de“ wurde DNSSEC-signiert und dort ein DANE Record hinterlegt. Darüber hinaus treibt das BSI die Verbreitung dieser Sicherheitsmechanismen voran. Um etwa die Einrichtung von RPKI zu erleichtern, hat das BSI eine entsprechende Anleitung verfasst und einen RPKI-Workshop organisiert. DNSSEC und DANE sind zudem in die Technische Richtlinie Sicherer E-Mail-Transport eingeflossen.

1.2 Angriffsmethoden und -mittel

1.2.1 Schadsoftware

Einleitung

Als Schadsoftware, Schadprogramm oder Malware werden Computerprogramme bezeichnet, die unerwünschte oder schädliche Funktionen auf einem infizierten Computer ausführen. Aktuelle Schadprogramme bestehen meist aus mehreren Komponenten, die unterschiedliche Funktionen haben, darunter auch die Möglichkeit, nach der Erstinfektion eines Systems weitere Module mit anderen Funktionen nachzuladen.

Lage

- Täglich werden ca. 380.000 neue Schadprogrammvarianten gesichtet. Allein bis August 2016 waren insgesamt mehr als 560 Millionen verschiedene Schadprogrammvarianten bekannt.

- Zu den häufigsten Infektionswegen eines Systems mit Schadprogrammen gehören E-Mail-Anhänge sowie die vom Anwender unbemerkte Infektion beim Besuch von Webseiten, sogenannte Drive-by Downloads. Auch Links auf Schadprogramme spielen weiterhin eine gewichtige Rolle. Quelle der Links auf Schadprogramme sind immer öfter Werbebanner, die von den Angreifern auf entsprechenden Plattformen eingestellt werden und die wie legitime Online-Werbung auch auf vertrauenswürdigen Webseiten angezeigt werden („Malvertising“).

- Ransomware verbreitete sich 2016 noch stärker als 2015. Anfang 2016 war insbesondere Deutschland von einer massiven Welle von Ransomware-Infektionen betroffen (vgl. hierzu Kapitel 1.2.2 Ransomware).

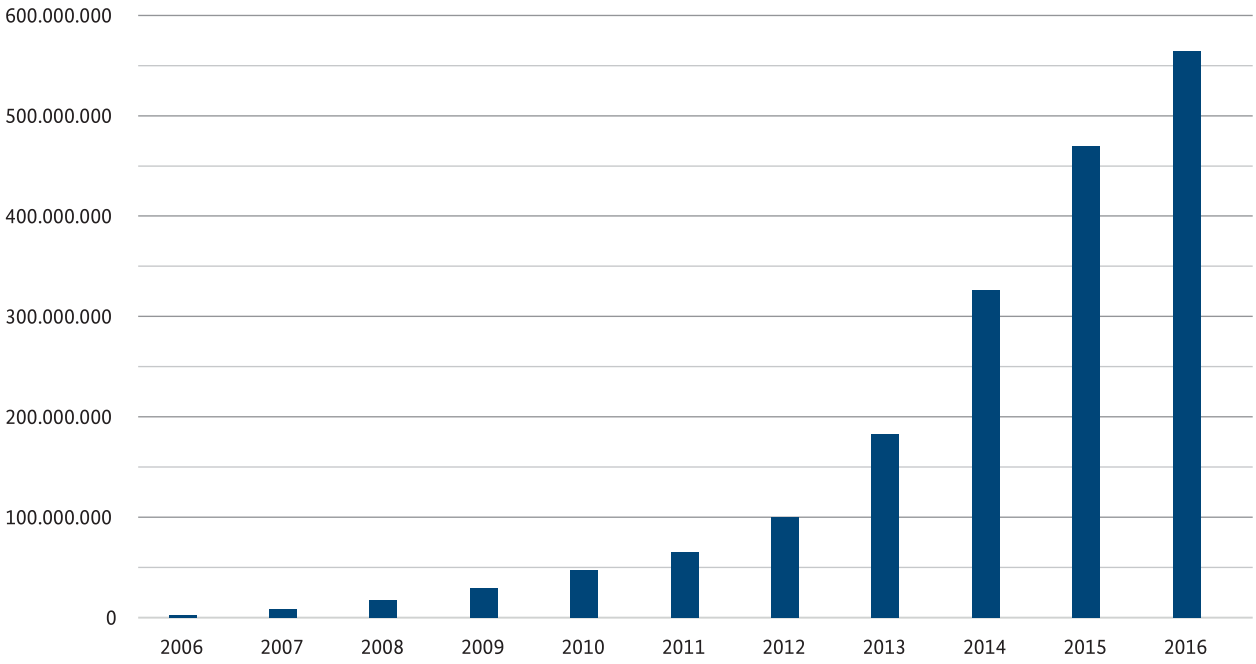


Abbildung 5: Bekannte Schadprogramme (2016 bis August)

- Klassische, signaturbasierte AV-Produkte bieten weiterhin nur einen Basisschutz, denn neue Varianten von Schadprogrammen werden schneller erzeugt, als sie analysiert werden können. Schadprogramm-Verteilwellen sind oft schon beendet, bevor AV-Signaturen erstellt und eingespielt werden konnten.

- Die Analyse von Schadprogrammen wird immer häufiger dadurch erschwert, dass Schadprogramme Funktionen mitbringen, mit denen sie Analyse-Tools und virtuelle Maschinen erkennen. Um die Entdeckung der Kommunikation eines Schadprogramms zu erschweren, werden weiterhin kompromittierte Webseiten Dritter als Steuerungsserver und als Verbreitungsweg missbraucht. Dabei wird eine gute Reputation einer schon bestehenden Webseite ausgenutzt, um potenzielle URL-Filter zu umgehen. Auch Makro-Viren nutzen inzwischen verschiedene Techniken, um zu erkennen, ob sie in einer Analyseumgebung ausgeführt werden.

- Abgesehen von den Techniken zur Erkennung von Analyseumgebungen bedienen sich Schadprogramme immer häufiger auch neuer Techniken, die bislang nur von deutlich geschickteren Angreifern bei gezielten Angriffen verwendet wurden. Es findet ein Technologietransfer aus dem Bereich der Advanced Persistent Threats (APT) hin zu den allgemeinen Schadprogrammen statt.

- Schadsoftware-Infektionen nach ungezielten Angriffen wurden sowohl in der Cyber-Sicherheitsumfrage 2015 der Allianz für Cyber-Sicherheit als auch in der Umfrage zur Betroffenheit durch Ransomware im Frühjahr 2016 von Unternehmen als häufigste Angriffsart benannt.

Bewertung

Wie schon 2015 sind Schadprogramme auch im aktuellen Berichtszeitraum eine der größten Bedrohungen sowohl für Privatanwender als auch für Unternehmen und Verwaltungseinrichtungen. Gegenüber 2015 haben sich die Schadprogramme abermals weiterentwickelt, die klassischen Abwehrmaßnahmen verlieren weiter an Wirksamkeit. Aufgrund der fortschreitenden Digitalisierung und Mobilität geraten auch mobile und alternative Plattformen weiter in den Fokus der Angreifer, wobei bei den mobilen Plattformen immer noch fast ausschließlich Android betroffen ist. Schadprogramme werden meist durch Mitwirkung des Nutzers installiert, wodurch technische Schutzmaßnahmen umgangen werden und Angreifer in abgesicherte Netze eindringen können. Auf klassische AV-Lösungen und Firewalls allein sollten sich Anwender somit nicht mehr verlassen. IT-Sicherheit muss als Gesamtkonzept verstanden und umgesetzt werden, wozu auch die Einbeziehung des Nutzers gehört.

Schadsoftware in Atomkraftwerk

Sachverhalt: Im Zuge von Vorbereitungen zu Revisionsarbeiten wurden in einem Atomkraftwerk in Deutschland Schadprogramme auf einem Rechner zur Darstellung und Aufzeichnung von Handhabungsvorgängen an der Brennelement-Lademaschine (Visualisierungsrechner) entdeckt.

Ursache: Die entdeckten Schadprogramme sind weit verbreitet und werden von Virenscannern seit längerer Zeit gut erkannt. Der Visualisierungsrechner selbst lief mit einer nicht mehr aktuellen Betriebssystemversion und verfügte nicht über einen Virenscanner. Dies ist im Umfeld von SCADA-Systemen nicht unüblich, bedingt durch dortige Zulassungsverfahren und Kompatibilitätsanforderungen. In dieser Kombination wurde ein Befall mit dem Conficker-Wurm möglich, der im Jahr 2009 für weltweites Aufsehen gesorgt hatte. Darüber hinaus wurde das Schadprogramm Ramnit, dessen Steuerungsserver im vergangenen Jahr durch Europol abgeschaltet worden war, auf dem Visualisierungsrechner gefunden.

Methode: Sowohl Conficker als auch Ramnit nutzen neben Computernetzwerken auch USB-Datenträger, um weitere Systeme zu infizieren. So konnte ein ursprünglich mit dem Internet verbundener PC, der via Internet mit der Schadsoftware infiziert wurde, die Schädlinge auf einen solchen USB-Datenträger übertragen. Der USB-Datenträger wurde zu einem späteren Zeitpunkt am Visualisierungsrechner verwendet und konnte so den ungeschützten Computer infizieren, obwohl dieser mit keinem Netzwerk verbunden war.

Schadenswirkung: Ein Schaden am AKW selbst, der dazugehörigen Infrastruktur oder Informationstechnik ist nicht entstanden. Für den Betreiber entstanden jedoch Aufwände durch die Arbeitszeit, die für die Rekonstruktion des Hergangs, die weitergehende Analyse und die anschließende Bereinigung der befallenen Computer und Datenträger aufgewendet werden musste.

Zielgruppen: Bei dieser Form von Schadprogrammen handelt es sich um Programme, die von Kriminellen in der Regel ungezielt eingesetzt werden.

Technische Fähigkeiten: Sowohl Conficker als auch Ramnit sind als übliche und zwischenzeitlich sogar veraltete Schadprogramme zu bewerten, die keine nach heutigem Maßstab besonderen Mechanismen verwenden. Auch der Verbreitungsweg über USB-Datenträger ist nicht ungewöhnlich.

1.2.2 Ransomware

Einleitung

Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes („ransom“) wieder freigeben. Das Lösegeld soll meist in Krypto-Währungen wie Bitcoin gezahlt werden. Cyber-Angriffe durch Ransomware sind eine Form digitaler Erpressung. Man unterscheidet zwei Typen:

- Ransomware, die den Zugang zu einem System sperrt oder unterbindet. Das System wird mit einem Bild oder einer Webseite überlagert und der Anwender so daran gehindert, das System zu nutzen. In einer Nachricht wird der Benutzer über die Sperrung des Systems informiert und zu einer Zahlung aufgefordert.
- Ransomware, die Daten verschlüsselt. Diese nutzt oder kombiniert symmetrische und/oder asymmetrische Verfahren zur Verschlüsselung von Nutzerdaten. Bei korrekter Implementierung ist die Wiederherstellung der verschlüsselten Daten nur mit dem passenden Schlüssel möglich.

Lage

- Aktuelle Ransomware-Familien zielen fast ausschließlich auf das Betriebssystem Microsoft Windows. Daneben gibt es Ransomware, die auf das Desktop-Betriebssystem Apple MacOS X, Server-Systeme unter GNU/Linux und mobile Betriebssysteme wie Android abzielt.
- Nach Auswertung der dem BSI vorliegenden Daten war Deutschland im ersten Halbjahr 2016 hauptsächlich von den Ransomware-Familien Locky, TeslaCrypt, Nemucod und Cerber betroffen.
- Die häufigsten Angriffsvektoren, über die Systeme mit Ransomware infiziert werden, sind Anhänge von Spam-E-Mails sowie Drive-by-Angriffe mittels Exploit-Kits. Der Versand der Spam-E-Mail erfolgt häufig über Botnetze, die bereits in der Vergangenheit durch die Verbreitung von anderen Schadprogramm-Arten in Erscheinung getreten sind (Dridex/Necurs).
- Beim überwiegenden Teil der Angriffe handelt es sich um ungezielte Massenangriffe. Daneben gibt es jedoch auch einzelne Ransomware-Familien sowie Berichte über Vorfälle, die auf ein gezieltes bzw. manuelles Vorgehen bei der Infektion mit Ransomware schließen lassen.

- Die Angreifer verwenden kryptografisch starke Algorithmen zur Verschlüsselung der Daten. Bei korrekter Verwendung und Implementierung dieser Algorithmen ist eine Entschlüsselung der Daten ohne den passenden Schlüssel unmöglich. Vor der Infektion angelegte Backups sind häufig die einzige Möglichkeit, die Daten wieder herzustellen.

- Für einige Ransomware-Familien haben Sicherheitsforscher und IT-Sicherheitsunternehmen Tools veröffentlicht, die eine Entschlüsselung der Daten ohne Zahlung eines Lösegeldes erlauben.

- Eine Auswertung der Detektionsdaten von Virenschutzprogrammen für Deutschland zeigt, dass die Anzahl der Systeme, die von Angriffsversuchen über den Angriffsvektor E-Mail betroffen waren, sehr stark angestiegen ist und im Mai 2016 ihren bisherigen Höhepunkt erreicht hat. Ab Juni 2016 ist eine deutliche Abnahme zu verzeichnen, die mit der Inaktivität des für Locky verantwortlichen Botnetzes in den ersten drei Wochen im Juni zu erklären ist. Die Anzahl der in Deutschland tatsächlich mit Ransomware infizierten Systeme ist im Verlauf des ersten Halbjahres ebenfalls angestiegen.

- Viele Ransomware-Familien verschlüsseln neben lokalen Laufwerken auch angeschlossene externe Medien wie USB-Sticks sowie Netzlaufwerke und nutzen weitere Methoden, um die Wiederherstellung von Daten zu erschweren. Gerade in Unternehmensnetzen mit weitreichenden Zugriffsmöglichkeiten können dadurch einzelne mit Ransomware infizierte Systeme unternehmensweite Datenverluste verursachen.

- Nach einer Umfrage des BSI war ein Drittel der befragten Unternehmen in den letzten sechs Monaten von Ransomware betroffen. Drei Viertel der Infektionen waren auf infizierte E-Mail-Anhänge zurückzuführen. Während 70 Prozent der betroffenen Unternehmen angaben, dass nur einzelne Arbeitsplatzrechner befallen waren, kam es in jedem fünften der betroffenen Unternehmen (22 Prozent) zu einem erheblichen Ausfall von Teilen der IT-Infrastruktur, 11 Prozent der Betroffenen erlitten einen Verlust wichtiger Daten.

Bewertung

Ransomware steht seit Anfang 2016 im öffentlichen Fokus, auch wenn diese Angriffsform ein für Cyber-Kriminelle bereits seit Längerem etabliertes Geschäftsmodell ist. Dem BSI vorliegende Daten belegen, dass sich die Bedrohungslage durch Ransomware in Deutschland seit Ende 2015 deutlich verschärft hat. Vorfälle in Krankenhäusern, kleinen und mittelständischen Unternehmen oder der öffentlichen Verwaltung wurden über Fachmedien hinaus breitflächig aufgegriffen. Anders als Infektionen mit anderen Schadprogrammtypen führen Infektionen mit Ransomware zu direkten, unmittelbar erkennbaren Schäden und zu konkreten Konsequenzen bei den Opfern. Da infolge der Infektion Systeme und Daten nicht mehr zur Verfügung stehen, entsteht bei den Betroffenen, egal ob Privatpersonen oder Unternehmen und Behörden, ein hoher Leidensdruck.

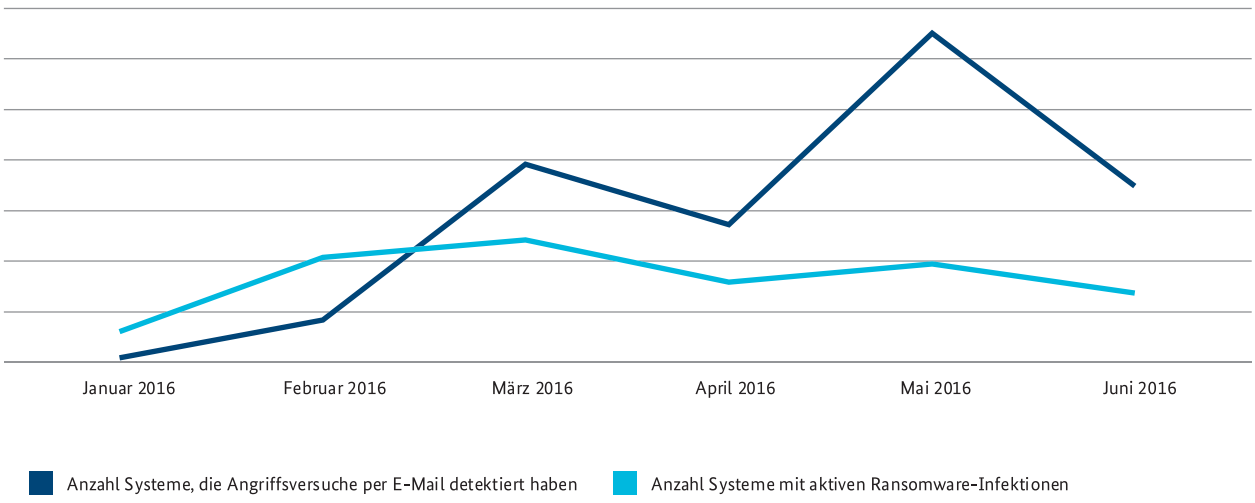


Abbildung 6: Trend der Anzahl Systeme mit Ransomware-Detektionen von Virenschutzprogrammen in Deutschland im ersten Halbjahr 2016

1.2.3 Social Engineering

Einleitung

Technische Schwachstellen und Sicherheitslücken stellen nur einen Teil der Risiken im Cyber-Raum dar. Wo Angreifer dank aktueller Software und Systeme, dank Firewalls und Virenscannern nicht weiterkommen, versuchen sie, Anwender auf andere Weise zur Installation von Schadsoftware oder zur Herausgabe sensibler Daten zu bewegen. Vergleichbar mit dem Trickbetrug an der Haustür setzen auch Cyber-Angreifer im Internet auf die Vortäuschung einer persönlichen Beziehung zum Opfer oder machen Gewinnversprechen. Viele weitere Varianten dieser Social Engineering genannten Vorgehensweise werden eingesetzt.

Lage

- Angreifer nutzen soziale Netzwerke, um die dort veröffentlichten persönlichen Informationen über potenzielle Opfer zu erhalten. Auch die erste Kontaktaufnahme läuft oftmals über soziale Netzwerke und wird in der Folge intensiviert, um die Opfer zu unüberlegten Handlungen zu verleiten, zum Beispiel eine infizierte E-Mail-Anlage zu öffnen oder eine infizierte Webseite aufzurufen. Dadurch gelingt es den Angreifern, das Nutzersystem mit Schadsoftware zu infizieren oder Zugang in ein Unternehmensnetz zu erlangen.

- Zur Ansprache der Opfer täuschen die Angreifer oftmals namhafte und bekannte Unternehmen oder Einrichtungen vor. Dies senkt die Hemmschwelle der Empfänger, einen Link oder Dateianhang anzuklicken, denn der Absender scheint bekannt oder vertraut zu sein.

- Im Zuge dieser Phishing-Angriffe werden fiktive Sicherheitsprobleme, gefälschte Rechnungen oder vorgetäuschte Statusmeldungen zu Aufträgen verwendet, um Nutzer dazu zu verleiten, unternehmensbezogene oder andere sensitive Informationen an Unberechtigte weiterzugeben. Zwecks Ablenkung des Opfers von der eigentlichen Problematik werden dabei Fristen gesetzt oder geringe Bearbeitungsgebühren erhoben. Zudem werden die Nutzer auf gefälschte Unternehmens-Webseiten gelockt, um dort in einer scheinbar vertrauten Umgebung Zugangs-, Konto- oder Kundendaten einzugeben oder zu bestätigen.

- Beliebte Angriffsmethoden sind nach wie vor der CEO-Betrug (vgl. Vorfallskasten CEO-Betrug) oder die Kontaktaufnahme per Telefon. Dabei geben sich die Angreifer als Support-Mitarbeiter von namhaften IT-Unternehmen wie Microsoft oder Dell aus, die angebliche Probleme mit dem Rechner des Anwenders beheben wollen. Dazu soll der Betroffene eine Fernwartungssoftware auf dem Rechner installieren, die dem vorgeblichen Techniker die Behebung der angeblichen Probleme ermöglicht. Folgt der Anwender der Anweisung, so haben die Angreifer durch diese Software Zugriff und Kontrolle über den Rechner.

- Gemäß einer Umfrage des BSI setzen zwar mehr als zwei Drittel der befragten Unternehmen Awareness-Maßnahmen um, diese werden aber meist nur sporadisch durchgeführt. Es fehlen vielfach kontinuierliche Prozesse, um die Mitarbeiter langfristig und nachhaltig zu sensibilisieren.

Bewertung

Social Engineering ist weiterhin eine vielfach genutzte Methode, um Cyber-Angriffe erfolgreich auszuführen oder zu unterstützen. Für Angreifer ist es einfacher, die Schwachstelle Mensch als oftmals schwächstes Glied der IT-Sicherheitskette zu überwinden, anstatt komplexe technische Sicherheitsmaßnahmen mit viel Aufwand zu umgehen. Wichtige Maßnahme gegen erfolgreiches Social Engineering ist die Sensibilisierung und Aufklärung der Anwender. Entsprechende Schulungsmaßnahmen sollten dabei nicht nur einmalig, sondern als Teil eines Gesamtkonzepts zur IT-Sicherheit regelmäßig durchgeführt werden.

1.2.4 Advanced Persistent Threats

Einleitung

Ein Advanced Persistent Threat (APT)-Angriff zeichnet sich im Gegensatz zu anderen Cyber-Angriffen dadurch aus, dass der Angreifer seine Ziele sorgfältig auswählt. Die Vorgehensweise unterscheidet sich teilweise stark von kriminell motivierten Angriffen und der Angreifer ist meist auch gewillt, mehr Ressourcen einzusetzen. So werden in der Regel nicht einzelne Rechner automatisiert infiziert. Stattdessen versuchen die Täter, sich im internen Netzwerk der angegriffenen Organisation auszubreiten und sich langfristig Zugang zu sichern. Dies erfordert in der Regel, dass sich die Täter manuell auf kompromittierte Rechner verbinden und über lange Zeit mit dem System interagieren.

Lage

- Im September und Oktober 2015 unterzeichnete China mit den USA und Großbritannien Abkommen, in denen vereinbart wurde, dass die Regierungen keine Cyber-Angriffe auf Unternehmen zum Zweck der Wirtschaftsspionage durchführen oder tolerieren sollten. Ausgenommen sind dabei Spionageangriffe gegen Regierungen und militärnahe Organisationen. Die entsprechenden Verhandlungen mit Deutschland wurden anlässlich der am

13. Juni 2016 durchgeführten 4. Deutsch-Chinesischen Regierungskonsultationen durch eine gemeinsame Erklärung abgeschlossen, wonach sich beide Seiten darauf verständigt haben, dass sie die Verletzung von geistigem Eigentum, Handels- oder Geschäftsgeheimnissen unter Verwendung des Cyber-Raums zur Erlangung von Wettbewerbsvorteilen für ihre Unternehmen oder kommerzielle Sektoren weder betreiben noch wissentlich unterstützen.

- Auf der operativen Ebene unterscheidet sich die Lage 2016 von den vorhergehenden Jahren. Ende 2015 nahm die Zahl der beobachteten Fälle von APT-Angriffen auf westliche Unternehmen ab und blieb 2016 auf diesem niedrigen Niveau. Beobachtete Aktivitäten von APT-Gruppen fokussierten vor allem auf Südostasien, Russland, Ukraine, Indien/Pakistan und generell Regionen, in denen es zwischenstaatliche Konflikte gab. Die Ziele waren meistens Regierungseinrichtungen, Rüstungsunternehmen und regierungskritische Personen wie Journalisten, Oppositionspolitiker oder Aktivisten.

- Ein Beispiel für diese Cyber-Angriffe in Konfliktregionen, das auch in den Medien diskutiert wurde, waren die Stromausfälle in der Ukraine. Die Täter nutzten dabei offenbar ein Schadprogramm namens BlackEnergy, um Zugang zu den Netzwerken von Stromversorgern zu erhalten (vgl. Vorfallskasten „Stromausfall in der Ukraine“, S. 40).

- Auch finanziell motivierte Täter übernehmen mitunter Techniken, die bisher nur APT-Akteuren zugeordnet wurden. So wurde beispielsweise die Ransomware „Samsam“ vergleichsweise gezielt verteilt. Die Täter identifizierten verwundbare Server, installierten dort Backdoors und breiteten sich dann wie APT-Täter im internen Netzwerk aus. Schließlich luden sie die Ransomware nach und verschlüsselten Daten, um Lösegeld zu erpressen.

Bewertung

Deutschland ist nach wie vor ein Ziel von Advanced Persistent Threats. Während sich die öffentliche Berichterstattung nur auf wenige prominente Angreifergruppen beschränkt, sind Unternehmen gut beraten, zu eruieren, welche Staaten und welche Angreifergruppen Interesse an Technologie und Geschäftsinteressen des Unternehmens haben. Präventionsmaßnahmen der IT-Sicherheit sollten idealerweise unabhängig von etwaigen Tätern sein. Es ist aber ratsam, darüber hinaus täterspezifische Indikatoren einzusetzen, um Angriffe erkennen zu können, die die Präventionsmaßnahmen unterlaufen haben.

CEO-Betrug

Sachverhalt: Bei dieser Variante des Social Engineerings werden vorrangig Mitarbeiter im Finanzwesen vorgeblich von einer real existierenden Führungskraft des eigenen Unternehmens per Telefon oder E-Mail angewiesen, eine größere Summe von einem Geschäftskonto auf ein fremdes Konto zu überweisen.

Methode: Die Kontaktdaten der Zielpersonen und der vorgetäuschten Absender werden häufig durch öffentliche Informationen auf der Webseite des Unternehmens, in Online-Karriereportalen, in Handelsregistereinträgen oder durch direkte Anrufe im Unternehmen gewonnen. Die Angreifer nutzen diese Informationen, um den vorgeblichen Absender, den Inhalt der E-Mail sowie den Stil der Kommunikation im Unternehmen glaubwürdig zu gestalten. Der Angreifer gibt sich als Geschäftsführer oder Mitglied der Unternehmensleitung aus und veranlasst einen Mitarbeiter, für ein vorgeblich dringendes Geheimprojekt einen hohen Geldbetrag auf ein fremdes Konto zu überweisen. Die telefonischen Instruktionen werden durch authentisch aussehende E-Mails des vermeintlichen Vorgesetzten flankiert. Alternativ werden Rufnummern von eingeweihten Externen mitgeteilt, die dem Mitarbeiter die Rechtmäßigkeit der Transaktion bestätigen. Das Opfer wird unter Zeitdruck gesetzt und durch die Verpflichtung auf Verschwiegenheit der Transaktion isoliert.

Schadenswirkung: Angaben des Bundeskriminalamts zufolge wurden seit 2013 in Deutschland bisher 250 Betrugsfälle bekannt. Davon waren 68 erfolgreich, 182 blieben im Versuchsstadium stecken. Der Gesamtschaden betrage demnach 110 Millionen Euro.
Da der Betrug in manchen Fällen erst nach mehreren Tagen entdeckt wird und die Kriminellen die Überweisung im Ausland rasch weiterleiten, ist das Geld bei einer getätigten Überweisung oft unwiederbringlich verloren.

Zielgruppen: Zu den Zielgruppen zählen insbesondere Mitarbeiter im Finanz- und Rechnungswesen, die Zugriff auf die Unternehmenskonten haben. Im Fokus stehen überwiegend mittlere bis große Unternehmen. Insbesondere im Falle von öffentlich in der Presse angesprochenen Investments und Übernahmen des Unternehmens besteht das Risiko von CEO-Betrug.

Technische Fähigkeiten: Die Kriminellen zeichnen sich durch gute Recherche- und Social-Engineering-Fähigkeiten aus. Die E-Mails mit den gefälschten Absendern sind in der Regel fehlerfrei formuliert und die Anrufe erfolgen in der Unternehmenssprache. Für die Durchführung des CEO-Betrugs kommt es weniger auf die technische Fähigkeit, sondern mehr auf die Überzeugungskraft der Kriminellen an. Wichtige Gegenmaßnahme seitens der Unternehmen ist die Sensibilisierung der Mitarbeiter für diese Angriffsmethode.

Cyber-Spionage bei Rüstungsunternehmen

Sachverhalt: Cyber-Spionage-Angriffe auf Industrieunternehmen befinden sich 2016 im Gegensatz zu Angriffen gegen Regierungsorganisationen auf einem niedrigeren Niveau. Im ersten Halbjahr 2016 wurde in der breiteren Öffentlichkeit ein Cyber-Angriff auf das Rüstungsunternehmen RUAG in der Schweiz bekannt.

Methode: Mithilfe der Schadprogramm-Familie Turla gelang es den Angreifern, durch Watering-Hole-Angriffe über präparierte Webseiten eine Erstinfektion zu erreichen. Per Drive-by-Exploit konnten die Angreifer eine Schwachstelle im Browser eines Mitarbeiters ausnutzen und ein Schadprogramm installieren. Im Nachgang kam es auf dem infizierten System zu einer Erweiterung der Benutzerprivilegien und über mehrere Stufen schließlich zur vollständigen Kontrolle über das Active Directory im Unternehmensnetz. Damit erlangten die Angreifer höchstmögliche Benutzerrechte. Insgesamt entwendeten die Angreifer über mehrere Monate ein Datenvolumen von 23 GB.

Schadenswirkung: Die hinter der Cyber-Spionage stehenden Angreifer hatten offenbar keine primär monetäre Motivation. Stattdessen zielte der Angriff auf das Ausspähen von Informationen ab. Diese können Staaten wiederum zur Gewinnung von Wettbewerbsvorteilen oder zur Anpassung der Wirtschafts- und Streitkräftepolitik verwenden.

Zielgruppen: Zu den Zielgruppen von Cyber-Spionage zählen Unternehmen, deren Wissen und Informationen für die Angreifer bzw. deren Auftraggeber wertvoll sind. Des Weiteren sind Behörden und nicht gewinnorientierte Organisationen betroffen, deren ausgespähte Informationen eine neue strategische Ausrichtung auf politischer oder wirtschaftlicher Ebene ermöglichen.

Technische Fähigkeiten: Hinter Cyber-Spionage stehen in der Regel Angreifer mit umfangreichen Personal- und Kapitalressourcen. Die potenziellen technischen Fähigkeiten sind im Vergleich zu Cyber-Crime sehr ausgeprägt, die Angreifer gehen zudem effizient vor. Wenn für einen erfolgreichen Angriff die Ausnutzung bekannter Schwachstellen in Kombination mit Social Engineering ausreichend ist, werden keine wertvollen Zero-Day-Exploits eingesetzt.

1.2.5 Spam

Einleitung

Unerwünscht zugesandte E-Mails werden generell als Spam bezeichnet. Dieser lässt sich in klassischen Spam, Schadprogramm-Spam und Phishing-Nachrichten unterteilen. 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. 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 bzw. im Anhang erfolgen, der auf das Schadprogramm oder eine Webseite mit Drive-by-Exploits verweist.

Lage

- Die Anzahl von Spam-Nachrichten mit Schadsoftware im Anhang ist seit Dezember 2015 förmlich explodiert und hat zum ersten Mal langfristig den Versand von sonstigen Spam-Nachrichten übertroffen. Im Dezember dominierte dabei der Versand von Downloadern, welche die Schadprogramme Dridex (Online-Banking-Trojaner) oder TeslaCrypt (Ransomware) nachgeladen haben. Der Distributionskanal für Dridex (Spamversand über mit Necurs infizierte Systeme) wurde ab Februar 2016 auch für die Verbreitung der Ransomware Locky sowie teilweise auch von TeslaCrypt und Cerber genutzt.

- Das Volumen der gesamten Spamaktivität hat im ersten Halbjahr 2016 im Vergleich zum Vorjahr um circa 73 Prozent zugenommen. Im Bereich des klassischen Spams ist eine moderate Zunahme um 16 Prozent zu verzeichnen. Um 1.270 Prozent zugenommen hat die Anzahl der Spam-Nachrichten mit Schadsoftware im Anhang (Quelle: BSI).

- Der Versand von Malware-Spam erfolgte vor allem aus Entwicklungs- und Schwellenländern wie Indien, Vietnam oder Mexiko. Es ist zu vermuten, dass hier eine globalisiert optimierte Strategie der Monetarisierung von kompromittierten Systemen verfolgt wird (Industrieländer: Ransomware und Banking-Trojaner, andere Länder: Spam- und DDoS-Bots).

- Als Downloader-Anhänge wurden Microsoft-Office-Dokumente mit Makros und seit Dezember auch Java-Script-Dateien beobachtet, zuerst bei TeslaCrypt-Kampagnen, später auch bei Locky-

und anderen Kampagnen. Im weiteren Verlauf wurden zusätzliche Skript- und Makro-Sprachen sowie Dateiformate (JS, VBS, VBE, Powershell, VBA-Makros in Office-Dokumenten, etc.) eingesetzt. Teilweise wurde die Schadsoftware in verschleierter Form als Teil des Anhangs mitgeliefert, durch Skripte entpackt und gestartet (Dropper vs. Downloader).

- Für alle Downloader- und Dropper-Varianten gilt: Die dort eingesetzten Techniken werden stets neu bzw. weiterentwickelt, um die Analyse zu erschweren und eine Erkennung durch Virenschutzprogramme zu verhindern.

- Die Verbreitung über das Necurs-Botnetz dominierte zahlenmäßig den Spamversand. Zusätzlich wurden kleinere, aber gezielter eingesetzte Ransomware-Kampagnen beobachtet, bei denen zum Beispiel angebliche Bewerbungsunterlagen an Unternehmen versendet wurden.

- Klassischer Spam hat heute kaum noch Auswirkungen auf die Verfügbarkeit der Mail-Systeme.

Bewertung

Die zahlreichen Meldungen von Betroffenen und das starke Echo in der Presse nach der Nutzung des Necurs-Botnetzes auch zur Verbreitung der Ransomware Locky zeigen die hohe Wirksamkeit der Verteilung von Schadprogrammen über Spam. Diese blieb bis dahin weitgehend verborgen, da die bis dato verteilte Schadsoftware (Spionage- bzw. Banking-Trojaner) sich möglichst unauffällig verhielt und die Infektion häufig nicht bemerkt wurde. Der explosionsartige Anstieg von Malware-Spam zeigt auch, dass die Verteilung von Schadsoftware und insbesondere von Ransomware offenbar ein lohnendes Geschäft für Kriminelle ist.

Die von den Angreifern immer professioneller aufbereiteten Spammails – nach E-Mail-Vorlagen bekannter Unternehmen und mit ansprechenden Themen – verleiten immer mehr Benutzer dazu, Schadprogramme aus Spamnachrichten auszuführen. Teilweise mehrstufige Verschleierungstechniken, die Nutzung von unterschiedlichsten Skriptsprachen und Dateiformaten zum Nachladen bzw. Entpacken der eigentlichen Schadsoftware, individuelle Varianten bei den versendeten und/oder zum Download bereitgestellten Schadprogrammen im Stundentakt und der zeitlich gesteuerte Versand führen dazu, dass zum Zeitpunkt, an dem die Spamnachricht den Nutzer erreicht, meist kein signaturbasiertes Virenschutzprogramm den Schädling erkennen und eine Infektion verhindern kann.

Als Gegenmaßnahme ist somit auch der aufmerksame Benutzer gefordert, mit gesundem Misstrauen E-Mails zu bearbeiten, die von unbekannten Absendern stammen oder bei denen etwas nicht in Ordnung zu sein scheint. Dies wird jedoch auch für Profis immer schwieriger, da teilweise persönliche Daten des Empfängers wie Name, Adresse und Telefonnummern in den Spam-Mails enthalten sind, welche zuvor bei Online-Dienstleistern gestohlen wurden.

Eine gute – wenn auch aufwendige – technische Gegenmaßnahme bietet das Whitelisting von Verzeichnissen, aus denen ausführbare Dateien gestartet werden dürfen. Gegen die Windows-Skript-Varianten hilft eine Deaktivierung des Windows-Skripting-Hosts. Vor allem ist es wichtig – sowohl für Behörden und Unternehmen als auch für Privatanwender – stets aktuelle Backups aller wichtigen Daten vorzuhalten. Das Backup sollte nicht dauerhaft von dem zu sichernden System aus zugreifbar sein, damit dieses im Falle einer Ransomware-Infektion nicht ebenfalls verschlüsselt wird.

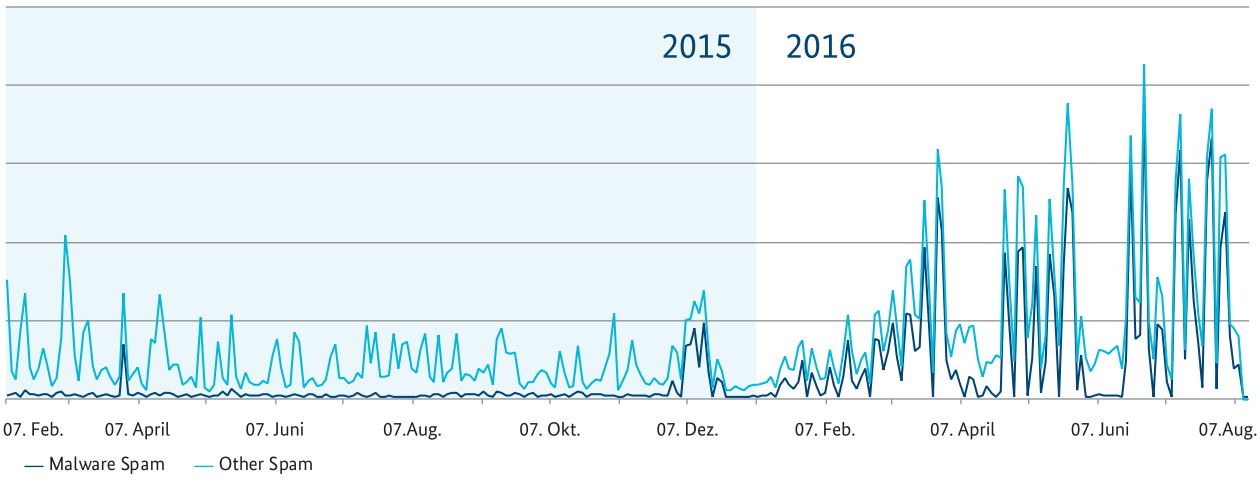


Abbildung 7: Spam-Verlauf pro Woche in Deutschland seit 1.1.2015

1.2.6 Botnetze

Einleitung

Als Botnetz wird ein Verbund von Systemen bezeichnet, die von einem fernsteuerbaren Schadprogramm befallen sind. Hierbei handelt es sich hauptsächlich um klassische PCs, zunehmend sind aber auch mobile Geräte wie Smartphones oder Tablets betroffen. Auch Webserver sind aufgrund ihrer hohen Verfügbarkeit und breitbandigen Anbindung ein zunehmend attraktives Ziel. Da prinzipiell jedes internetfähige System Teil eines Botnetzes werden kann, stellen auch infizierte Internetrouter oder Unterhaltungsgeräte wie Smart-TVs keine Ausnahmen mehr dar. Der Zugriff auf Bots erfolgt über zentrale Systeme, die von den Botnetz-Betreibern kontrolliert werden und die es ermöglichen, den Bots Steuerbefehle zu schicken. Diese Systeme werden als Command-and-Control-Server (C&C-Server) bezeichnet.

Lage

- Botnetze werden von Kriminellen nach wie vor in großem Stil zum Informationsdiebstahl, für Angriffe auf die Verfügbarkeit von IT-Systemen sowie zum Versand von Spam genutzt.

- Im Berichtszeitraum wurden von Sicherheitsforschern täglich bis zu 39.000 Infektionen deutscher Systeme registriert und über das BSI an die deutschen Internetanbieter gemeldet. Im Vorjahreszeitraum lag die Zahl der Infektionen bei rund 60.000, somit ist dieser Wert deutlich gesunken. Die Internetanbieter informieren ihre Kunden über die Infektion und bieten zum Teil auch Hilfestellung bei der Bereinigung der Systeme an.

- Um Botnetzinfektionen zu detektieren, betreiben Sicherheitsforscher Sinkhole-Systeme, die anstelle der C&C-Server Kontaktanfragen von Bots entgegennehmen. Möglich wird dies durch eine Registrierung der verwendeten Domänennamen oder auch der IP-Adressen. 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. Da Bots in der Regel die Adressen der C&C-Server über spezielle Verfahren ermitteln, kann es sein, dass ein Kontakt zu einem Sinkhole-System nicht zustande kommt, falls vorher ein aktiver C&C-Server gefunden wurde.

- Im Juni beobachtete CERT-Bund für ca. drei Wochen das Ausbleiben einschlägiger Spamwellen des Botnetzes Necurs. Da nahezu zeitgleich die Anzahl der Necurs-Bots, die sich an den für die BSI-Warnungen verwendeten Sinkhole-Systemen meldeten, sprunghaft von 500 auf 5.000 im Tagesdurchschnitt anstieg, legte dies die Vermutung nahe, dass ein für den Betrieb von Necurs zentrales Steuersystem weggefallen war und sich die Bots deshalb zu den Sinkhole-Systemen von Sicherheitsforschern verbanden. Durch die Verbindung mit dem Sinkhole-Server erhielten die Bots keine Kommandos des Botmasters mehr und führten deshalb keine schädlichen Aktionen mehr aus. Ab dem 21. Juni nahm das Botnetz seine Aktivitäten wieder auf. Über die genauen Hintergründe ist bislang nichts bekannt. Mit einer Größe von ca. einer Million Bots war Necurs zu diesem Zeitpunkt ein großes Botnetz. Die Größe ist jedoch nicht ungewöhnlich und wurde beispielsweise von Citadel in den Jahren 2014 und 2015 übertroffen. Das größte bislang bekannte Botnetz war Bredolab mit 30 Millionen Bots im Jahr 2012.

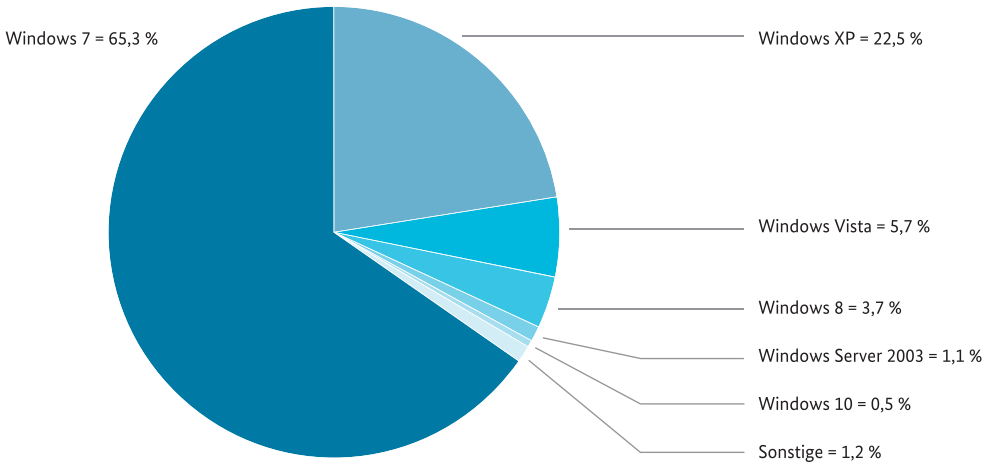


Abbildung 8: Betriebssystemverteilung Nymaim-Infektionen

- Aufgrund des hohen Marktanteils sind überwiegend Microsoft-Windows-Systeme von Bot-Infektionen betroffen. Abbildung 8 zeigt eine Verteilung anhand einer Stichprobe von Nymaim-Infektionen Mitte Juni 2016. Bei Nymaim (Hauptzweck: Informationsdiebstahl) handelt es sich um eines der aktivsten Botnetze in Deutschland, welches das verwendete Betriebssystem des Opfersystems an einen Sinkhole-Server überträgt. Hier führt Windows 7 mit ca. 65,3 Prozent vor Windows XP (22,5 Prozent) sowie Windows Vista (5,7 Prozent). Bei anderen Windows-Versionen sind die Zahlen geringer.

- Auch Mac OS X und Android-Geräte rücken zunehmend in den Fokus der Cyber-Kriminellen. Aktuell sind mehrere Botnetze bekannt, die sich ausschließlich auf Android konzentrieren und zum Informationsdiebstahl eingesetzt werden. Weiterhin hält der Trend an, kompromittierte legitime Webserver zum Betrieb von C&C-Servern zu missbrauchen.

- Auch wenn im Berichtszeitraum im Tagesdurchschnitt nur wenige Hundert Infektionen von Mobilfunkgeräten in Deutschland berichtet wurden, so ist der Trend steigend und die Anzahl der auf mobile Endgeräte fokussierten Botnetze nimmt zu. Analog hierzu wurden auch Botnetze von Apple iOS-Geräten beobachtet, die für Deutschland jedoch keine Relevanz haben.

- Die gemeldeten Infektionen verteilten sich im Berichtszeitraum auf annähernd 120 verschiedene Botnetzfamilien. Eine genauere Betrachtung der zwanzig häufigsten Familien Anfang Juni zeigt, dass der Großteil (ca. 55 Prozent) vorrangig zum Online-Banking-Betrug verwendet wird. Knapp 25 Prozent der betrachteten Botnetzfamilien fungieren hauptsächlich als Dropper und dienen somit dem Nachladen weiterer Schadprogramme. Für Klickbetrug bzw. Bitcoin-Mining werden ca. 15 Prozent eingesetzt, während lediglich 5 Prozent zum Spamversand genutzt werden. Botnetze mit dem Hauptzweck DDoS fanden sich in der Stichprobe nicht.

- Es wurden im Tagesdurchschnitt 765 aktive C&C-Server beobachtet, die mehr als 50 unterschiedlichen Botnetzfamilien zuzuordnen waren. Die Anzahl und die Lokalisierung der Systeme variiert ständig, da viele C&C-Server aufgrund von Gegenmaßnahmen nur kurzzeitig bei einem bestimmten Webhoster betrieben und oft bereits nach wenigen Stunden zu einem anderen Anbieter geschwenkt werden.

Bewertung

Da nicht für alle weltweit existierenden Botnetze valide C&C-Adressen für Sinkhole-Systeme registriert werden können, stellen die im Berichtszeitraum gemeldeten 39.000 Infektionen nur eine Untergrenze für Deutschland dar. Aufgrund der Erfahrungen aus erfolgreichen Botnetzabschaltungen ist davon auszugehen, dass die Dunkelziffer deutlich höher liegt und sich mindestens in einem sechsstelligen Bereich bewegt.

Wie die Betriebssystemverteilung der Nymaim-Infektionen zeigt, laufen die meisten infizierten Systeme unter Windows 7. Da davon auszugehen ist, dass viele Schadprogramme für Windows-Betriebssysteme unter allen aktuellen Versionen lauffähig sind, empfiehlt sich beim Umstieg auf eine neuere Betriebssystemversion eine saubere Neuinstallation. Im Fall von Nymaim würde eine vorhandene Infektion bei einem Windows 7-System bei einem Upgrade auf Windows 10 erhalten bleiben und das Schadprogramm wäre auch nach dem Upgrade weiterhin aktiv.

Botnetz-Infrastrukturen bieten Kriminellen Zugriff auf große Ressourcen an Rechnerkapazität und Bandbreite, die sie für ihre kriminellen Handlungen nutzen können. Aufgrund von Professionalisierung und Kommerzialisierung des Cybercrime ist der Betrieb eines Botnetzes auch für technische Laien vergleichsweise einfach und kostengünstig realisierbar. Die Bedrohungslage durch Botnetze ist im Vergleich zum Vorjahr gleichbleibend hoch. Dies resultiert einerseits aus der Vielzahl verwundbarer Internetsysteme, die als Bots verwendet werden können, sowie andererseits aus der niedrigen Einstiegshürde für Cyber-Kriminelle.

1.2.7 DDoS

Einleitung

Bei einem Distributed-Denial-of-Service-Angriff (DDoS-Angriff) wird versucht, die Verfügbarkeit eines Dienstes durch eine Vielzahl von Anfragen oder Datenpaketen zu beeinträchtigen. Die Angriffe erfolgen in der Regel entweder durch Botnetze und/oder als Reflection-Angriffe (DRDoS-Angriffe) unter missbräuchlicher Ausnutzung öffentlich erreichbarer und fehlerhaft konfigurierter Server von Dritten. Durch DDoS-Angriffe können dem Betreiber teils bedeutende Schäden entstehen, wenn ein angebotener Dienst – etwa eine Webseite oder ein Onlineshop – nicht zur Verfügung steht. Drohende Umsatzeinbußen oder Reputationsverlust werden von Angreifern als Druckmittel eingesetzt, mit denen sie versuchen, ihre Opfer unter der Androhung von DDoS-Angriffen zu erpressen.

Lage

- Während sich im Berichtszeitraum die maximale Bandbreite von Einzelangriffen nochmals gesteigert hat – einzelne Angriffe erreichen Bandbreiten von mehr als 200 Gbps –, konnten bei der durchschnittlichen Bandbreite aller dem BSI bekannten DDoS-Angriffe nur geringfügige Steigerungen beobachtet werden. Die Mediane der Angriffsbandbreite und der Angriffspaketrate sind im Berichtszeitraum sogar gesunken.
- Erneut war festzustellen, dass lang andauernde Angriffe eher selten sind. Vielfach verwenden die Angreifer mehr als einen Angriffsvektor, etwa HTTP-Flooding in Kombination mit DNS-Reflection.
- Im Berichtszeitraum gab es zahlreiche Erpressungsversuche von verschiedenen Angreifergruppierungen, darunter aber auch viele Trittbrettfahrer. Einige beschränken sich auf das Verschicken von Erpresserschreiben, während andere Gruppen dem Erpresserschreiben mit einem initialen DDoS-Angriff Nachdruck verleihen.

Bewertung

DDoS-Angriffe stellen nach wie vor eine Bedrohung für Anbieter von Internetdienstleistungen dar. Auch wenn die Durchschnittswerte aller Angriffe nur moderate Steigerungen zeigen und die Mediane sogar sinken, sind für eine Bewertung der eigenen Betroffenheit auch die Angriffe mit sehr hohen Bandbreiten zu berücksichtigen. Bei diesen Angriffen ist häufig einer der Angriffsvektoren ein Reflection-Angriff. Das BSI hat in Zusammenarbeit mit Providern und anderen Netzbetreibern in Deutschland die Anzahl von offen erreichbaren Server-Diensten, die sich für Reflection-Angriffe ausnutzen lassen, in den letzten Jahren stark reduzieren können. Die folgende Grafik zeigt die Entwicklung seit Juni 2014 in Deutschland und weltweit. Die Anzahl offener Server-Dienste ist zwar auch weltweit rückläufig, in Deutschland jedoch stärker als im weltweiten Durchschnitt. (Die Anzahl der Systeme im Juni 2014 entspricht 100%.)

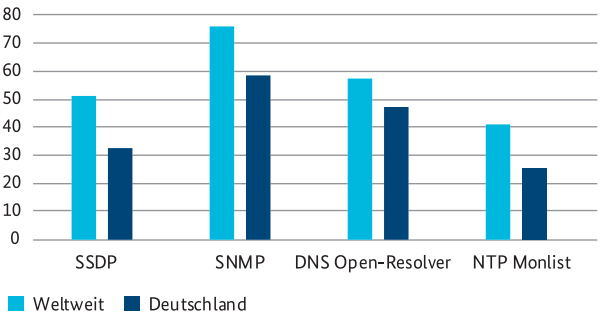


Abbildung 9: Anteil offener Server im Vergleich zu Juni 2014
Quelle: Shadowserver, Stand: Juni 2016

In der Betrachtung einzelner Server-Typen lässt sich sehr gut die kontinuierliche Entwicklung erkennen:

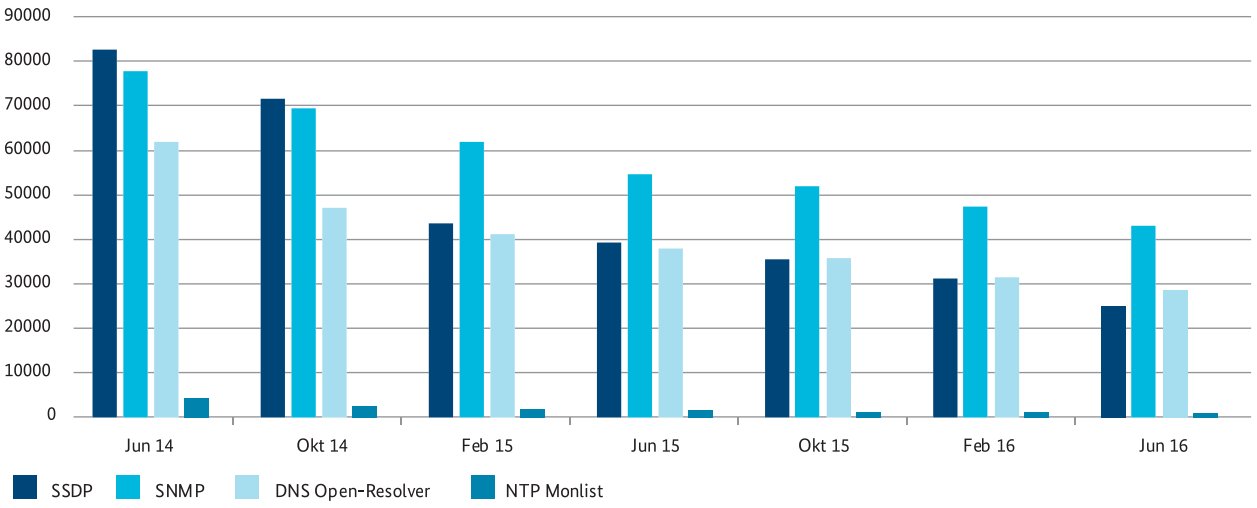


Abbildung 10: Entwicklung der Anzahl offener Server-Dienste in Deutschland seit Juni 2014, Quelle: Shadowserver, Stand: Juni 2016

DDoS-Erpressung

Sachverhalt: Dem BSI wurden im Berichtszeitraum zahlreiche Fälle von DDoS-Erpressungen gemeldet. In den jeweiligen Vorfällen gingen bei Internet-Dienstleistern und Onlineshops per E-Mail Erpresserschreiben ein, die einen DDoS-Angriff für den Fall ankündigten, dass nicht ein Lösegeld gezahlt würde. Am häufigsten traten dabei die Tätergruppen DD4BC, Armada Collective und Kadyrovtsy in Erscheinung. Viele betroffene Unternehmen erstatteten Strafanzeige.

Methode: Parallel zum Versand der Erpresserschreiben führten die Täter kurze Angriffe durch, um ihre Leistungsfähigkeit zu demonstrieren und die Ernsthaftigkeit der DDoS-Erpressung zu unterstreichen. Gingen die Betroffenen nicht auf die Erpressung ein, kam es zu DDoS-Angriffen durch die beiden Gruppen DD4BC und Armada Collective, bei Kadyrovtsy wurden solche Angriffe hingegen nicht beobachtet. Aufgrund der öffentlichen Berichterstattung traten zudem mehrere Trittbrettfahrer auf den Plan, die ohne tatsächlich durchgeführte DDoS-Angriffe auf eine Zahlung der Empfänger hofften. Das Lösegeld wurde in vielen Fällen in Form der Kryptowährung Bitcoin gefordert.

Schadenswirkung: Bei Internet-Dienstleistern und Onlineshops kam es aufgrund der DDoS-Angriffe zu Umsatzeinbußen, eingeschränkter Dienstgüte, Aufwänden durch die Implementierung von DDoS-Abwehrmaßnahmen sowie zu Reputationsschäden.

Zielgruppen: Von DDoS-Erpressung betroffen waren vorrangig Online-Händler und Internet-Dienstleister, deren Geschäftsmodell auf der Verfügbarkeit ihrer Angebote und Dienste basiert. Vereinzelt erhielten zudem auch Banken die DDoS-Erpresserschreiben.

Technische Fähigkeiten: Angreifer müssen keine wesentlichen technischen Fähigkeiten aufweisen, denn die notwendigen Angriffsmittel wie Botnetze oder entsprechende DDoS-Dienstleistungen können in Untergrundforen gemietet oder beauftragt werden. Im Falle der Trittbrettfahrer wurden die DDoS-Erpresserschreiben lediglich kopiert.

1.2.8 Drive-by-Exploits und Exploit-Kits

Einleitung

Drive-by-Exploits nutzen Schwachstellen im Webbrowser, in Browser-Plug-ins oder im Betriebssystem aus, um Schadprogramme unbemerkt und ohne Zutun des Benutzers auf verwundbaren Systemen zu installieren. Dazu reicht allein der Besuch einer entsprechend präparierten Webseite. Drive-by-Exploits werden einzeln oder gesammelt in Exploit-Kits verwendet. Die Verbreitung erfolgt über manipulierte Werbebanner oder direkt kompromittierte Webserver. Während Exploit-Kits primär bei breiten, ungezielten Angriffen zum Einsatz kommen, werden einzelne Drive-by-Exploits sowohl bei gezielten Kampagnen als auch bei ungezielten Angriffen verwendet.

Lage

- Nach Auswertung der dem BSI vorliegenden Detektionsdaten für Exploit-Kit-Angriffe in Deutschland sind die Angriffe im Zeitraum zwischen März und Juni 2016 am häufigsten auf die Exploit-Kits Angler, Neutrino und Magnitude zurückzuführen. Der Exploit-Kit-Markt zeigt sich jedoch aktuell sehr flexibel: Etablierte Exploit-Kits wie das Angler- oder das Nuclear Exploit-Kit verschwinden augenscheinlich vom Markt, doch deren Aktivität wird umgehend durch andere Exploit-Kits ersetzt.
- Die Schadsoftware, die nach einem erfolgreichen Angriff von einem Exploit-Kit installiert wird, variiert und kann jederzeit von den Angreifern angepasst werden. Exploit-Kits gehören jedoch – neben Spam-E-Mails – zu den häufigsten Infektionsvektoren für Ransomware. Auch die in Deutschland am häufigsten detektierten Exploit-Kits Angler, Neutrino und Magnitude werden auch zur Installation von Ransomware verwendet.
- Schädliche Werbebanner sind weiterhin eine Hauptursache für Drive-by-Angriffe. Ursache ist, dass Werbebanner häufig von unbekannten Dritten bereitgestellt oder von Agenturen vermarktet werden, die dann ohne Überprüfung oder Qualitätskontrolle in eine Webseite eingebunden werden. Auf diese Weise werden auch populäre und ansonsten gut abgesicherte Webseiten Ausgangspunkt von Angriffen mit Drive-by-Exploits.
- Wie im Jahr 2015 bleibt auch 2016 der Adobe Flash Player im Fokus von Drive-by-Angriffen. Von sieben neuen Schwachstellen, die im ersten Halbjahr 2016 erstmalig in Drive-by-Angriffen und Exploit-Kits verwendet wurden, betrafen fünf den Adobe Flash Player, eine Microsoft Silverlight und eine den Microsoft Internet Explorer. Die Schwachstellen CVE-2016-4171 (Adobe Flash-Player), CVE-2016-4117 (Adobe Flash Player) und CVE-2016-0189 (Microsoft Internet Explorer) wurden als 0-Day-Exploits in gezielten Angriffen ausgenutzt, bevor Sicherheitsupdates der Hersteller zur Verfügung standen.

- Watering-Hole-Angriffe sind gezielte Angriffe, bei denen Drive-by-Exploits zielgerichtet auf Webseiten platziert werden, die für die anvisierte Organisation relevant sein könnten. Zweck solcher Angriffe ist in der Regel Spionage. Gezielte Angriffe per Drive-by-Exploit erfolgen weiterhin auch durch E-Mails, die speziell auf das Tätigkeits- oder Interessengebiet des Empfängers zugeschnitten sind und die Links auf präparierte Webseiten enthalten (Spear-Phishing). Im Juni 2016 wurde beispielsweise eine Welle entsprechender E-Mails festgestellt, die durch Informationen, welche die Angreifer im sozialen Netzwerk LinkedIn gesammelt hatten, auf den Empfänger zugeschnitten waren und die ein Schadprogramm in Form einer angeblichen Rechnung enthielten.

Bewertung

Im Vergleich zum Vorjahr hat sich die Bedrohungslage durch Drive-by-Exploits und Exploit-Kits nicht verändert: Wie im Jahr 2015 werden neue Schwachstellen, vornehmlich im Adobe Flash Player, weiterhin regelmäßig und binnen kürzester Zeit in Exploit-Kits integriert oder für Drive-by-Angriffe verwendet. Bei einer erfolgreichen Infektion wird vermehrt Ransomware auf den Opfersystemen installiert, wodurch die Betroffenen einen Schaden durch Verlust von Daten erleiden.

Vor diesem Hintergrund bleibt die regelmäßige Aktualisierung von Anwendungen und für Unternehmen die Etablierung eines Patch-Management-Prozesses, mit dem Software-Schwachstellen geschlossen werden, besonders wichtig. Sicherheitsupdates müssen unverzüglich nach ihrer Bereitstellung durch den jeweiligen Hersteller angewendet und im Unternehmensumfeld idealerweise über eine zentrale Softwareverteilung eingespielt werden. Wenn das nicht möglich ist, kann die zumindest temporäre Deaktivierung betroffener Programme oder Plug-ins notwendig sein, um sich vor Angriffen, z. B. durch 0-Day-Exploits, zu schützen.

1.2.9 Identitätsdiebstahl

Einleitung

Im Kontext des Internets besteht die Identität einer Person meist aus Identifikations- und Authentisierungsdaten, wie etwa der Kombination von Benutzername und Passwort, Bank- oder Kreditkarteninformationen oder E-Mail-Adressen. Verschafft sich ein Unberechtigter Zugang zu solchen Daten, so spricht man von Identitätsdiebstahl. Von Interesse ist für die Täter insbesondere der monetäre Gewinn, der durch den Missbrauch oder den Verkauf von gestohlenen Identitäten erzielt werden kann.

Lage

- Von Juli 2015 bis Juni 2016 hat das BSI rund 141.000 neue Schadprogramme analysiert, die einen Bezug zum Identitätsdiebstahl in Deutschland aufweisen.

- Dem BSI sind ca. 62.000 Infektionen durch eine einzige Schadprogramm-Familie mit Identitätsdiebstahlfunktion („Peer-to-Peer-Zeus“) in Deutschland bekannt. Es ist davon auszugehen, dass die Gesamtzahl der Infektionen erheblich höher liegt.

- 2015 lag die Zahl der bekannten Infektionen noch bei 100.000. Der Rückgang ist vor allem auf die Fokussierung der Täter auf Ransomware zurückzuführen. So werden Botnetze, die bislang zur Verbreitung von Banking-Schadprogrammen dienten, nun zur Verteilung von Ransomware genutzt. Zudem gibt es Zusammenhänge zwischen dem Banking-Schadprogramm Dridex und der Ransomware Locky. Offenbar wurden hier Entwicklerressourcen zugunsten der Ransomware verlagert.

- Die Angriffsformen haben sich im Vergleich zum letzten Jahr nicht verändert. Die meisten Identitätsdaten werden weiterhin entweder durch Schadprogramme von Client-Systemen oder durch Ausnutzung einer Schwachstelle von Unternehmensservern gestohlen.

- Passwörter ihrer Kunden werden von Unternehmen oftmals nur mit unzureichenden Hashverfahren oder unzureichend verschlüsselt gesichert. Ein erfolgreicher Diebstahl vom Server liefert somit oft mehrere Millionen von verwertbaren Datensätzen.

- Meldungen zu Diebstählen von Datenbanken mit Kundeninformationen sind inzwischen an der Tagesordnung. Oftmals kann jedoch die Qualität der in Umlauf gebrachten oder zum Verkauf angebotenen Datensätze nicht geprüft werden. Vor allem, wenn der betroffene Dienstleister den Diebstahl nicht bestätigt, ist fraglich, ob die Daten tatsächlich aus einem Diebstahl stammen. In solchen Fällen ist nicht auszuschließen, dass die Daten von Betrügern generiert wurden, um diese an leichtgläubige Interessenten zu verkaufen.

- Verstärkt hat sich der Trend, mit Datensätzen zu handeln, die aus lange zurückliegenden Einbrüchen stammen. Nicht selten liegt der Umfang bei weit über 50 Millionen gestohlenen Identitäten. Die Qualität bzw. Gültigkeit der gehandelten

Passwörter dürfte grundsätzlich niedriger als üblich sein, da die Passwörter entweder vom Anbieter in der Zwischenzeit zurückgesetzt oder vom betroffenen Nutzer geändert wurden.

Bewertung

Durch den Verkauf oder den Missbrauch von gestohlenen Identitäten können Angreifer oft einen direkten monetären Gewinn erzielen. Dennoch geht der Trend weg von Identitätsdiebstahl und hin zu Ransomware, da die Zahlung bei Ransomware anonym erfolgen kann und somit das Entdeckungsrisiko für den Täter erheblich geringer ist. Zudem ist beim Einsatz von Ransomware keine Arbeitsteilung für Diebstahl und Missbrauch von gestohlenen Identitäten notwendig. Damit entfällt der Einsatz kostenintensiver Mittelsmänner.

1.2.10 Seitenkanalangriffe

Einleitung

Bei Seitenkanalangriffen werden aus beobachtbaren Effekten bei der Verarbeitung von sensitiven Daten, in der Regel Schlüsselmaterial, Rückschlüsse auf diese Daten gezogen, sodass die Entropie der Daten signifikant verringert wird. Beobachtbare Effekte sind beispielsweise Laufzeitverhalten, Energieverbrauch und elektromagnetische Abstrahlung. Seitenkanalresistente Implementierungen von kryptografischen Verfahren verwenden soft- und hardwareseitig Gegenmaßnahmen, um diese unerwünschten Nebeneffekte zu verringern, d.h., insbesondere sollte das Verfahren so implementiert werden, dass die Verarbeitung von sensitiven Daten maskiert und in konstanter Zeit erfolgt. Eine völlig seitenkanalfreie Verarbeitung ist jedoch unmöglich. Grundsätzlich gilt: Je weniger beobachtbare Effekte zur Seitenkanalanalyse ausgenutzt werden können, desto aufwendiger ist das zur Messung der Effekte notwendige Equipment und desto mehr Messdaten werden benötigt, um ein auswertbares Signal mit statistischen Methoden vom überlagerten Rauschen zu trennen.

Lage

Da inzwischen hochauflösende Oszilloskope relativ günstig am Markt verfügbar sind bzw. in Forschungseinrichtungen zur Verfügung stehen, stellt die Messung von lokaler elektromagnetischer Abstrahlung etwa eines Kryptocoprozessors keine große Herausforderung mehr dar. Auch im Bereich der statistischen Auswertung der Messdaten sind erhebliche Fortschritte im wissenschaftlichen Bereich gemacht worden. Während bei den klassischen Seitenkanalangriffen eine große Menge an Messdaten erforderlich war, die mit dem gleichen Schlüssel erstellt worden sind, um diesen Schlüssel per Differential Power Analysis zu extrahieren, unterscheiden modernere Angriffsmethoden wie Template Attacks zwischen einer aufwendigen Vorbereitung des Angriffs und der einfacheren Durchführung von Angriffen.

Bewertung

Durch die Asymmetrie in Bezug auf Vorbereitung und Durchführung von Seitenkanalangriffen bei Template-Attacken skalieren die Angriffe deutlich besser, sodass für das Zielobjekt nur eine geringe Anzahl an Messungen benötigt wird. Dadurch kann insbesondere auch durch häufige Schlüsselwechsel nicht verhindert werden, dass ausreichend viele Messdaten zur Extraktion des Schlüssels erfasst werden können. Da weiterhin an dieser Thematik geforscht wird und fortlaufend optimierte Angriffsvektoren entwickelt werden, stellen Seitenkanalangriffe eine Bedrohung für viele aktuell verwendete Sicherheitselemente dar, selbst wenn deren Sicherheit in der Vergangenheit 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.

Durch die steigende Verwendung solcher Chips im Zuge der fortschreitenden Digitalisierung ergeben sich ständig neue Angriffsziele. So werden hardwarebasierte Sicherheitselemente beispielsweise in Keyless-entry-and-drive-Systemen im Bereich Automotive, in Zutrittssystemen in Firmen und Behörden, in elektronischen Ausweisdokumenten oder bei Zwei-Faktor-Authentisierungen für Internetdienste genutzt. Wenn es einem Angreifer gelingt, Schlüsselmaterial aus einem Sicherheitschip auszulesen, erhält er den gleichen Zugriff auf die Daten oder Dienste wie der rechtmäßige Eigentümer. Somit sind Staat, Wirtschaft und Gesellschaft von Seitenkanalangriffen insbesondere dort betroffen, wo sich mit dem Verkauf von extrahierten Schlüsseln hohe Gewinne erzielen lassen.

2 Gefährdungslage der Bundesverwaltung

2 Gefährdungslage der Bundesverwaltung

2.1 Abwehr von Angriffen auf die Regierungsnetze

Die Abwehr von Gefahren für die IT des Bundes ist eine Kernaufgabe des BSI. Seit seiner Gründung hat das BSI die Aufgabe wahrgenommen, die Netze der Bundesverwaltung zu schützen. Als im Zuge des Regierungsumzugs nach Berlin das Regierungsnetz (Informationsverbund Berlin-Bonn, IVBB) entstand, wurde dem BSI die Gesamtverantwortung für das IT-Sicherheitskonzept übertragen. Wichtigste Sicherheitsmaßnahmen des zentralen Regierungsnetzes sind eine durchgängig verschlüsselte Kommunikation und eine robuste, redundante Architektur. Darüber hinaus wird ein geregelter, vertrauensvoller Betrieb gewährleistet. Zudem werden permanente Verbesserungen in der sicherheitstechnischen Aufstellung der Netze sowie auch eine enge Anbindung der Netze der Länder und Kommunen realisiert. Die Maßnahmen des BSI zum Schutz der Regierungsnetze unterliegen einer kontinuierlichen Überprüfung, Weiterentwicklung und Anpassung an die dynamische Bedrohungslage. Cyber-Angriffe auf die Regierungsnetze finden täglich statt. Neben ungezielten Massenangriffen sind die Regierungsnetze auch gezielten Angriffskampagnen ausgesetzt. Zum Schutz der IT-Systeme und Netze hat das BSI ein mehrstufiges Sicherheitssystem aufgebaut, bei dem neben handelsüblichen Virenschutzprogrammen auch individuell angepasste Schutzmaßnahmen greifen.

Im Bereich Abwehr schädlicher E-Mails wurden in der ersten Jahreshälfte 2016 in den Regierungsnetzen durchschnittlich etwa 44.000 infizierte E-Mails pro Monat in Echtzeit abgefangen, bevor sie die Postfächer der Empfänger erreichten. Dabei handelt es sich um eine Vervierfachung gegenüber dem Vorjahr. Den größten Anteil an dieser Zunahme haben E-Mails mit Anhängen wie Makro-Dokumenten oder Javascript-Archiven, wie sie für Ransomware typisch sind. Um diese E-Mails zu blockieren, werden im ersten Schritt kommerzielle Virenschutzprogramme eingesetzt und mit eigenen Signaturen ergänzt. Darüber hinaus wurden durch die Optimierung der Detektionsmechanismen durch eigene Erkenntnisse und Signaturen pro Tag im Mittelwert über 400 Angriffe auf die Regierungsnetze detektiert, die mit den eingesetzten kommerziellen Schutzprodukten nicht erkannt wurden. Hierunter fallen auch täglich ca. 20 hochspezialisierte Angriffe, die nur durch manuelle Analysen erkannt werden konnten. Durchschnittlich einer dieser Angriffe pro Woche hatte einen nachrichtendienstlichen Hintergrund.

2.1.1 Prävention, Detektion und Reaktion

Aufgrund der dynamischen Bedrohungslage und der zunehmenden Professionalisierung der Angreifer muss man heute davon ausgehen, dass die Netzgrenzen der IT-Systeme überwunden werden können. Daher sind neben der Prävention auch Maßnahmen der Detektion und Reaktion aufzusetzen, die im Falle eines erfolgreichen Angriffs greifen und die negativen Effekte des Angriffs minimieren. Eine weitere Schutzkomponente im Regierungsnetz blockiert daher ausgehende Netzverbindungen auf infizierte Webseiten, die Schadprogramme verteilen sowie Verbindungsversuche von bereits aktiven Schadprogrammen zu Kontrollservern, die für die Steuerung und den Datenabfluss genutzt werden. Diese Maßnahme wirkt zum einen präventiv und erkennt zum anderen bereits infizierte Systeme, bei denen die eingesetzten IT-Sicherheitsprodukte nicht gegriffen haben. In der ersten Jahreshälfte 2016 wurden mit dieser Methode bisher täglich rund 3.600 Verbindungsversuche zu Schadcodeservern blockiert.

Auffällig sind dabei 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.

Seit Anfang des Jahres wurden sechsmal aktive Schadprogramme detektiert, die kommerzielle Schutzsysteme unterlaufen haben, aber eindeutig einem kriminellen Zweck dienten. Diese niedrige Zahl an Infektionen ist auch zurückzuführen auf die engmaschigen E-Mail-Filter, die als Reaktion auf Ransomware-Kampagnen wie Locky eingerichtet wurden. Dadurch wurden auch andere Schadsoftware-Familien gefiltert, da diese teilweise dieselben Verbreitungsmechanismen wie Ransomware verwenden.

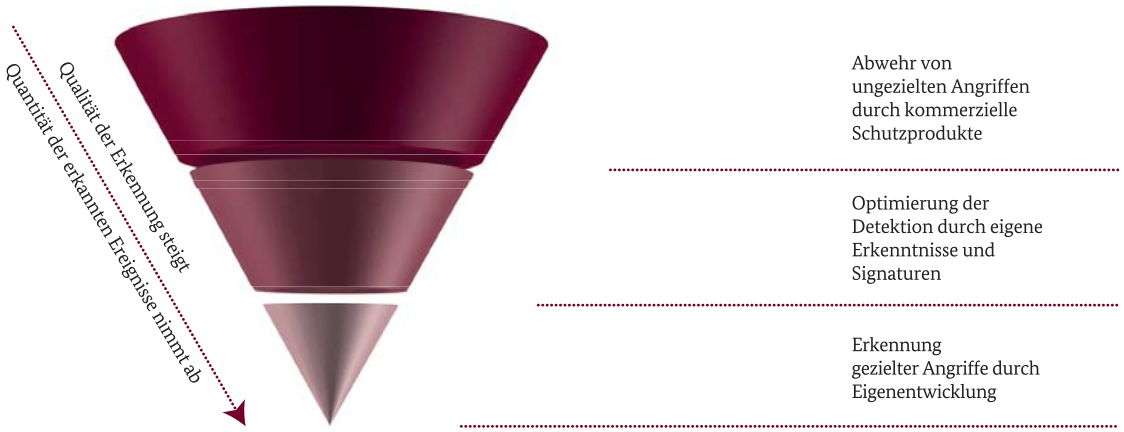


Abbildung 11: Gestufte Schutzmaßnahmen in den Regierungsnetzen gegen E-Mail-basierte Angriffe

2.2 Erkenntnisse aus Meldungen aus der Bundesverwaltung

Behörden der Bundesverwaltung müssen nach § 4 BSI-Gesetz gravierende Sicherheitsvorfälle unverzüglich und weniger kritische Vorfälle monatlich an das Lagezentrum des BSI übermitteln. Nicht alle Behörden der Bundesverwaltung sind an das Regierungsnetz mit seinen zentralen Schutzkomponenten angeschlossen.

Bis Ende Juni 2016 wurden in der Bundesverwaltung von kommerziellen Schutzprodukten rund 200 Schadsoftware-Infektionen pro Monat erkannt. Die Anzahl der auf den Endsystemen erfolgreich abgewehrten Schadprogramme lag im selben Zeitraum bei knapp 95.000 pro Monat.

Die Entwicklung der vergangenen Jahre zeigt Abbildung 12.

Die massiv verbreiteten Ransomware-Schadprogramme, die in vielen Organisationen zu Infektionen geführt haben, sind in den Bundesbehörden kaum bis zu den Endsystemen durchgedrungen. Die Mailserver der Regierungsnetze filtern verdächtige Anhänge heraus. Darüber hinaus erstellt das BSI aus beobachteten Schadprogramm-Kampagnen selbst Antiviren-Signaturen, die kurzfristig im Regierungsnetz aktiviert werden. Pro Monat wurden durchschnittlich 44.000 Schadprogramme aus dem Mailverkehr gefiltert.

Das BSI verzeichnete in den letzten Jahren stetig steigende Zahlen bei den gemeldeten Denial-of-Service (DoS)-Angriffen auf einzelne Webseiten der Bundesbehörden. Im Zeitraum von 2010 bis Mitte 2016 hat sich die Zahl der Angriffe, bei denen die jeweils betroffene Behörde unverzüglich um Unterstützung des BSI bittet, vervierfacht.

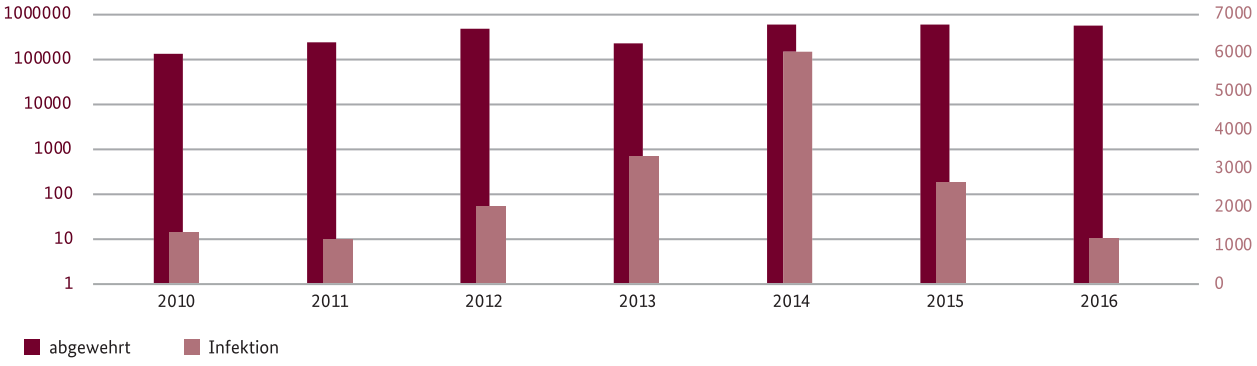


Abbildung 12 : Schadsoftware-Infektionen und abgewehrte Schadprogramme

2.3 Erkenntnisse aus der IT-Sicherheitsberatung des BSI

Die IT-Sicherheitsberatung des BSI ist die Anlaufstelle für Behörden zu allen Fragen der IT-Sicherheit. Aufgrund enger Behördenkontakte und der Mitarbeit in Arbeitsgremien erhält das Team der Sicherheitsberatung einen kontinuierlichen Einblick in die Lage der Informationssicherheit vor Ort. Kontaktstellen sind die IT-Sicherheitsbeauftragten (IT-SiBes) der Behörden, mit denen das BSI effiziente Abläufe bei der Beratung und Unterstützung zu Fragen der IT-Sicherheit etabliert hat.

Die Verantwortlichen für IT-Sicherheit stehen vor besonderen Problemen, wenn Technik, Funktionen und Nutzerverhalten aus dem Consumer-Bereich unverändert in den Arbeitsplatz übertragen werden. Eine sichere Umsetzung wird zudem erschwert, wenn persönliche Sonderlösungen beansprucht werden – wie spezielle Produkte oder „Bring Your Own Device“ – obwohl in der IT-Sicherheitsstrategie für eine Organisation andere Lösungen flächendeckend vorgesehen sind. Die Medienberichte über IT-Sicherheitsvorfälle und erfolgreiche Angriffe scheinen zur Sensibilisierung der Nutzer beizutragen, das Bewusstsein für die Notwendigkeit von mehr Sicherheitsmaßnahmen ist gestiegen. Es ist jedoch auch weiterhin eine elementare Herausforderung, auf die Umsetzung dieser Sicherheitsmaßnahmen hinzuwirken und dabei Einsicht und Akzeptanz zu schaffen.

Technik im Umbruch

Aus betriebswirtschaftlichen und administrativen Gründen werden Möglichkeiten der Konsolidierung und Virtualisierung diskutiert und neue Konzepte erstellt. Ganze Technikbereiche befinden sich im Umbruch. Bei Audits und Revisionen werden Sicherheitslücken besonders in verbreiteten Monokulturen von Betriebssystemen und Anwendungssoftware mit nachlässiger Konfiguration entdeckt. In vielen Behörden sind historisch gewachsene Netzstrukturen entstanden, die durch den Zusammenschluss von Netzen oder aufgrund sicherheitstechnischer Analysen von Netzwerkübergängen nun konsolidiert werden müssen. Der Zeitpunkt für eine Neukonzeptionierung ist besonders geeignet, wenn eine Vielzahl von Standardlösungen wie Betriebssysteme, Firewalls oder Produkte des Virenschutzes aufgrund von Alterung oder wegen Auslaufen des Supports ausgetauscht werden. Über die Beschaffung neuer Hard- und Software hinaus müssen dabei die Sicherheitskonzepte angepasst werden.

Informationssicherheitsmanagement (ISMS)

Historisch bedingt setzt sich Informationssicherheit häufig aus einer Sammlung von Einzelmaßnahmen zusammen. In vielen Organisationen fehlt derzeit noch ein strukturiertes ISMS mit ausreichendem Personal und klar geregelten Aufgaben und Kompetenzen. Ein elementares Problemfeld bildet nach wie vor die Schatten-IT, denn bei Sicherheitsvorfällen sind es häufig nicht intern geprüfte und freigegebene Geräte, die von den Angreifern erfolgreich als Einfallstor genutzt werden. Zahlreiche Behörden können die Kritikalität ihrer IT-gestützten Geschäftsprozesse nicht konkret angeben, etablierte Verfahren zur Analyse und Dokumentation werden selten angewendet. Unzureichend dokumentierte Prozesse können in akuten Sicherheitslagen fatale Folgen für eine gesamte Organisation haben.

IT-Sicherheitsbeauftragte

Es ist notwendig, dass IT-Sicherheitsteams ihrer verantwortungsvollen Aufgabe entsprechend mit genügend Personal ausgestattet werden. Finanzielle Entscheidungen über Ressourcen werden immer noch häufig zugunsten von Technik anstatt von Personal getroffen. Zur Abwehr von Angriffen reichen technische Maßnahmen jedoch allein nicht aus. Dem technischen Fortschritt aufseiten der Angreifer muss mit ebenso gut ausgebildeten IT-Sicherheitsexperten begegnet werden.

Fazit

Die Informationssicherheit in Behörden kann weiter verbessert werden, wenn das Personal sich in IT-Sicherheitsteams mit den IT-Risiken und zunehmender Komplexität kontinuierlich auseinandersetzt. Dazu gehört eine den Aufgaben angemessene personelle, technische und organisatorische Ausstattung. Eine Lösung bietet die „Arbeitshilfe zur Feststellung des Aufwandes und zur Planung des personellen Ressourceneinsatzes für IT-Sicherheitsteams“ des BSI, die auf der BSI-Webseite zur Verfügung steht.

IT-Sicherheitsvorfälle mit Auswirkungen auf die Bundesverwaltung

Das BSI-Lagezentrum verfügt im Rahmen des § 4 BSI-Gesetz (BSIG) als zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes über ein umfassendes Lagebild von IT-Sicherheitsvorfällen in der Bundesverwaltung. Im Meldeprozess haben die IT-Sicherheitsbeauftragten in den jeweiligen Behörden neben der formalen und statistischen Meldung von IT-Sicherheitsvorfällen auch die Möglichkeit, zusätzliche Unterstützung beim BSI anzufordern. Erfreulich ist, dass im Beobachtungszeitraum die Ausfälle von für den Rechenzentrumsbetrieb notwendiger Infrastruktur wie Stromversorgung und Klimatechnik zurückgegangen sind. Dies ist vermutlich durch eine Verbesserung der Ausfallsicherheit begründet, zum Beispiel durch redundante Versorgung.

DDoS-Angriffe legen Webseiten lahm: DDoS-Angriffe auf Webseiten der Bundesverwaltung waren die am häufigsten vorkommenden IT-Sicherheitsvorfälle mit größeren Auswirkungen. DDoS-Angriffe gehören zu den alltäglichen Vorfällen im Internet. Im Gegensatz zu den Angriffen auf die Webseiten der Bundesregierung und des Deutschen Bundestags mit stark variierendem Angriffsverkehr im Januar 2015 ließen sich die Angriffe im aktuellen Berichtszeitraum nach Erkennung verhältnismäßig einfach durch DDoS-Gegenmaßnahmen abwehren, etwa in Form einer selektiven Filterung und der Erzwingung standardkonformen Protokollverhaltens. DDoS-Erpressungen, wie sie bei Unternehmen oder bei kommunalen Einrichtungen zu verzeichnen waren, gingen in der Bundesverwaltung nicht ein.

Missbrauch von Telefon- und Videokonferenzanlagen: Auffallend war im Berichtszeitraum der Anstieg von Missbrauchsvorfällen von Telefon- und Videokonferenzanlagen. Durch illegitime Auslandstelefonate entstanden finanzielle Schäden, die in Einzelfällen im fünfstelligen Bereich lagen. Ursächlich waren in den beobachteten Fällen entweder Sicherheitslücken in der Software oder unsicher konfigurierte Telefon-/Videokonferenzanlagen mit einfach zu erratenden PINs und aktivierter möglicher Rufweiterleitung. Es handelte sich jeweils nicht um gezielte Angriffe, sondern um automatisierte Wahlversuche, die Rufnummernblöcke durchlaufen und nach anfälligen Video-/Telefonkonferenzanlagen suchen. Die gleiche Problematik besteht bei unsicher konfigurierten Voice-over-IP (VoIP)-Diensten, die häufig das Ziel von VoIP-spezifischen Session Initiation Protocol (SIP)-Scans sind. Das Testen von Rufnummernblöcken und die Durchführung von SIP-Scans gehören inzwischen ebenso zum Hintergrundrauschen in IP-/Telefonnetzen wie SSH- / RDP- / SMB-Brute-Force-Scans.

E-Mails und Anrufe im Namen von Behörden: Im Berichtszeitraum sind durch Spammer gehäuft E-Mails im Namen von Behörden an Bürger und Unternehmen versendet worden. Der Inhalt der E-Mails reichte dabei von Spam bis hin zu präparierten Links, die auf Webseiten mit Schadcode verwiesen. Die Spammer verwendeten dabei bewusst einen Absender aus dem Namensraum von Behörden, um das Interesse des Empfängers zu erhöhen. E-Mail-Administratoren von Behörden bemerkten die Verwendung ihrer Domains, da sie mehrfach Nichtzustellbarkeitsmeldungen von Opfern erhielten, deren Postfach nicht (mehr) existierte. Um die E-Mail-Server-Validierung zu fördern und die Erkennung von gefälschten E-Mails zu verbessern, bietet das BSI den an die Netze der Bundesverwaltung angeschlossenen Behörden die folgenden Dienste an:

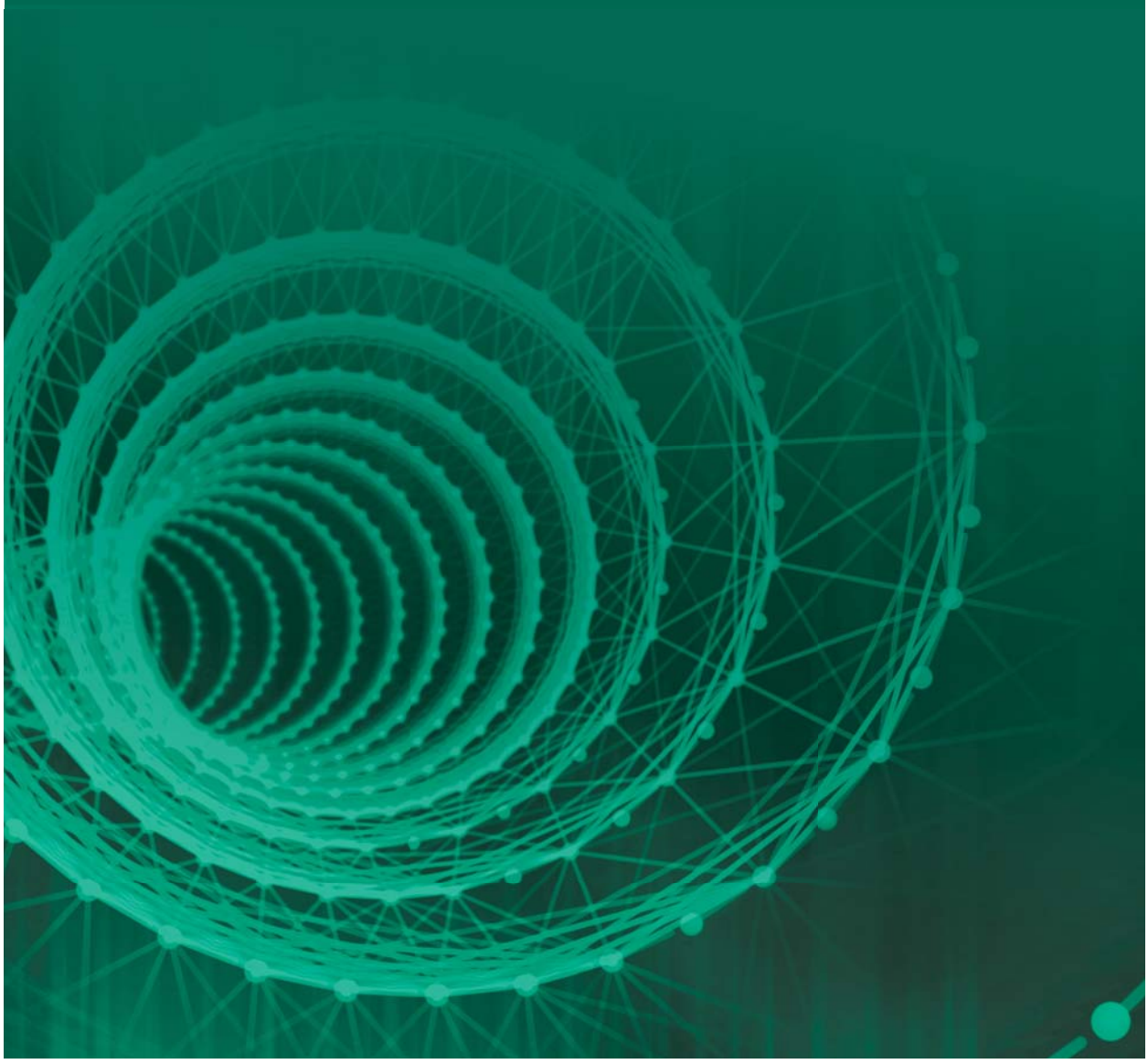
- „DNS-based Authentication of Named Entities“ (DANE) zur Validierung von E-Mail- und Web-Server-SSL-Zertifikaten (standardmäßig aktiv für die Domain *.bund.de),
- „Sender Policy Framework“ (SPF) zur Vermeidung von Adressfälschungen im E-Mail-Verkehr
- „DomainKeys Identified Mail“ (DKIM) ebenfalls zur Vermeidung von Adressfälschungen.

In der Vergangenheit traten ähnliche Vorfälle auch bei der Telefonie auf, indem Dritte mittels sogenannten Call ID Spoofings durch präparierte VoIP-Telefonanlagen die beim Angerufenen im Display angezeigte Rufnummer fälschten und so den Eindruck erweckten, der Anruf käme von einer Behörde. Hintergrund war in diesen Fällen oft Vorschussbetrug.

Schwachstellen in Webanwendungen: Aufgrund der hohen Entwicklungs- und Änderungsdynamik im Bereich von Webanwendungen werden bei neuen und teilweise auch bei bestehenden Webanwendungen der Bundesverwaltung Schwachstellen entdeckt, die sich potenziell ausnutzen lassen. Die Entdeckung erfolgt sowohl durch interne Penetrationstests als auch durch die Hinweise Dritter. Bei Entdeckung einer Schwachstelle in einer Webanwendung kontaktiert das BSI die Ansprechpartner in der betroffenen Behörde und unterstützt bei Bedarf die Behebung. Die in Webanwendungen entdeckten Schwachstellen und unsicher konfigurierten Internetdienste sowie Botnetz-Infektionen verdeutlichen die Bedeutung der Prüfung der eigenen Dienste zur Vermeidung von Sicherheitsvorfällen.

Unsichere Konfiguration von Server-Diensten und Schadprogramm-Infektionen: Das CERT-Bund des BSI erhält aus vertrauenswürdigen Quellen regelmäßig Informationen zu unsicher konfigurierten Server-Diensten, beispielsweise zu offenen DNS-Resolvern oder NoSQL-Datenbanken, sowie zu Schadprogramm-Infektionen auf Systemen, welche auf Basis der IP-Adressen Deutschland zugeordnet werden. Neben den zuständigen Netzbetreibern sowie den für die Benachrichtigung registrierten KRITIS-Unternehmen und Landesverwaltungen kontaktiert CERT-Bund bei einer Betroffenheit in der Bundesverwaltung die jeweils zuständigen IT-Sicherheitsbeauftragten mit dem Ziel der sicheren Konfiguration des Server-Dienstes bzw. der Bereinigung der Schadprogramm-Infektion.

3 Gefährdungslage KRITIS



3 Gefährdungslage KRITIS

3.1 Überblick

Kritische Dienstleistungen wie die Versorgung mit Trinkwasser oder Strom, aber auch der reibungslose Ablauf von logistischen Prozessen und die Nahrungsmittelproduktion sind immer stärker von funktionierender Informations- und Kommunikationstechnik (IKT) abhängig. Grundsätzlich sind KRITIS-Betreiber dabei den gleichen Gefahren ausgesetzt wie andere Unternehmen. Das Risiko liegt bei KRITIS-Betreibern jedoch meist auf deutlich höherem Niveau, da Störungen der IKT leicht zu Beeinträchtigungen oder Ausfall der Versorgungsdienstleistungen führen können.

Im Berichtszeitraum hat das BSI verschiedene Gefährdungen für Kritische Infrastrukturen beobachtet, die in besonderer Häufung oder mit herausragender Auswirkung auftraten:

- Auch Kritische Infrastrukturen sind von Ransomware betroffen. Neben einer Vielzahl von kleineren Störungen sind dabei insbesondere die Fälle öffentlich bekannt geworden, in denen Krankenhäuser und andere Einrichtungen des Gesundheitswesens betroffen waren.

  Betroffene Kritische Dienstleistung:
  Gesundheitsversorgung

- In der Ukraine ereignete sich im Dezember 2015 ein Stromausfall, der offenbar Folge eines koordinierten Cyber-Angriffs auf mehrere Energienetzbetreiber war. Betroffen waren ca. 225.000 Einwohner (vgl. Vorfall: „Stromausfall in der Ukraine“, S. 40).

  Betroffene Kritische Dienstleistung:
  Stromversorgung

Cyber-Angriffe auf das SWIFT-System

Sachverhalt: Im Verlauf des ersten Halbjahres 2016 wurden mehrere Vorfälle bekannt, in denen sich Unbekannte einen nicht autorisierten Zugang zu Kommunikationsdienstleistungen der „Society for Worldwide Interbank Financial Telecommunication“ (SWIFT) verschafft haben. So berichtete das philippinische Nachrichtenportal „Inquirer.net“ im März über einen Cyber-Bankraub. Demnach gelang es den Angreifern, 81 Millionen US-Dollar der Zentralbank von Bangladesch unautorisiert abfließen zu lassen. Der Versuch einer weiteren Transaktion über 830 Millionen US-Dollar wurde vorzeitig erkannt und unterbunden. Es folgten weitere Berichte über einen Angriffsversuch auf eine vietnamesische Bank sowie erfolgreiche Angriffe gegen die ecuadorianische Banco del Austro (Schaden: 12 Millionen US-Dollar) sowie eine ukrainische Bank (Schaden: 10 Millionen US-Dollar).

Methode: Erstes Ziel der Angreifer ist es, in die Kernbankensysteme der betroffenen Banken vorzudringen. Dabei werden gängige Angriffsmethoden verwendet, wie sie auch in anderen Zusammenhängen beobachtet werden, zum Beispiel SpearPhishing oder Watering-Hole-Angriffe. Als Nächstes versuchen die Angreifer, gültige Authentifizierungsdaten für den Zugang zur SWIFT-Kommunikationsinfrastruktur „SWIFTNet“ abzuschöpfen. Damit eignen sich die Angreifer dieselben Berechtigungen zur Nutzung dieses Netzwerks an, wie sie auch der angegriffenen Bank selbst zur Verfügung stehen. Anschließend treffen die Angreifer Maßnahmen in der kompromittierten Bank, die zur Verschleierung von Transaktionen dienen. Über das SWIFTNet können nunmehr Nachrichten an andere Banken versendet werden. Diese haben das Ziel, beim Adressaten eine Überweisung auszulösen. Um das Zurückholen des Geldes zu verhindern, muss es dann von den Angreifern aus dem Zahlungsverkehrssystem ausgeleitet und „gewaschen“ werden.

Schadenswirkung: Insgesamt kam es allein bei den drei oben genannten erfolgreichen Angriffen zu finanziellen Schäden von insgesamt 103 Millionen US-Dollar.

Zielgruppen: Die Angriffe richten sich gegen Finanzinstitute in aller Welt.

Technische Fähigkeiten: Für den Erfolg eines solchen Angriffs sind umfangreiche Kenntnisse der Finanzbranche und der Zielunternehmen notwendig sowie eine umfangreiche Logistik für Vorbereitungen und Geldwäsche. Aus technischer Sicht ist der Angriffsvektor nicht neu, für die Durchführung sind keine besonderen technischen Fähigkeiten notwendig. Den Angreifern ist es gelungen, mit gängigen Angriffsmethoden, wie sie auch in vielen andern Fällen von Kriminellen eingesetzt werden, erfolgreich zu sein.

- In Deutschland kam es zu drei größeren Störungen bei IKT-Providern, die jeweils zwischen 750.000 und 2,7 Millionen Einwohner betrafen und bei diesen zum Ausfall von Internetzugang, Telefonie oder Mobilfunk führten.

  Betroffene Kritische Dienstleistung:
  Sprach- und Datenübertragung

Durch das hohe Schadenspotenzial sind Kritische Infrastrukturen ein Ziel für politisch motivierte Angreifer wie Hacktivisten, Nachrichtendienste oder Terroristen. Aber auch Kriminelle entdecken zunehmend KRITIS als Ziel: Erpressungsmethoden wie DDoS und Krypto-Ransomware betreffen grundsätzlich alle Sektoren und Branchen. Erpressungsversuche mit der Androhung eines DDoS zielen jedoch meist auf Unternehmen aus dem Sektor „Finanz- und Versicherungswesen", da hier häufig Kundenportale genutzt werden und damit eine direkte Verwundbarkeit gegeben ist.

Die Hürde zur Absicherung von bereits bekannten Schwachstellen liegt bei den in Kritischen Infrastrukturen – wie auch in anderen Industriezweigen – eingesetzten industriellen Steuerungssystemen deutlich höher als bei konventioneller Büro-IT. Geschäfts- und versorgungskritische Infrastruktursysteme oder Fachsysteme können oft nicht mit Sicherheitsupdates versorgt werden und weisen zum Teil Lebenszyklen auf, die die der handelsüblichen Büro-IT weit übersteigen. Betreiber solcher Systeme sind somit oft gezwungen, alternative Wege zur Absicherung verwundbarer Systeme zu finden.

Ransomware im Krankenhaus

Sachverhalt: : Im Februar 2016 brachten Unbekannte ein Schadprogramm in das interne Netz des Lukaskrankenhauses in Neuss ein. Dieses Schadprogramm führte zeitnah zu Störungen in IT-Systemen und behinderte auch die Behandlung von Patienten. Zur Vermeidung möglicher weiterer Schäden, insbesondere der Kompromittierung von Patientendaten, und zur Analyse der Störungen wurde das interne Computer-Netzwerk heruntergefahren.
Die Analyse ergab, dass ein Ransomware-Trojaner Ursache der Störung war. Das Schadprogramm hinterließ vereinzelt Hinweise, wie das Krankenhaus die für die Wiederherstellung der Daten notwendigen kryptografischen Schlüssel bekommen könnte. Da das Netzwerk allerdings unmittelbar nach den ersten Auffälligkeiten heruntergefahren worden war, wurde nur ein sehr kleiner Anteil der gesamten Datenmenge verschlüsselt.
Das Krankenhaus entschied sich gegen eine Lösegeldzahlung und stellte nach der Überprüfung aller Server und Rechner mit einer neu geschriebenen Anti-Schadsoftware die Daten aus den verfügbaren Backups wieder her. Das BSI hat das Krankenhaus vor Ort bei der Analyse und Bewältigung des Vorfalls unterstützt.

Methode: Das Eindringen von Schadprogrammen in interne Netze ist schon allein deshalb nicht auszuschließen, weil in gängigen Programmen immer wieder Schwachstellen gefunden werden, die durch Angreifer ausgenutzt werden können. Ausnutzbar werden diese Schwachstellen, weil die Durchdringung der Gesellschaft durch IT in nahezu allen größeren Organisationen zu einer Vielzahl komplexer Kommunikationsverbindungen geführt hat – und zwar auch unter Verwendung des Internets mit Rechnern, die unter der Kontrolle böswilliger Dritter stehen. Die Schutzmechanismen von Computer-Netzwerken müssen also darauf ausgerichtet sein, dass ein erfolgreicher Angriff auf ein einzelnes internes System nicht sofort Auswirkungen auf das gesamte Netzwerk hat. Im konkreten Fall konnte das Schadprogramm mit wenig Aufwand weitere IT-Systeme schädigen, da die internen Schutzmechanismen dem infizierten System vertrauten.

Schadenswirkung: Im Krankenhaus gab es keinen Schaden an Leib und Leben, da der Betrieb auch ohne umfassende IT-Unterstützung weitergeführt werden konnte. Aber allein die Kosten für die Analyse des Angriffs und die Wiederherstellung des IT-Betriebs werden von der Geschäftsführung des Lukaskrankenhauses mit einem Betrag in Höhe von ca. 1 Million Euro angegeben.

Technische Fähigkeiten: Angreifer können sich Ransomware am Markt einkaufen und Lösegeldzahlungen anonym über das Internet abwickeln, sodass sie für ihre Angriffe kein ausgeprägtes Fachwissen benötigen. Die Spezialisten hinter solchen Angriffen sind die Programmierer der Schadsoftware, die immer wieder Methoden finden, Schutzmechanismen zu umgehen.

Stromausfall in der Ukraine

Sachverhalt: Am 23. Dezember 2015 wurden zwischen 16:00 und 17:00 Uhr Ortszeit mindestens drei Stromverteilnetzbetreiber in der Ukraine Opfer eines gezielten Cyber-Angriffs.

Ursache: Hinter den Angriffen wird die Sandworm-Gruppe vermutet, die bereits früher durch Cyber-Angriffe mit der Schadsoftware BlackEnergy in Verbindung gebracht wurde. Es gelang den Angreifern, Schadsoftware auf Systemen mit veralteten Softwareständen aufzuspielen und zur Ausführung zu bringen. Mutmaßlich kamen hierbei SpearPhishing-E-Mails zum Einsatz, die Mitarbeiter der Betreiber zum Öffnen der schadhaften Anhänge bewogen haben.

Methode: Der genaue Zeitpunkt der initialen Infektion ist nicht bestimmt worden, es wird jedoch von ähnlichen Angriffen mittels SpearPhishing im Frühjahr 2015 auf andere Betreiber im Energiesektor der Ukraine berichtet. Nach der Erstinfektion erlangten die Angreifer schrittweise Kontrolle über weitere Rechnersysteme im angeschlossenen Netz des Betreibers, bis hin zu den Systemen, auf denen die eigentliche Steuerungssoftware für die Umspannwerke bzw. Schaltanlagen ausgeführt wird. Hierbei kamen unterschiedliche Versionen der Schadsoftware-Familie BlackEnergy zum Einsatz, die für jeweils spezialisierte Zwecke genutzt wurden. In den verschiedenen BlackEnergy-Versionen wurden unterschiedliche Module für spezifische weitere Funktionen genutzt. Hierunter fällt auch die eher neue, sogenannte „KillDisk-Komponente“, die im späteren Verlauf des Angriffs maßgeblich zur Erschwerung der Störungsbeseitigung beigetragen hat.
Beim eigentlichen Angriff am 23. Dezember 2015 haben die Angreifer verschiedene Schritte zum Herbeiführen, Verschleiern und Erschweren der Beseitigung der Störung sehr koordiniert durchgeführt. Im ersten Schritt wurden die eigentlichen Hochspannungsleistungsschalter der etwa 30 Umspannwerke bzw. Schaltanlagen durch eine eingeschleuste Fernwartungssoftware geöffnet, was unmittelbar zum Ausfall der Stromversorgung bei den Betroffenen geführt hat. Gleichzeitig wurden die Überwachungssysteme der Netzleitstellen „eingefroren“ bzw. abgeschaltet, sodass die Störung hier nicht feststellbar war. Die im zweiten Schritt auftretende Überlastung der Telefonleitungen wird einem TDoS-Angriff (Telephone Denial of Service) auf mindestens ein Callcenter eines Verteilnetzbetreibers zugeschrieben, wodurch telefonische Störungsmeldungen durch Betroffene verhindert wurden. Im dritten Schritt wurde die KillDisk-Komponente eingesetzt. Dieses Modul löscht Daten auf Windows-Systemen und macht damit das Betriebssystem unbrauchbar, was ein Wiederherstellen der Funktionsbereitschaft und eine Analyse des Vorfalls deutlich erschwerte. Darüber hinaus wurde die Firmware auf Seriell-Ethernet-Konvertern überschrieben, die die Schnittstelle zwischen Anlagensteuerung und Steuerungssoftware bilden, wodurch diese effektiv zerstört wurden. Auch wurden die Unterbrechungsfreien Stromversorgungen (USV) der Server von den Angreifern über die Management-Schnittstellen abgeschaltet, wodurch die Störungsbeseitigung weiter erschwert und verzögert wurde.

Schadenswirkung: Mindestens 225.000 Einwohner der Ukraine waren von einem mehrstündigen Ausfall der Stromversorgung betroffen. Aufgrund der Sabotage der im Regelbetrieb für die Fernsteuerung der Umspannwerke genutzten Leittechnik mussten die Schaltvorgänge vor Ort in den Umspannwerken manuell ausgelöst werden. Dadurch wurde die Wiederherstellung der Stromversorgung deutlich verzögert.
Zielgruppen: Die Schadsoftware BlackEnergy wurde bisher unter anderem gegen Organisationen aus den Sektoren Energie sowie Transport und Verkehr eingesetzt. Bei derartig zielgerichteten Angriffen auf Kritische Infrastrukturen ist die Zielgruppe jedoch nicht nur der Betreiber selbst, sondern – zumindest indirekt – auch die Bevölkerung.

Technische Fähigkeiten: Die technischen Fähigkeiten der Täter sind als hoch einzuschätzen. Zwar ist die eingesetzte Schadsoftware nicht sehr ausgefeilt, beispielsweise wurden keine Zero-Day-Schwachstellen ausgenutzt. Die Angreifer konnten sich jedoch über einen langen Zeitraum unbemerkt im Computernetz der Opfer ausbreiten und ihren Angriff vorbereiten. Die Täter gingen äußerst koordiniert vor und benutzten mehrere Angriffstechniken, um ihren Angriff zu verschleiern und eine Störungsbehebung zu erschweren.

3.1.1 Erkenntnisse aus Meldungen nach IT-Sicherheitsgesetz

Mit Inkrafttreten des IT-Sicherheitsgesetzes im Juli 2015 sind verschiedene Meldepflichten für KRITIS-Betreiber eingeführt worden. Für die meisten Betreiber jedoch werden diese erst einige Zeit nach Inkrafttreten der BSI-Kritisverordnung relevant. Unmittelbar mit Inkrafttreten des Gesetzes besteht die Meldepflicht nur für jenen Teil der KRITIS-Betreiber, der gemäß Atomgesetz, Energiewirtschaftsgesetz oder Telekommunikationsgesetz zu Meldungen verpflichtet ist. Für die sonstigen Betreiber wird die Meldepflicht gestaffelt eingeführt, sodass voraussichtlich erst Ende 2017 sämtliche Betreiber Kritischer Infrastrukturen meldepflichtig sein werden..

Im aktuellen Berichtszeitraum wurden dem BSI drei große Störungen bei IKT-Providern gemeldet. Insgesamt sind allein durch diese drei Störungen ca. 36 Millionen Nutzerstunden Telefonie bzw. Internetzugang ausgefallen. Die umfangreichste Störung umfasste allein 27 Millionen Nutzerstunden und betraf den Mobilfunkbereich. Alle drei Störungen hatten ihre Ursache in Beeinträchtigungen der Verfügbarkeit von zentralen Authentifizierungs- bzw. Routingkomponenten.

In einer kerntechnischen Anlage wurden im Rahmen einer Routinerevision zwei Schadprogramme auf USB-Datenträgern und einem Computer zur Steuerungsvisualisierung entdeckt (vgl. Vorfall: „Schadsoftware im Atomkraftwerk“, S. 20).

Ferner wurden zwei Vorkommnisse in anderen KRITIS-Sektoren gemeldet, die aber die Erbringung der kritischen Versorgungsleistungen nicht beeinträchtigten. Auch hier waren Software- und Hardwareprobleme Ursache der Störungen.

3.2 Erkenntnisse aus dem UP KRITIS

Im Rahmen des UP KRITIS hat das BSI im Frühjahr 2016 eine Umfrage zur Betroffenheit durch Ransomware im deutschen Gesundheitswesen durchgeführt. Die Deutsche Krankenhausgesellschaft hat hierzu eine Reihe von Rückmeldungen veranlasst, auf deren Grundlage das BSI eine Einschätzung zur Lage vornehmen konnte.

Erwartungsgemäß hat der überwiegende Teil der Betreiber versuchte Angriffe mittels Ransomware beobachten können. Diese waren jedoch nur bei einem Teil der Betreiber erfolgreich. In einer Betroffenheitsabfrage durch das BSI äußerten die Betreiber, dass bei der überwiegenden Menge der überhaupt erfolgreichen Angriffe die Störung innerhalb weniger Stunden beseitigt werden konnte und die Erbringung der kritischen Versorgungsdienstleistung zu keinem Zeitpunkt gefährdet war. Dies zeigt, dass die Krankenhäuser, zumindest in dieser Stichprobe, sich der Gefahr bewusst sind und effektive Gegenmaßnahmen einsetzen. Dennoch ist Ransomware ein ernst zu nehmendes Problem, da es ohnehin schon begrenzte Ressourcen der IT-Abteilungen bindet und es je nach Funktion des befallen Systems zu erheblichen Störungen kommen kann.

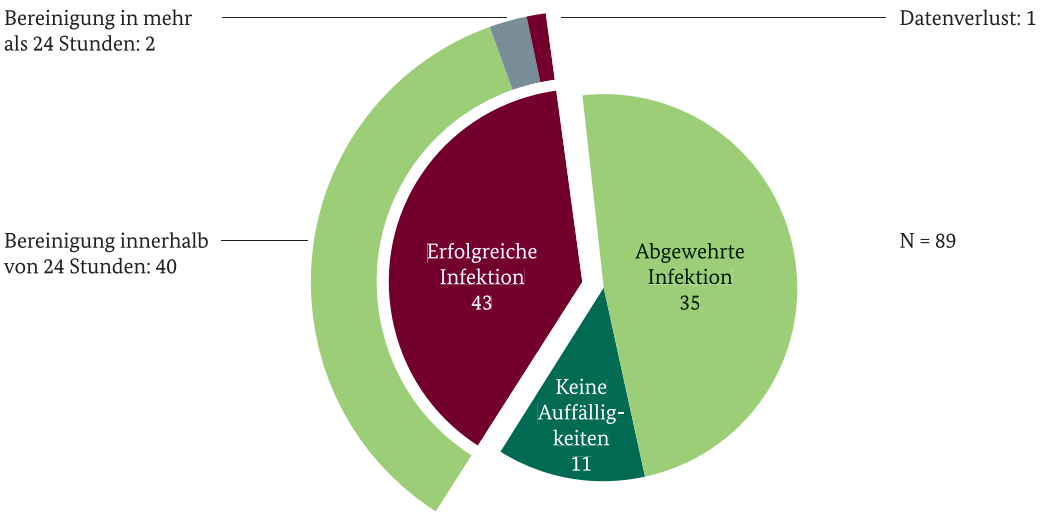
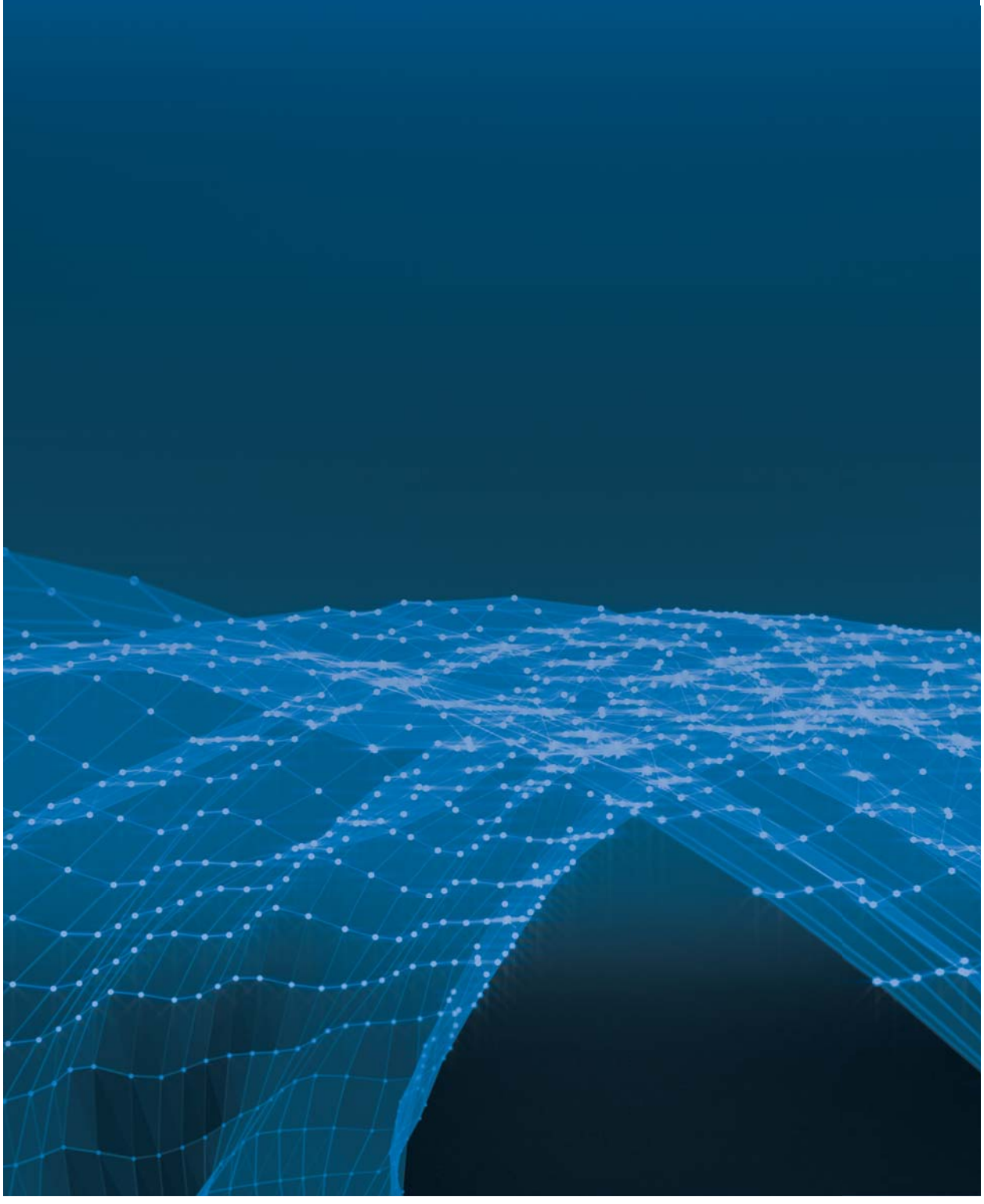


Abbildung 13: Ergebnisse der Umfrage zur Betroffenheit durch Ransomware im deutschen Gesundheitswesen

4 Cyber-Sicherheit gestalten



4 Cyber-Sicherheit gestalten

Als nationale Cyber-Sicherheitsbehörde trägt das Bundesamt für Sicherheit in der Informationstechnik einen wesentlichen Teil zur erfolgreichen Gestaltung der IT-Sicherheit in Deutschland für Staat, Wirtschaft und Gesellschaft bei. Anhand einiger ausgewählter Themenfelder werden im folgenden Kapitel Kernthemen und Lösungsansätze des BSI beleuchtet.

4.1 IT-Sicherheit für Staat und Verwaltung

4.1.1 IT-Konsolidierung des Bundes

Basierend auf Entscheidungen des Haushaltsausschusses des Deutschen Bundestages und des Bundeskabinetts werden im Rahmen des ressortübergreifenden Projekts „IT-Konsolidierung Bund“ unter der Gesamtprojektleitung des Bundesinnenministeriums große Teile der Informationstechnik des Bundes in zentralen Rechenzentren zusammengefasst. Die IT-Konsolidierung hat unter anderem zum Ziel, das IT-Sicherheitsniveau in der Bundesverwaltung signifikant zu erhöhen. Dies kann vor allem erreicht werden, wenn bei den Planungen zu den Infrastrukturen und Diensten risikoadäquate Sicherheitsmaßnahmen berücksichtigt und im Betrieb umgesetzt werden (u. a. Umsetzung geltender und zukünftiger Sicherheitsstandards).

Im Projekt „IT-Konsolidierung Bund“ hat das BSI den Auftrag, den Konsolidierungsprozess durch Analysen, Entwicklung von Sicherheitsmaßnahmen und konzeptionelle Beratung sicherheitstechnisch zu begleiten sowie dauerhaft zur Sicherheit der konsolidierten IT beizutragen. Dazu nimmt das BSI folgende Aufgaben wahr:

- Analyse des IT-Sicherheitsniveaus aller Rechenzentren der Bundesverwaltung
- Erarbeitung adäquater Sicherheitsmaßnahmen für die Rechenzentren des Bundes
- Informationssicherheitsberatung der Rechenzentren des Bundes, insbesondere des Informationstechnik-Zentrums Bund (ITZBund)
- Informationssicherheitsberatung der zu konsolidierenden Behörden zu Sicherheitsaspekten
- Unterstützung bei der Sicherheitskonzeption der Bundescloud
- Erarbeitung einer IT-Sicherheitsrichtlinie

Im Berichtszeitraum hat das BSI im Rahmen einer Pilotierung 15 Rechenzentren der sechs zentralen IT-Dienstleistungszentren (DLZ) des Bundes hinsichtlich ihres IT-Sicherheitsniveaus untersucht. Die Untersuchung erfolgte mit dem vom BSI entwickelten Bewertungsschema „HV-Benchmark“, mit dessen Hilfe Verlässlichkeit und IT-Sicherheit von IT-Dienstleistern und Rechenzentren mit vergleichsweise geringem Aufwand analysiert und bewertet werden können. Die Ergebnisse der Untersuchung liefern den Betreibern der DLZ, der Gesamtprojektleitung des Vorhabens „IT-Konsolidierung Bund“ und dem BSI wichtige Erkenntnisse zur IT-Sicherheit innerhalb der unmittelbaren Bundesverwaltung und geben Hinweise für die Optimierung der IT-Sicherheit sowie für die Ertüchtigung der Rechenzentren. Nachdem die Pilotierung bei den sechs DLZ erfolgreich abgeschlossen ist, wird die Sicherheitsanalyse in zwei Schritten auf alle Rechenzentren der Bundesverwaltung ausgeweitet.

Das BSI erarbeitet gemeinsam mit dem ITZBund Sicherheitsmaßnahmen, die es erlauben, die Vorteile einer zentralisierten IT-Dienstleistungserbringung zu nutzen und dabei gleichzeitig die hohen Anforderungen an IT-Sicherheit der vom Bund verarbeiteten Daten zu gewährleisten. Darüber hinaus berät das BSI die Gesamtprojektleitung und die Teilprojekte des Vorhabens „IT-Konsolidierung Bund“ zu Fragen der IT-Sicherheit, etwa zur sicheren Überführung des IT-Betriebs in die zentralen Rechenzentren oder zur Sicherheit zentraler Konsolidierungsprojekte (zum Beispiel Entwicklung und Einführung des Basisdiensts E-Akte oder die Einführung eines Bundesclients). Zudem ist angedacht, dem BSI hinsichtlich des Informationssicherheits-Managements für die IT-Konsolidierung Bund eine zentrale Rolle zuzuweisen. Einzelheiten werden derzeit in der IT-Sicherheitsleitlinie und im übergreifenden Managementsystem für Informationssicherheit für die IT-Konsolidierung Bund festgelegt.

4.1.2 Schutz der Regierungsnetze/Schutz der Bundesverwaltung

Gemäß BSI-Gesetz ist die Abwehr von Gefahren für die IT des Bundes eine Kernaufgabe des BSI. Seit seiner Gründung hat das BSI die Aufgabe wahrgenommen, die Netze der Bundesverwaltung zu schützen. Wichtigste Sicherheitsmaßnahmen des zentralen Regierungsnetzes sind eine durchgängig verschlüsselte Kommunikation und eine robuste, redundante Architektur. Die Maßnahmen des BSI

zum Schutz der Regierungsnetze unterliegen einer kontinuierlichen Überprüfung, Weiterentwicklung und Anpassung an die dynamische Bedrohungslage.

Aktuelle Angriffe zeigen, dass flache Hierarchien in Netzen und nicht ausreichende Segmentierungsmaßnahmen zwischen Diensten und Nutzern erhebliche Sicherheitsrisiken darstellen. Daher hat das BSI für die Regierungsnetze eine gesamtheitliche Strategie zur Segmentierung entwickelt, welche im Rahmen des Projekts „Netze des Bundes“ unter Berücksichtigung der Anforderungen des Projekts „IT-Konsolidierung Bund“ umgesetzt werden sollte. Neben der Segmentierung zwischen internem und externem Bereich geht es hierbei auch um die Subsegmentierung nach Organisationsstrukturen und gleichartigen funktionalen Bereichen. Nur durch eine wirksame Trennung mit zuverlässigen Mechanismen können die Auswirkungen bei einem erfolgreichen Angriff begrenzt und eine schnellstmögliche Wiederherstellung des Betriebs gewährleistet werden. Auch die Absicherung der Übergänge zwischen Segmenten auf einem einheitlich hohen Niveau ist eine wesentliche Aufgabe, die bereits bei der Planung von Netzen und Rechenzentren berücksichtigt werden muss, so beispielweise beim Übergang von externen in interne Netze im Fall von Fernwartungsdiensten durch Dritte.

Viele IT-Dienstleister bieten Fernwartung als Supportleistung an, da diese meist eine Kostenersparnis und eine schnellere Reaktionsfähigkeit verspricht. Fernwartung bringt jedoch auch viele Risiken mit sich. Das BSI hat daher Anforderungen für einen sicheren zentralen Fernwartungsdienst erarbeitet, die neben den Sicherheitseigenschaften besonders auch die Betriebsanforderungen berücksichtigen. Der Dienst soll die Vertraulichkeit und Integrität der sensiblen Daten der Fernwartungstätigkeit mit ausreichend starken kryptografischen Verfahren schützen, wobei die zentralen Komponenten durch den Bund selbst betrieben werden. Des Weiteren soll sichergestellt sein, dass die Behörden sehr differenziert festlegen können, auf welche Systeme der Fernwartungs-Dienstleister Zugriff haben darf. Auch die Kontrolle über den eigentlichen Zugriff und eine Live-Beobachtung und Aufzeichnung sämtlicher Aktivitäten soll durch den Dienst ermöglicht werden. Obwohl die Fernwartung von Systemen immer ein zusätzliches Risiko darstellt, kann durch zukünftige Verwendung dieses Dienstes eine sichere technische Lösung verwendet werden. In Verbindung mit einer organisatorisch geregelten fachlichen Überwachung der Tätigkeit besteht die Möglichkeit, die Restrisiken auf ein vertretbares Niveau zu senken.

IT-Sicherheitsbeauftragte: Zertifizierte Kompetenz

In Zusammenarbeit mit der Bundesakademie für öffentliche Verwaltung (BAköV) bietet das BSI Kurse zur Aus- und Fortbildung zum „Zertifizierten IT-Sicherheitsbeauftragten“ an. Die Fortbildung umfasst fachlich modulare IT-Sicherheitsthemen. Der vermittelte Lernstoff wird über eine Prüfung abgefragt. Zudem sind eine Projektarbeit und deren Präsentation vor einem Prüfungsausschuss Bestandteile der Prüfungsordnung. Der „Leitfaden IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung“ enthält Informationen und Vorlagen zur Vorbereitung und Durchführung der Fortbildung und Zertifizierung.

Das BSI unterstützt die BAköV bei der Konzeption und Durchführung einer Schulungsreihe für IT-Sicherheitsbeauftragte in Behörden. Das Jobprofil „IT-Sicherheitsbeauftragter“ definiert Verantwortlichkeiten und Kompetenzen, die den Absolventinnen und Absolventen nach erfolgreicher Ausbildung mit einem Zertifikat bestätigt werden. Zielgruppe der Fortbildung sind Teilnehmer aus Bundes- und Landesbehörden.

Die Ausbildungsinhalte und der Ausbildungsgang für behördliche IT-Sicherheitsbeauftragte haben Vorbildcharakter für die Wirtschaft und werden dort auch aufgenommen. Einige Hochschulen haben Curriculum und Handbuch übernommen und vermitteln die Lehrinhalte im Umfang eines Semesters. Die von den Hochschulen vergebenen Zertifikate basieren auf identischen Prüffragen der BAköV-Kurse. Die Erstellung einer Projektarbeit sowie die Präsentation sind auch an den Hochschulen Voraussetzung für den Erwerb des Zertifikates. Seit Bestehen der Fortbildung zum zertifizierten IT-Sicherheitsbeauftragten (2007) haben 246 Personen erfolgreich das Zertifikat erlangt, im Berichtszeitraum 2015/2016 waren es 27 Personen.

Für die IT-Sicherheitsbeauftragten in der öffentlichen Verwaltung bietet das BSI unterjährige Informationsveranstaltungen zum Erfahrungsaustausch sowie themenspezifische Workshops an und begleitet die BAköV mit fachlichen Beiträgen bei der Planung und Durchführung der Jahrestagung für IT-Sicherheitsbeauftragte von Bundesbehörden.

In enger Zusammenarbeit mit CERT-Bund und dem Nationalen IT-Lagezentrum erhalten die IT-Sicherheitsbeauftragten Informationen, Sicherheitshinweise und Warnungen über etablierte E-Mail-Kontakte. Im internen Bereich der Sicherheitsberatung des BSI gibt es ein Archiv mit aktuellen Informationen, die – wo erforderlich – auch den Anforderungen des Geheimschutzes entsprechen.

4.1.3 Cyber-Abwehrzentrum

Auf Grundlage des Kabinettsbeschlusses vom 23. Februar 2011 wurde das Nationale Cyber-Abwehrzentrum (Cyber-AZ) 2011 unter Federführung des BSI und in Zusammenarbeit mit dem Bundesamt für Verfassungsschutz (BfV), dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), dem Bundeskriminalamt (BKA), der Bundespolizei (BPol), dem Zollkriminalamt (ZKA), dem Bundesnachrichtendienst (BND) und der Bundeswehr eingerichtet. Als Informationsdrehscheibe gestartet, übernahm das Cyber-AZ in der Folgezeit immer mehr die Rolle einer Kooperationsplattform, über die auch operative Maßnahmen der einzelnen Behörden bei Cyber-Vorfällen koordiniert werden.

So wird bei Cyber-Sicherheitsvorfällen, die akuten Handlungsbedarf mit sich bringen, etwa bei Incident Response, technischer Gefahrenabwehr oder Täterermittlung, im Rahmen der „Koordinierten Fallbearbeitung“ kurzfristig eine Arbeitsgruppe aus den jeweils zuständigen Behörden gebildet. Die Arbeitsgruppe analysiert die vorliegenden Informationen und stimmt darüber hinaus auch das weitere Vorgehen und insbesondere die jeweiligen operativen Maßnahmen der einzelnen Behörden ab. In besonderen Fällen werden gemeinsame Termine bei den Betroffenen vor Ort durchgeführt.

Grundsätzliche Themen werden in Arbeitskreisen diskutiert und bewertet. Deren Zusammensetzung richtet sich nach dem jeweiligen Themenschwerpunkt, zum Beispiel Cyber-Crime, Cyber-Spionage oder Bedrohung Kritischer Infrastrukturen. Als federführende Behörde des Cyber-AZ ist das BSI in allen Arbeitsgruppen und Arbeitskreisen vertreten.

Der Weiterentwicklung zur Kooperationsplattform und dem vermehrten Informationsbedürfnis ministerieller Entscheidungsträger wurde durch die Anpassung interner Prozesse sowie einer Intensivierung des Berichtswesens des Cyber-AZ begegnet. Mit der „Cyber-Lage“ zu aktuellen Vorfällen und den etwa einmal monatlich erscheinenden, umfangreicheren „Informationen des Nationalen Cyber-Abwehrzentrums“ informiert das Cyber-AZ relevante Stellen aktuell und zielgruppengerecht über wichtige Vorfälle und Entwicklungen im Bereich der Cyber-Sicherheit. Die Empfänger erhalten auf diese Weise die konsolidierten Bewertungen der beteiligten Behörden aus einer Hand. Im Berichtszeitraum wurden 48 „Cyber-Lagen“ zu den Themen Cyber-Spionage (12), Cyber-Crime (10), Schwachstellen (9), KRITIS (10) und Sonstiges (7) sowie fünf Ausgaben der „Informationen des Nationalen Cyber-Abwehrzentrums“ herausgegeben.

4.1.4 CERT-Bund und nationales IT-Lagezentrum

CERT-Bund ist das Computer-Notfallteam der Bundesverwaltung (Computer Emergency Response Team) und zentrale Anlaufstelle für präventive und reaktive Maßnahmen bei sicherheitsrelevanten Vorfällen in Computersystemen. Das Notfallteam im BSI besteht seit 1994, seit 2001 als eigenständiges Referat. Neben seinen ursprünglich auf die Bundesverwaltung konzentrierten Aufgaben nimmt CERT-Bund seit vielen Jahren zunehmend auch Aufgaben eines nationalen CERTs für die Wirtschaft und die Bürger wahr und ist sehr gut in der nationalen, europäischen und internationalen CERT-Community vernetzt.

CERT-Bund bietet seinen Zielgruppen einige zentrale Dienste an:

1. Warn- und Informationsdienst zu technischen Schwachstellen in IT-Systemen:
   CERT-Bund und das Nationale IT-Lagezentrum geben gemeinsam pro Jahr mehrere tausend öffentliche Kurzinformationen und mehrere Hundert ausführliche Warnungen an die Bundesverwaltung heraus. Mehr als 30 Sicherheitsereignisse erforderten darüber hinaus eine besondere Unterrichtung der Zielgruppen.

2. Unterstützung bei der Vorfallsbearbeitung (Incident Response):
   Das BSI unterstützt Betroffene bei der Bewältigung von IT-Sicherheitsvorfällen. Die Unterstützung reicht von telefonischer Fachberatung über die Weitergabe von „Good Practice“-Dokumenten bis hin zur technischen Auswertung von Samples oder Festplatten. Die aufwendige Vor-Ort-Unterstützung, wie sie 2015 beispielsweise im Rahmen des IT-Sicherheitsvorfalls im Deutschen Bundestag erfolgreich geleistet wurde, soll in Zukunft weiter ausgebaut werden.

3. „Abuse-Handling“:
   CERT-Bund unterrichtet meist automatisiert täglich bis zu Hunderttausend Betroffene sowie Internet- und Hosting-Service-Provider über Infektionen auf ihren Systemen bzw. zu Schwachstellen oder Fehlkonfigurationen, die einen Missbrauch z.B. für DDoS-Reflection-Angriffe ermöglichen. Im Berichtszeitraum hat das BSI rund fünf Millionen Benachrichtigungen zu infizierten Systemen und über 15 Millionen Benachrichtigungen zu anfälligen Server-Diensten versendet.

4. Für Privatanwender stellt das BSI mit dem „Bürger-CERT“ einen Warn- und Informationsdienst in verschiedenen technischen Tiefen bereit. Das Bürger-CERT informiert kostenfrei und neutral über aktuelle Attacken durch Schadsoftware sowie über Sicherheitslücken in Anwendungen.

5. Prävention und Reaktion im Regierungsnetz:
   CERT-Bund betreibt im Regierungsnetz zentrale Sicherheitskomponenten, die Infektionen mit Schadprogrammen verhindern und erfolgte Kompromittierungen detektieren können.

Seit Ende 2015 beobachtet und analysiert CERT-Bund die explosionsartige Verbreitung von Ransomware, die Unternehmen, Behörden und Privatanwender stark betroffen hat. Die Ergebnisse der Analysen flossen in das vom BSI im März 2016 veröffentlichte „Themenpapier Ransomware“ ein, das die verschärfte Bedrohungslage durch Ransomware beschreibt und konkrete Empfehlungen und Hilfestellungen zur Prävention und Reaktion im Schadensfall beinhaltet.

Nationales IT-Lagezentrum BSI

Das Nationale IT-Lagezentrum wurde 2005 gegründet. Im Lagezentrum beobachten Mitarbeiter des BSI täglich die IT-Sicherheitslage, um den Handlungsbedarf und die Handlungsoptionen bei IT-Sicherheitsvorfällen sowohl auf staatlicher Ebene als auch in der Wirtschaft schnell und kompetent einschätzen zu können. Dafür steht dem Lagezentrum neben öffentlichen auch eine Vielzahl von nicht öffentlichen Quellen zur Verfügung. Hierzu zählen Experten aus dem BSI mit ihren Fachkontakten, die Teilnahme an verschiedenen Austauschkreisen wie dem UP KRITIS, dem Deutschen CERT-Verbund sowie verschiedene internationale Kreise wie Trusted Introducer und FIRST. Dabei werden jeden Monat etwa 500 Ereignisse als relevant bewertet. Rund die Hälfte dieser Ereignisse lösen BSI-interne Maßnahmen aus.

Eine besondere Quelle sind die Meldungen, die über die verschiedenen Meldestellen im Lagezentrum gebündelt auflaufen. Neben den langjährig etablierten Meldungen nach § 4 BSI-Gesetz aus der Bundesverwaltung und den freiwilligen Meldungen der Wirtschaft über die Allianz für Cyber-Sicherheit wird die Meldestelle zukünftig wichtige Informationen zur IT-Sicherheitslage in Deutschland beisteuern. Die im Zuge der Umsetzung des IT-Sicherheitsgesetzes neu eingerichtete Meldestelle nach § 8b BSI-Gesetz ist für die Entgegennahme und Bewertung von Störungsmeldungen im Bereich Kritischer Infrastrukturen zuständig. Die so gewonnenen und bewerteten Informationen fließen in verschiedene Lageprodukte ein, die wiederum den unterschiedlichen Zielgruppen des BSI zur Verfügung gestellt werden, damit diese ihre Sicherheitsmaßnahmen anpassen können. Anlassbezogen arbeitet das Lagezentrum eng mit dem Cyber-Abwehrzentrum zusammen, das den Austausch mit Partnerbehörden koordiniert.

4.1.5 Sichere Mobilkommunikation

Die Nutzung mobiler Lösungen, Smartphones und Tablets nimmt in der Behördenkommunikation zu. In Bezug auf die Sicherheit spielen dabei neben den Mobilgeräten selbst auch die Anbindung an die zugehörige Backend-Infrastruktur (Mobile Device Management, Mobile Application Management, VPN-Server, etc.) sowie deren Sicherheit eine entscheidende Rolle. Auch Apps, die auf mobilen Geräten installiert sind, können große Auswirkungen auf die Sicherheit der Gesamtlösung haben. Das BSI betrachtet alle Aspekte, bevor eine Mobilkommunikationslösung zur Verarbeitung von eingestuften Daten durch das BSI für den Behördeneinsatz zugelassen wird.

Ein Spannungsfeld entsteht dort, wo Nutzer immer aktuelle Hardware und Software verwenden wollen, eine gründliche Prüfung der Produkte jedoch Zeit in Anspruch nehmen würde. Daher entwickelt das BSI zusammen mit Unternehmen Lösungen, die sowohl die Wünsche der Anwender als auch die Anforderungen an die Sicherheit erfüllen. Im Bereich mobiler Kommunikation werden derzeit mehrere Lösungen hinsichtlich ihrer Sicherheit laufend durch das BSI geprüft:

- Smartphones
  - SecuSUITE von Secusmart/BlackBerry
  - SecurePIM von Virtual Solution/Apple
  - SiMKo 3 von T-Systems/Samsung
- Tablets
  - SINA Tablet von Secunet/Microsoft
  - SecuTABLET von Secusmart/IBM/Samsung
- Bluetooth-Zusatzgeräte
  - TopSec Mobile von Rohde & Schwarz.

Bislang hat das BSI der Bundesverwaltung rund 10.000 Mobilgeräte zur sicheren Kommunikation bereitgestellt. Bis Ende 2017 werden voraussichtlich weitere 8.000 bis 10.000 Geräte hinzukommen.

Neben der Evaluierung des Grundsystems müssen auch einzelne Apps hinsichtlich ihrer Sicherheit einzeln geprüft werden. Die traditionellen Methoden aus dem Bereich der PC-Virenscanner können aufgrund der Isolierung der Apps untereinander (Sandboxing) nicht übernommen werden. Stattdessen hat das BSI Regelwerke und Kriterien zur Bewertung der App-Sicherheit definiert, nach denen spezialisierte Firmen die Apps verschiedenen Prüfverfahren unterziehen. Seit 2014 hat das BSI rund 200 Apps für die Betriebssysteme Android, iOS und Blackberry OS anhand verschiedener Kriterien wie Zugriff auf Kalender und Adressbücher, Standortdaten und die Nutzung von Tracking-Netzwerken prüfen lassen. Während einige Apps nur wenige Kriterien verletzen, sind bei anderen Apps erhebliche Mängel im Umgang mit Nutzerdaten festzustellen. Um ein differenzierteres Risikomanagement zu ermöglichen, werden Prüfberichte vom BSI einer Nachbearbeitung unterzogen, bei der die verschiedenen Kriterien je nach Anwendungsfall gegeneinander gewichtet werden. Besonders häufig sind bei den bisherigen Prüfungen die Einbindung von nicht abschaltbaren Tracking-Netzwerken, die Erhebung von Geodaten sowie nicht vorhandene Datenschutzerklärungen aufgefallen. Die Prüfberichte werden der Bundesverwaltung zur Verfügung gestellt, die auf dieser Basis eine fundierte Entscheidung über den Einsatz der jeweiligen App treffen kann.

4.1.6 Zulassung

Das BSI hat die gesetzliche Aufgabe, IT-Sicherheitsprodukte zu prüfen (Evaluierung) und eine verbindliche Aussage zum Sicherheitswert zu machen (Zulassung). Betroffen sind IT-Sicherheitsprodukte, die für die Verarbeitung und Übertragung 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. 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 (Bedarfsträger) gestellt werden.

Nach § 37 der Verschlusssachenanweisung des Bundesministeriums des Innern (VSA) müssen Produkte zur Herstellung von Schlüsselmitteln, zur Verschlüsselung, zur Sicherung von Übertragungsleitungen und zur Trennung von Netzen mit unterschiedlichen maximalen Einstufungen der zu verarbeitenden Verschlusssachen vom BSI zugelassen werden. Im Berichtszeitraum September 2015 bis Juni 2016 hat das BSI hierzu 47 Zulassungen ausgesprochen bzw. verlängert. 27 Zulassungen wurden zurückgezogen bzw. durch Zulassungen neuerer Versionen ersetzt. Eine tagesaktuelle Auflistung der zugelassenen IT-Sicherheitsprodukte ist BSI-Schrift 7164 zu entnehmen, die auf der Webseite des BSI zur Verfügung steht.

Um auch weiterhin den Bedarf der (Bundes-) Verwaltung nach zugelassenen Produkten decken zu können, betreut das BSI derzeit mehr als 50 laufende Verfahren mit dem Ziel einer Zulassung. Um dem steigenden Anspruch an die Reaktionsfähigkeit im Rahmen von Zulassungsverfahren Rechnung zu tragen, hat das BSI gemeinsam mit dem Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) das VSF-Verfahren entwickelt und im Anschluss erfolgreich validiert. Ziel des „Verfahrens für Szenariobasierte Freigabegenehmigung“ (VSF) ist es, in vom Normalfall abweichenden bundeswehrspezifischen Ausnahmesituationen – etwa bei dringlichen, nicht vorhersehbaren Einsätzen – reaktionsschnell eine anforderungskonforme Anwendung der VSA zu gewährleisten. Beispiele für VSF-Verfahren sind Zulassungen im Rahmen der EU-Operation EU NAVFOR MED zur Seenotrettung von Flüchtlingen im Mittelmeer.

Als weiteres Instrument für die Zulassung dienen VS-Anforderungsprofile (VS-AP) und nationale Protection Profiles (nPP), die zur Vereinheitlichung und klaren Definition von IT-Sicherheitsanforderungen verschiedener Produktklassen und -typen erforderlich sind. Das BSI hat – zum Teil gemeinsam mit der Industrie – eine Vielzahl an VS-APs bzw. nPPs für den Einsatz im VS-Bereich entwickelt.

4.2 IT-Sicherheit für die Wirtschaft

4.2.1 UP KRITIS und IT-Sicherheitsgesetz

Kritische Infrastrukturen versorgen Bevölkerung und Wirtschaft mit wesentlichen Dienstleistungen, ohne die unser modernes Leben nicht denkbar wäre – angefangen von der Versorgung mit Wasser, Lebensmitteln und Gesundheitsdienstleistungen über Strom und Telekommunikation, Finanz- und Transportdienstleistungen bis hin zur Verfügbarkeit von Datennetzen und Datenverarbeitung in großen Rechenzentren. Diese Dienstleistungen hängen mehr und mehr von funktionierenden IT-Systemen ab: von klassischer Büro-IT, von Spezialsoftware für einzelne Prozesse, von eingebetteten Systemen, von Prozesssteuerungshardware und -software oder von Operational Technology.

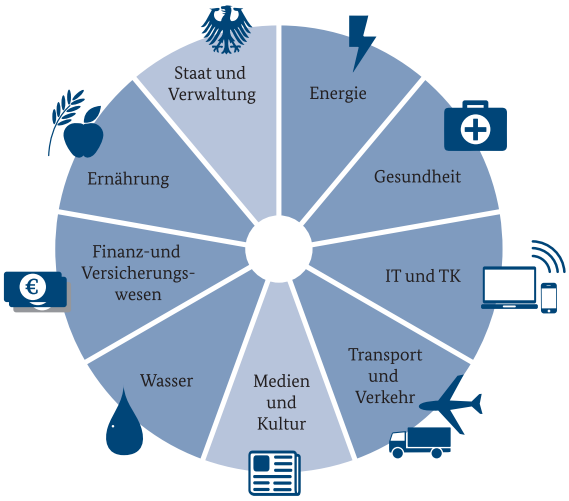


Abbildung 14: Sieben der neun KRITIS-Sektoren fallen unter die KRITIS-Neuregelungen des IT-Sicherheitsgesetzes [1]

Am 25. Juli 2015 ist das IT-Sicherheitsgesetz in Kraft getreten. Mit dem verabschiedeten Artikelgesetz wurden Änderungen an verschiedenen Gesetzen vollzogen: am BSI-Gesetz (BSIG), Telekommunikationsgesetz (TKG), Energiewirtschaftsgesetz (EnWG) und Atomgesetz (AtG). Im Vordergrund steht dabei die Absicherung der IT in sieben der neun Sektoren der Kritischen Infrastrukturen. Kernpunkte der Neuregelungen für Betreiber Kritischer Infrastrukturen sind die Pflicht,

- prozessrelevante IT angemessen abzusichern und dabei den Stand der Technik zu berücksichtigen,
- ihre IT alle zwei Jahre einem Audit oder einer sonstigen Prüfung zu unterziehen sowie
- erhebliche Störungen der IT unverzüglich an das BSI zu melden.

Das BSI hat im Gegenzug die Aufgabe, alle ihm vorliegenden Informationen zur IT-Sicherheitslage zu analysieren und KRITIS-Betreiber und Aufsichtsbehörden umfassend zu informieren. Außerdem unterstützt und berät das BSI auf Anfrage die KRITIS-Betreiber.

UP KRITIS – eine erfolgreiche Kooperation

Das Ziel, die IT in Kritischen Infrastrukturen resilient zu gestalten, verfolgt das BSI schon seit über zehn Jahren. 2007 wurde nach einer zweijährigen Vorbereitungszeit die öffentlich-private Kooperation UP KRITIS gegründet, um sich den wachsenden Herausforderungen im Kontext des zunehmenden IT-Einsatzes in Kritischen Infrastrukturen zu widmen. Ohne regulatorische Grundlage arbeiteten hierbei zunächst rund 30 der größten Betreiber Kritischer Infrastrukturen Deutschlands mit dem Staat zusammen. Die Kooperation verlief gut, doch die Reichweite war zu gering und nicht alle gesetzten Ziele konnten auf dieser Basis erreicht werden. 2013/14 erfolgte eine Neuausrichtung der Kooperation, einhergehend mit einer deutlichen Öffnung des Teilnehmerkreises. Derzeit kooperieren 380 Organisationen im UP KRITIS. Aktuell befasst sich der UP KRITIS mit der Umsetzung des IT-Sicherheitsgesetzes. Die unter langjähriger Federführung des BSI aufgebaute Kooperation erweist sich hier als ideale Ergänzung zu den neuen regulatorischen Vorgaben.

Kritische Infrastrukturen im Sinne des BSIG

Die BSI-Kritisverordnung (BSI-KritisV) regelt anhand bestimmter Kriterien, welche Betreiber die Vorgaben des IT-Sicherheitsgesetzes zu erfüllen haben. Erlassen wird die Verordnung durch das Bundesministerium des Innern, die inhaltliche Vorarbeit basierte dabei ganz wesentlich auf der Kooperation im UP KRITIS. Für jeden Sektor wurden Kernteams gebildet, in denen neben Vertretern des Staates auch die Sprecher der Branchenarbeitskreise im UP KRITIS sowie Vertreter von KRITIS-Betreibern oder deren Verbänden ihre Expertise und Positionen einbringen konnten. Die 2014 im UP KRITIS eingeführten Branchenarbeitskreise existieren inzwischen in fast allen Branchen. Auch die im Auftrag des BSI erstellten Sektorstudien

[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.

(*www.kritis.bund.de/Sektorstudien*) wurden zuvor in diesen Arbeitskreisen diskutiert.

Der erste Teil der Verordnung ist am 3. Mai 2016 in Kraft getreten und bestimmt zunächst Kritische Infrastrukturen in den Sektoren Energie, Informationstechnik und Telekommunikation sowie Wasser und Ernährung. Bis Frühjahr 2017 sollen auch die Kritischen Infrastrukturen in den Sektoren Transport und Verkehr, Gesundheit sowie Finanz- und Versicherungswesen für die Betreiber identifizierbar werden.

Warnungen und Lagebild

Die Versorgung der Betreiber Kritischer Infrastrukturen aller neun Sektoren sowie weiterer Unternehmen mit aktuellen Warn- und Lageinformationen ist eine seit Jahren etablierte Dienstleistung des BSI. Die Vorgehensweisen und Prozesse wurden dabei u. a. im Rahmen eines Themenarbeitskreises des UP KRITIS immer weiter verfeinert. Eine Herausforderung ist und blieb jedoch von Anfang an die Informationslage zu IT-Störungen und IT-Sicherheitsvorfällen in der Wirtschaft. Oft überwog bei den Betreibern das Interesse der Geheimhaltung den gleichwohl vorhandenen Willen zum Erfahrungsaustausch über eingetretene Fehler und Pannen. Mit dem IT-Sicherheitsgesetz und der darin verankerten Meldepflicht erheblicher Sicherheitsvorfälle erwartet das BSI nach einer Anlaufphase eine deutlich steigende Zahl an Meldungen und somit ein erheblich verbessertes Lagebild.

Personell gestärkt durch das IT-Sicherheitsgesetz kann das BSI die gewonnenen Informationen zukünftig noch öfter, schneller und besser in Produkte übersetzen, von denen die Unternehmen profitieren können. Die im Themenarbeitskreis Operativer Informationsaustausch des UP KRITIS vorbereiteten Prozesse bilden hierfür die Basis, die Single Points of Contact (SPOCs) im UP KRITIS die Blaupause für entsprechende Multiplikatoren gemäß BSI-Gesetz.

Erste Meldungen nach BSI-Gesetz haben das BSI bereits erreicht und wurden entsprechend den Neuregelungen verarbeitet. Mit einer großen Anzahl an Meldungen ist zu rechnen, wenn alle KRITIS-Betreiber ihre Kontaktstellen registriert haben. Betreiber, die unter den ersten Teil der BSI-KritisV fallen, haben dazu bis Anfang November 2016 Zeit.

Robuste IT nach Stand der Technik

Die wichtigste im IT-Sicherheitsgesetz verankerte Neuerung für KRITIS-Betreiber ist die Verpflichtung, angemessene Vorkehrungen zur Vermeidung von Störungen ihrer IT umzusetzen, die für die Funktionsfähigkeit der Kritischen Infrastrukturen maßgeblich ist. Hierbei muss der Stand der Technik berücksichtigt werden. Diese Umsetzung muss zudem alle zwei Jahre im Rahmen einer Prüfung nachgewiesen werden. Welche konkreten Maßnahmen umzusetzen sind, schreibt das BSI-Gesetz nicht vor. Dem kooperativen Ansatz des Gesetzes folgend wird den Branchen die Möglichkeit gegeben, die Maßnahmen im Rahmen von „branchenspezifischen Sicherheitsstandards“ (B3S) selbst zu definieren. Auf Antrag kann das BSI die Eignung eines solchen B3S feststellen.

Das BSI hat dazu eine Orientierungshilfe (*www.bsi.bund.de/Stand-der-Technik*) veröffentlicht, die die Anforderungen an einen B3S und somit auch die Anforderungen an die „angemessenen Vorkehrungen“ gemäß BSI-Gesetz zusammenstellt. Darüber hinaus wird das BSI eine im neuen Themenarbeitskreis „Audits und Standards“ des UP KRITIS gemeinsam mit Prüfern und Normungsorganisationen erarbeitete Orientierungshilfe zum Thema Prüfungen und Audits veröffentlichen. Diese beschreibt die Erwartungen des BSI an Prüfungen nach BSI-Gesetz, um diese als geeignet anzuerkennen. Denn auch die im BSI-Gesetz vorgeschriebenen Prüfungen, Audits oder Zertifizierungen werden nicht durch das BSI selbst durchgeführt. Hier können Betreiber auf bei ihnen bereits eingesetzte Prüfmethoden aufbauen.

Einige Branchenarbeitskreise des UP KRITIS arbeiten bereits intensiv an ihren branchenspezifischen Sicherheitsstandards, sodass den Betreibern rasch eine in den jeweiligen Branchen erstellte Konkretisierung der sinnvollen Sicherheitsmaßnahmen zur Verfügung stehen wird. Die im Rahmen eins solchen Sicherheitsstandards zusammengestellten Maßnahmen sind zudem eine sinnvolle Orientierungshilfe auch für Unternehmen, die nicht den Regelungen des IT-Sicherheitsgesetzes unterliegen.

Fazit

Der UP KRITIS hat die Grundlagen für eine resiliente IT in Kritischen Infrastrukturen gelegt. Bislang fehlte jedoch eine rechtlich verbriefte Möglichkeit, die erarbeiteten Ansätze gegen andere Interessen durchzusetzen. Das IT-Sicherheitsgesetz baut auf dem kooperativen Ansatz auf, verschafft den guten Ideen durch rechtliche Vorgaben nun mehr Durchsetzungskraft. Das BSI erhält durch die mit dem Gesetz verbundene Stärkung mehr Handlungsfähigkeit zur Gestaltung der IT-Sicherheit in Bereichen, die für das Gemeinwohl von höchster Bedeutung sind.

4.2.2 Allianz für Cyber-Sicherheit

Fast alle Bereiche der deutschen Wirtschaft stehen der Herausforderung gegenüber, die Chancen der Digitalisierung zu nutzen und dabei gleichzeitig deren Risiken effektiv zu begegnen. Dabei geht es längst nicht mehr nur um den ohnehin schon seit Jahren zunehmenden unternehmensinternen IT-Einsatz in Bereichen wie Produktion, Logistik und Verwaltung. Neue Konzepte aus dem Feld der Industrie 4.0, die Präsenz auf Online-Marktplätzen sowie der unumgängliche Austausch mit Kunden und Zulieferern über das Internet bieten zahlreiche neue Möglichkeiten für die Unternehmen, können aber auch zu neuen Verwundbarkeiten führen. Wird ein Unternehmen so zum Ziel eines Cyber-Angriffs, können durch Betriebs- bzw. Produktionsausfälle oder den Diebstahl von Daten relevante Schäden entstehen. Gerade der starke und innovative deutsche Mittelstand mit zahlreichen Weltmarktführern und „Hidden Champions“ muss damit rechnen, das Ziel von digitaler Industriespionage zu werden.

Mit der 2012 gegründeten Allianz für Cyber-Sicherheit hat sich das BSI zum Ziel gesetzt, die Widerstandsfähigkeit des Standorts Deutschland gegen Cyber-Angriffe zu stärken. Im Fokus der für alle Institutionen aus Wirtschaft, Wissenschaft und Behörden offenen Initiative steht dabei der deutsche Mittelstand. Als größte nationale Kooperationsplattform zum Thema Cyber-Sicherheit bietet die schnell wachsende Allianz für Cyber-Sicherheit ihren rund 2.000 Teilnehmern, annähernd 100 Partnern und 40 Multiplikatoren umfangreiche Informationen zur Prävention vor wie auch zur Reaktion bei Cyber-Angriffen. Für das gesamte Informationsangebot wird besonderer Wert auf die Anwendbarkeit vorgeschlagener Maßnahmen durch KMU gelegt, d.h., es wird versucht, ein möglichst hohes Maß an Sicherheit mit angemessenen, aber begrenzten Mitteln zu erzielen. Dieses Angebot aus mittlerweile über 100 thematisch sortierten Dokumenten wird abgerundet durch monatliche Lageberichte und aktuelle Warnmeldungen. Diese sind gleichfalls ein gutes Beispiel dafür, wie die Teilnehmer gegenseitig voneinander profitieren können. So tragen freiwillige Meldungen zu Cyber-Sicherheitsvorfällen, welche das BSI über die anonyme Meldestelle der Allianz erreichen, bei entsprechender Freigabe regelmäßig zu den Lageberichten bei.

Neben der reinen Information profitieren die Teilnehmer vor allem vom offenen Austausch von Erfahrungen aus der Praxis untereinander. Dazu bietet die Allianz für Cyber-Sicherheit unter anderem mit dem erfolgreichen Veranstaltungsformat der Cyber-Sicherheitstage überregional Gelegenheit. Im vergangenen Jahr nahmen rund 600 Personen an einem der vier Cyber-Sicherheitstage teil. Darüber hinaus treffen sich in verschiedenen Arbeitsgruppen der Erfahrungs- und Expertenkreise regelmäßig IT-Professionals und IT-Security Experten zur Diskussion aktueller Themen und Ereignisse.

Im Sinne der Kooperation aller Akteure der Cyber-Sicherheit in Deutschland können sich alle Teilnehmer mit eigenen Angeboten als Partner aktiv in die Arbeit der Initiative einbringen. Dass auch in diesem Jahr über einhundert kostenfreie Plätze in Schulungen und Seminaren, Videos zur Mitarbeitersensibilisierung, kostenfreie Revisionen und Sicherheitschecks angeboten wurden, belegt das große Engagement der beteiligten Partner. Mit zwei Durchläufen des fünftägigen Übungszentrums Netzverteidigung hat sich das BSI auch im letzten Jahr wieder an den kostenfreien Fortbildungsangeboten im Rahmen der Allianz für Cyber-Sicherheit beteiligt, sodass allein hierüber weitere 40 IT-Verantwortliche zu aktuellen Bedrohungen sensibilisiert werden konnten.

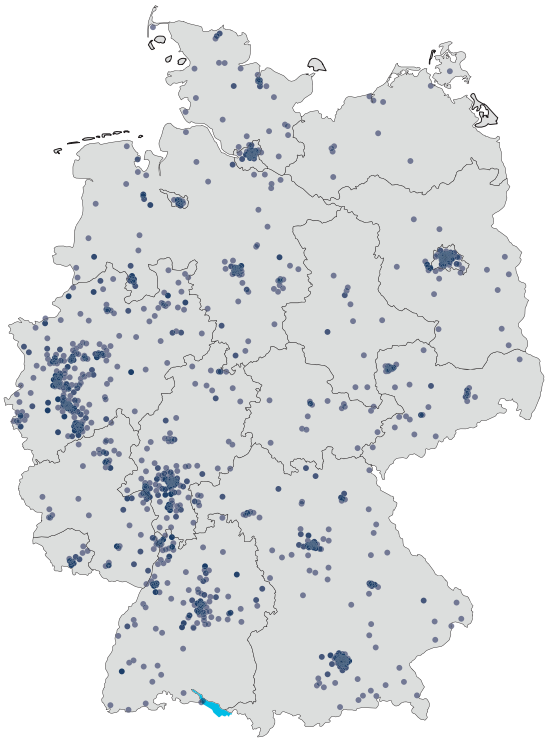


Abbildung 15:
Die Allianz für Cyber-Sicherheit: flächendeckende Kooperationsplattform

4.2.3 Erhöhung der Cyber-Sicherheit im Internet

Zur Erhöhung der Cyber-Sicherheit im Internet arbeitet das BSI eng mit den Internet-Providern zusammen. Im „Expertenkreis Internetbetreiber" der Allianz für Cybersicherheit steht das BSI dazu im kontinuierlichen Austausch mit den führenden Internet- und Hosting-Providern in Deutschland. In dieser Kooperation wird regelmäßig die aktuelle Gefährdungslage erhoben. Zur Abwehr dieser Gefährdungen sind bereits neun Cyber-Sicherheitsempfehlungen des BSI erschienen, die mit den Mitgliedern des Expertenkreises erarbeitet wurden. Die Empfehlungen werden regelmäßig an die aktuelle Lage angepasst und stehen auch mittleren und kleineren Betreibern bei der Absicherung ihrer Netze zur Verfügung. Bei akuten Vorfällen unterstützt das BSI die Betreiber nach Bedarf. Insbesondere, wenn nicht nur ein einzelner Betreiber betroffen ist, ist ein Austausch an Informationen über den Vorfall und mögliche Gegenmaßnahmen mit allen betroffenen Betreibern zu koordinieren.

Zusammen mit Forschungseinrichtungen hat das BSI das Providerinformationssystem als wichtige Maßnahme zur Information von Bürgerinnen und Bürgern mit infizierten Rechnern aus Botnetzen etabliert. Werden dem BSI Informationen über infizierte Rechner zur Verfügung gestellt, sorgt PI dafür, dass diese Informationen schnell an den zuständigen Internet Service Provider weitergegeben werden. Dieser informiert wiederum seine betroffenen Kunden. Seit dem Start des Systems im August 2014 wurden so Bürgerinnen und Bürger mit infizierten Rechnern auf der Basis von insgesamt ca. 17 Millionen verschiedenen IP-Adressen (2016 durchschnittlich rund 15.000 IPs pro Tag) informiert.

Wichtige Bestandteile des Internets sind die vielen dort angebotenen Telemediendienste. Im Rahmen des IT-Sicherheitsgesetzes wurden die Telemediendiensteanbieter verpflichtet, ihre Dienste nach dem Stand der Technik abzusichern. Dazu hat das BSI ein Diskussionspapier zur Absicherung von Telemediendiensten veröffentlicht, das unter Beteiligung des Bitkom und des Expertenkreises Internetbetreiber der Allianz für Cyber-Sicherheit entstanden ist. Das Papier schlägt Maßnahmen vor, wie Telemediendienste gegen unerlaubten Zugriff auf technische Einrichtungen, Verletzung des Schutzes personenbezogener Daten sowie Störungen abgesichert werden können. Bei den vorgeschlagenen Maßnahmen wird jeweils der Stand der Technik berücksichtigt, d.h., dass die Eignung der Maßnahmen sich in der Praxis bewährt hat. Das Diskussionspapier richtet sich vornehmlich an Anbieter und Verantwortliche von geschäftsmäßig angebotenen Telemediendiensten, beispielsweise Betreiber von Onlineshops oder Anbieter von Hosting- und Server-Dienstleistungen. Die Rückmeldungen werden bei der Weiterentwicklung des Papiers berücksichtigt, das später als Cyber-Sicherheitsempfehlung veröffentlicht werden soll.

Ergänzend dazu hat das BSI die meistgenutzten Content-Management-Systeme auf ihre Sicherheit untersucht. Die im Rahmen der Untersuchung gefundenen Probleme wurden an die Hersteller gemeldet und von diesen weitestgehend beseitigt. Zu den verschiedenen Content-Management-Systemen wurden Sicherheitsempfehlungen mit zugehörigen Checklisten erarbeitet. Diese werden vom BSI in absehbarer Zeit veröffentlicht und können von allen Diensteanbietern zur Verbesserung der Sicherheit ihres Angebotes genutzt werden.

Für die Nutzung moderner Breitbandanschlüsse werden in der Regel Breitbandrouter als Telekommunikationsschaltzentrale eingesetzt. Diese Router übernehmen zusätzlich oft auch die Absicherung des eigenen internen Netzes vor Angriffen aus dem Internet. Sie stellen somit mittlerweile eine wesentliche Sicherheitskomponente dar. Trotzdem sind in der Vergangenheit in dieser Komponente Sicherheitsprobleme aufgetreten, die von Kriminellen genutzt wurden, etwa um auf Kosten der Betroffenen teure Telefonate zu führen. Das BSI hat deshalb zusammen mit den Herstellern und den Providern ein Testkonzept für Breitbandrouter erarbeitet. Das Konzept ermöglicht eine Überprüfung relevanter Sicherheitseigenschaften von Routern. Dabei betrachtet das BSI grundlegende sicherheitsrelevante Funktionen sowie die Unterstützung und Einhaltung etablierter Sicherheitsstandards. Ziel ist es, die Sicherheit von Breitband-Routern wie xDSL- oder Kabel-Routern messbar zu machen und ein einheitliches Sicherheitsniveau der Geräte zu erreichen. Das Testkonzept des BSI richtet sich vornehmlich an Internet Service Provider und an Hersteller von Breitbandroutern. Es ist beabsichtigt, in Zusammenarbeit mit den in Deutschland tätigen Internet Service Providern und Herstellern Router entsprechend der im Testkonzept beschriebenen Methodik zu testen.

Des Weiteren beteiligt sich das BSI im Rahmen der internationalen Internetgremien, wie der Internet Engineering Task Force (IETF) oder des Réseaux IP Européens Network Coordination Centre (RIPE NCC), an der Weiterentwicklung sicherer Internet-Protokolle wie DNSSEC, DANE oder RPKI und unterstützt die Internet Service Provider in Deutschland ebenso wie die Betreiber des Informationsverbunds Berlin-Bonn bei der

Einführung dieser Protokolle. Das BSI arbeitet auch eng mit der für den Telekommunikationsbereich zuständigen Regulierungsbehörde Bundesnetzagentur sowie mit der Bundesbeauftragten für den Datenschutz zusammen, um gemeinsam die Cyber-Sicherheit im Internet zu erhöhen. So wurde der Katalog von Sicherheitsanforderungen nach TKG § 109 gemeinsam erarbeitet. Dieser Katalog ist die Grundlage für die Sicherheitskonzepte der Telekommunikationsanbieter.

4.2.4 Industrie 4.0: BSI-Studie zum Kommunikationsstandard OPC UA

Insbesondere im Zuge der Industrie 4.0 schreitet die Vernetzung industrieller Steuerungssysteme (ICS) stetig voran. ICS sind komplexe und über die Jahre gewachsene Systeme, in denen oft Komponenten vieler unterschiedlicher Hersteller zum Einsatz kommen. Diese sind typischerweise wenig dynamisch, haben nicht selten eine Lebensdauer von Jahrzehnten und nutzen häufig proprietäre und unsichere Kommunikationsprotokolle. Hier Sicherheit zu gewährleisten und gleichzeitig den Anforderungen an eine moderne und flexible Smart Factory gerecht zu werden, ist eine nur schwer zu meisternde Herausforderung.

Innerhalb der Initiative Industrie 4.0 der Bundesregierung ist eine intelligente, vor allem aber sichere Vernetzung der Produktionsprozesse ein elementarer Bestandteil. Das plattformunabhängige und weltweit anerkannte Kommunikationsprotokoll OPC UA stellt für eine sichere Fabrik notwendige kryptografische Mechanismen bereit und wird als zentraler Baustein auf dem Weg zu Industrie 4.0 angesehen. Es ermöglicht eine Integration von Industriekomponenten und -prozessen über unterschiedliche Schichten der Automatisierungspyramide. Um die Entwicklungen im Kontext Industrie 4.0 auf eine solide Grundlage zu stellen, hat das BSI 2015 eine unabhängige Untersuchung der sicherheitsrelevanten Elemente von OPC UA durchgeführt.

Die Studie des BSI liefert eine fundierte Bewertung der spezifizierten und realisierten Sicherheitsfunktionen von OPC UA. Durch die umfassende Analyse der Spezifikation konnte bestätigt werden, dass OPC UA unter Berücksichtigung von Sicherheitsaspekten entwickelt wurde und hinsichtlich aller relevanten Schutzziele und Bedrohungen keine systematischen Sicherheitslücken enthält. Es wurden nur kleinere Inkonsistenzen festgestellt, die zu einer Überarbeitung der Spezifikation durch die OPC Foundation führten.

Bei der Prüfung einer ausgewählten Referenzimplementierung des OPC UA Kommunikations-Stacks der OPC Foundation wurde die Umsetzung der in der Spezifikation beschriebenen Sicherheitsfunktionalitäten, aber auch der Schutz vor allgemeinen Angriffsmöglichkeiten wie zum Beispiel Denial of Service mithilfe von statischen und dynamischen Analysemethoden untersucht. Dabei wurden wenige kleinere Fehler und Inkonsistenzen gegenüber der Spezifikation sowie eine Schwachstelle gefunden, die bei ausgeschalteten Sicherheitsfunktionen ausgenutzt werden kann. Die OPC-Foundation wurde vorab informiert und hat die Referenzimplementierung rasch aktualisiert sowie als Reaktion eine eigene Informationsseite zum Thema Security eingerichtet. Systematische oder kritische Fehler wurden bei der Analyse nicht gefunden.

Auch wenn im Rahmen der Studie „Sicherheitsanalyse von OPC UA“ nur Teilbereiche der Spezifikation und der Referenzimplementierung des Kommunikations-Stacks hinsichtlich IT-Sicherheit untersucht werden konnten, so ist in der Gesamtschau das Ergebnis sehr positiv. Abgesehen von einigen Kleinigkeiten kann festgestellt werden, dass OPC UA das Prinzip „Security by Design“ konsequent umsetzt und bei korrekter Verwendung und ganzheitlich abgesicherter Infrastruktur eine sichere Vernetzung von Industriesystemen ermöglicht. Die Studie des BSI steht auf der Webseite des BSI zum Download zur Verfügung.

4.2.5 Novellierung IT-Grundschutz: Etablierte Informationssicherheit heute und in Zukunft

Die Innovationszyklen in der Informationstechnik werden immer kürzer. Neue Produkte und Dienstleistungen entstehen und werden immer schneller weiterentwickelt, gleichzeitig werden die technischen Systeme komplexer. Aufgrund der wachsenden Durchdringung vieler Bereiche der Wirtschaft und Gesellschaft wird die Abhängigkeit von funktionierender Technik immer größer. Das Management von Unternehmen und Institutionen muss sich dabei zunehmend mit der Frage befassen, welche Auswirkungen ein Cyber-Angriff mit sich bringen kann. Neben der eigenen Institution können auch Kunden, Lieferanten und Geschäftspartner sowie weitere Gruppen betroffen sein. Daher ist ein geplantes Vorgehen aller Beteiligten notwendig, um ein angemessenes und ausreichendes Sicherheitsniveau aufzubauen und aufrechtzuerhalten. Der IT-Grundschutz ist der meistgenutzte Standard für Informationssicherheit in Deutschland. Das etablierte Managementsystem für Informationssicherheit (ISMS) wird derzeit grundlegend überarbeitet, damit es den gestiegenen Anforderungen an die Absicherung von Informationen in einer

Institution auch weiterhin Rechnung tragen kann. Ziele der Modernisierung sind unter anderem die bessere Strukturierung und Verschlankung der IT-Grundschutz-Kataloge, die Beschleunigung der Umsetzung von Sicherheitsmaßnahmen, die Flexibilisierung der Vorgehensweise sowie die stärkere Berücksichtigung von anwenderspezifischen Anforderungen.

Flexibler und dynamischer

Aufgrund der sich rasant verändernden Bedrohungslage für IT-Systeme rückt das Thema Cyber-Sicherheit verstärkt in den Fokus des IT-Grundschutzes. Zugleich sollen künftig alle IT-Grundschutz-Veröffentlichungen dem Stand der Technik entsprechen. Einzelne Formate wie die bewährten IT-Grundschutz-Bausteine können innerhalb der gesamten IT-Grundschutz-Methodik flexibler und zügiger erstellt und veröffentlicht werden. Die Anwender sparen mit den modernisierten Bausteinen Zeit und Ressourcen. Und auch ihre Expertise ist stärker gefragt: In einem neuen Veröffentlichungsprozess werden neue Bausteine künftig als „Community Drafts“ auf der BSI-Webseite zur Kommentierung veröffentlicht. Mit dem Input aus der Praxis können die Inhalte bis zum fertigen Baustein noch weiter optimiert werden. Die ersten Community Drafts sind bereits veröffentlicht. Bis Ende 2016 sollen rund 50 bis 70 weitere Bausteine veröffentlicht werden. Auch für die unterschiedlichen Zielgruppen des IT-Grundschutzes soll künftig mehr Flexibilität in der Umsetzung möglich sein. Neben Behörden und größeren Wirtschaftsunternehmen werden auch kleine und mittelständische Unternehmen (KMU) stärker angesprochen. Die überarbeitete IT-Grundschutz-Methodik wird künftig für diese Unternehmen ihren Anforderungen entsprechende Angebote bereitstellen.

Neue Vorgehensweisen, mehr Themen

Eine elementare Neuerung besteht in der veränderten Ausrichtung der im IT-Grundschutz verankerten Vorgehensweisen. Institutionen können künftig zwischen drei Vorgehensweisen auswählen:

1. Basis-Absicherung: Hierbei handelt es sich um eine grundlegende Absicherung der Geschäftsprozesse und Ressourcen einer Institution. Sie ermöglicht einen Einstieg in ein Sicherheitsmanagement, um schnellstmöglich die größten Risiken zu senken. Im nächsten Schritt können die tatsächlichen Sicherheitsanforderungen im Detail analysiert werden. Diese Vorgehensweise ist daher besonders für KMU geeignet.

2. Kern-Absicherung: Die Kern-Absicherung dient als weitere Einstiegsvorgehensweise dem Schutz der elementarsten Geschäftsprozesse und Ressourcen. Sie unterscheidet sich vom klassischen IT-Grundschutz durch die Fokussierung auf einen kleinen, aber sehr wichtigen Teil eines Informationsverbundes.

3. Standard-Absicherung: Die Standard-Absicherung entspricht in den Grundzügen der Vorgehensweise nach dem aktuellen IT-Grundschutz nach BSI-Standard 100-2. Bei der Neukonzeption des IT-Grundschutzes ist zudem vorgesehen, ein noch breiteres Themenspektrum abzudecken. Neue Entwicklungen in der Informationstechnik sollen möglichst rasch in IT-Grundschutz-Veröffentlichungen wie beispielsweise die Bausteine einfließen. Als komplexe neue Themen sind Automatisierungs-, Prozesssteuerungs- und Prozessleitsysteme aufgenommen sowie um die Aspekte Detektion und Reaktion erweitert worden.

IT-Grundschutz-Profile: Know-how und Erfahrungen teilen

Eine weitere Neuheit stellen die IT-Grundschutz-Profile dar. Damit stellt das BSI ein flexibles Angebot bereit, mit dem Anwendergruppen den IT-Grundschutz an ihre konkreten Bedürfnisse anpassen und anschließend und für weitere interessierte Nutzer veröffentlichen können. Im nächsten Schritt liefern die IT-Grundschutz-Profile die Grundlage, um branchenspezifische Sicherheitsstandards entwickeln und stetig fortschreiben zu können. Neben der Weitergabe von Know-how können sich Unternehmen mit denselben Sicherheitsthemen vernetzen und gegenseitig von den Erfahrungen anderer Institutionen profitieren.

Die neuen Angebote des IT-Grundschutzes können künftig von Institutionen jeder Größenordnung zur Absicherung ihrer Informationsverbünde genutzt werden. Der komplexe Prozess zur Überarbeitung der IT-Grundschutz-Methodik wird im Jahr 2017 abgeschlossen. Das BSI wird die IT-Grundschutz-Community frühzeitig darüber informieren, welche Übergangsfristen für Zertifikate gelten werden, und wird den Wechsel von der alten auf die neue IT-Grundschutz-Vorgehensweise so gestalten, dass dies für Anwender gut umsetzbar ist. Die grundlegende Modernisierung der bewährten IT-Grundschutz-Methodik ermöglicht es, noch effizienter infrastrukturelle, organisatorische, personelle und technische Standard-Sicherheitsmaßnahmen zu identifizieren und zu ergreifen. Mit diesem ganzheitlichen Ansatz können Institutionen jeder Größenordnung ein Standard-Sicherheitsniveau aufbauen, um geschäftlich relevante Informationen zu schützen. Der IT-Grundschutz des BSI leistet damit einen wichtigen Beitrag zur Erhöhung des Sicherheitsniveaus in Deutschland.

4.2.6 Zertifizierung: Vertrauen schaffen, IT-Sicherheit gestalten

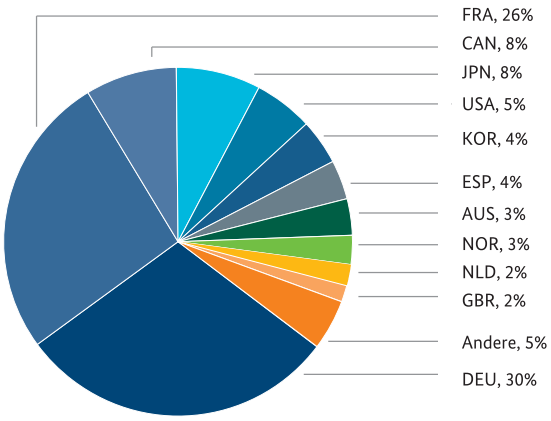


Abbildung 16: Common-Criteria-Zertifikate 2007 bis Q2 2016 (Quelle: Zertifikate gem. http://www.commoncriteriaportal.org)

Deutschland und Europa sind in der globalen Informations- und Kommunikationstechnik lediglich in Teilsegmenten signifikante Anbietermärkte für Software- und Hardwareprodukte. Vor diesem Hintergrund ist eine IT-Sicherheitszertifizierung dieser Produkte von besonderer Bedeutung, da ein aktuelles Sicherheitszertifikat bei Kaufentscheidungen das ausschlaggebende Element sein kann. Aus Nutzersicht stehen mit der Sicherheitsstandardisierung und der IT-Sicherheitszertifizierung wirksame Instrumente zur Verfügung, um die Transparenz der Informationssicherheit zu erhöhen, die Vertrauenswürdigkeit von Produkten zu bewerten und auch aus Anwenderinteresse ein höheres Niveau der Informationssicherheit am Markt durchsetzen zu können. Wegen der Globalität des Marktes spielen IT-Sicherheitsstandards und IT-Sicherheitszertifizierungen nur nach internationalen Standards wie den „Common Criteria“ eine Rolle, um das Vertrauen in Hard- und Softwareprodukte zu gewährleisten. Nur auf Basis internationaler Standards sind die großen, international agierenden Unternehmen in der IKT-Branche bereit, in Prüfaufwände mit anschließender Zertifizierung zu investieren.

Dem BSI wird aufgrund der erteilten Zertifikate innerhalb der internationalen Anerkennungsabkommen, aber auch durch das große Engagement in diesem Bereich eine Schlüsselrolle zuteil. Diese wird genutzt, um Produkte nationaler und internationaler Hersteller sicherer zu entwickeln sowie durch unabhängige Prüfinstitutionen Evaluierungen mit Schwachstellenanalysen durchzuführen. Im Rahmen der Common-Criteria-Zertifizierung sind in Deutschland neun Prüfstellen mit der entsprechenden Kompetenz durch das BSI anerkannt. Zusätzlich kann auch IT-Sicherheitskonformität nach Technischen Richtlinien zertifiziert werden.

Gerade für Anwendungsfälle hoher Kritikalität, etwa aufgrund der Notwendigkeit des Schutzes einer Infrastruktur oder des Schutzes persönlicher Daten, müssen IT-Produkte hohen Anforderungen genügen. Diese werden standardisiert in sogenannten Schutzprofilen (Protection Profiles), mit denen für bestimmte Produktgruppen oder Techniksysteme Sicherheitsstandards definiert werden, deren Einhaltung durch die Zertifizierung gewährleistet wird. Diese Schutzprofile schaffen in den verschiedenen Produktklassen eine Vergleichbarkeit für den Anwender. Insbesondere machen die unterschiedlichen Prüftiefen transparent, ob und wie intensiv das Produkt im Rahmen der Evaluierung analysiert worden ist. Gerade wenn die direkte oder indirekte Nutzung von IT reguliert wird, ist es für die Akzeptanz durch den Anwender unerlässlich, dessen Sicherheitsbedürfnis objektiv und transparent zu erfüllen. Dies sind wichtige technische Eckpfeiler für die Sicherheit für Großprojekte der Bundesregierung im Rahmen gesetzlicher Initiativen, die jede Bürgerin und jeden Bürger erreichen, sei es in Form des neuen Personalausweises, des elektronischen Reisepasses, der elektronischen Gesundheitskarte oder der intelligenten Messsysteme wie zum Beispiel im Bereich der Stromzähler.

Bei den vom BSI verantworteten Zertifizierungsverfahren arbeitet das Amt eng mit den Herstellern sowie den von ihnen beauftragten Prüflaboren zusammen und erörtert dabei konkrete Sicherheitsfragen und -lösungen, die sich aus den Produktprüfungen und -analysen ergeben. Dabei geht es oftmals um Fragestellungen aus Bereichen wie

- Umsetzung sicherheitskritischer Produktänderungen

- konkrete Einbindung von Kryptoverfahren in IT-Sicherheitsprodukte
- Integration von neuen Produktions- und Entwicklungsstandorten bei Herstellern
- Einzelfragen im Kontext von Korrektheitsprüfungen bei Sicherheitsfunktionen
- Umgang mit und Berücksichtigung von produktbezogenen IT-Schwachstellen-Informationen durch Prüflabore und Hersteller, etwa bei der Simulation von Seitenkanal-Angriffen
- Eignung der Implementierung neuer Sicherheitsfunktionalitäten.

Erst wenn alle Fragen geklärt und die in den Schutzprofilen oder Technischen Richtlinien vorgeschriebenen Sicherheits- und Funktionsvorgaben durch den Hersteller nachvollziehbar umgesetzt worden sind, stellt das BSI ein entsprechendes Zertifikat aus. Dieses Zertifikat belegt, dass das geprüfte Produkt die versprochenen Eigenschaften auch tatsächlich besitzt.

Im Jahr 2015 hat das BSI insgesamt 271 Zertifikate ausgestellt, darunter 61 Common-Criteria-Zertifikate. Aktuell (Stand: Juli 2016) bearbeitet das BSI allein 149 Common-Criteria-Zertifizierungsverfahren.

4.3 IT-Sicherheit für die Gesellschaft

Die Digitalisierung erfasst immer mehr Lebens- und Arbeitsbereiche. Laut Bitkom nutzen mehr als 80 Prozent aller Deutschen inzwischen das Internet, über die Hälfte der Menschen in Deutschland tut dies mobil per Smartphone oder Tablet. Immer mehr Menschen nutzen smarte Haushaltsgeräte, steuern ihre Rollläden per App oder tätigen Bank- und andere Geschäfte online. Neben den immensen Vorteilen, die diese neuen Technologien und Möglichkeiten mit sich bringen, vergrößern sie auch die Angriffsfläche für Cyber-Angriffe und andere Risiken des Internets. Je abhängiger die Gesellschaft von funktionierender Informationstechnik und sicheren Informationsinfrastrukturen wird, desto mehr Bedeutung erlangt auch die IT-Sicherheit für die Bürgerinnen und Bürger.

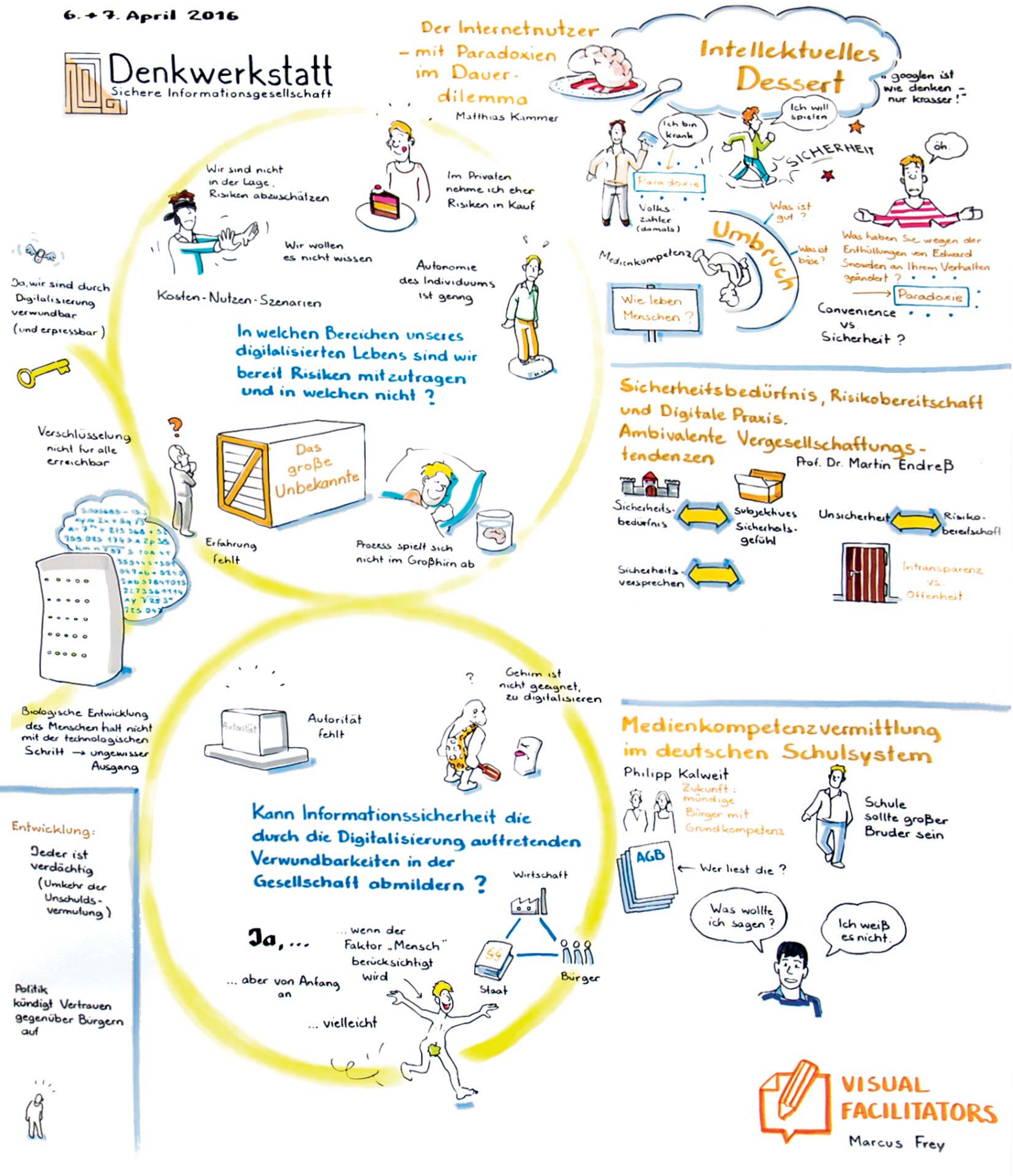
4.3.1 BSI bietet Plattform für gesellschaftlichen Diskurs

Dem BSI geht es daher darum, den gesellschaftlichen Diskurs zu Themen der Cyber-Sicherheit anzustoßen und voranzutreiben. Das BSI bietet dazu Plattformen für einen offenen Interessenaustausch zwischen verschiedenen gesellschaftlichen Bereichen. Im April 2016 hat das BSI beispielsweise Vertreter aus Zivilgesellschaft, Wissenschaft, Wirtschaft und Verwaltung zur „Denkwerkstatt sichere Informationsgesellschaft“ eingeladen. Bei der zweitägigen Veranstaltung haben sich 51 Teilnehmer mit den Themen der digitalen Zukunft auseinandergesetzt.

Die sicherheitsrelevanten Auswirkungen der Digitalisierung auf die Gesellschaft standen im Zentrum zahlreicher konstruktiver Debatten, die teils im Plenum, aber auch in Kleingruppen, etwa in Form eines „World Cafés“, geführt wurden. Das Format der Veranstaltung hat dazu angeregt, Standpunkte zu hinterfragen und weiterzuentwickeln, Kontroversen anzustoßen, aber auch mögliche Überschneidungen von Interessen ganz unterschiedlicher Akteure zu erkennen, die bisher nicht offenkundig geworden sind. Dabei ist es gelungen, ein breites Spektrum an Positionen zu versammeln, um unterschiedliche Herangehensweisen an Themen, wie etwa die Schaffung entsprechender Anreizstrukturen für mehr Informationssicherheit, Medienkompetenzvermittlung im Schulsystem, Fragen des Datenschutzes oder der Sicherheitsverantwortung und vieles mehr zu diskutieren. Das Ergebnis des Workshops bilden „Sieben Thesen für eine sichere Informationsgesellschaft“, die im Konsens verabschiedet wurden und auf der Webseite des BSI abrufbar sind.

Die Denkwerkstatt ist Initialzündung für weitere Projekte und Veranstaltungen. Das BSI wird den gesamtgesellschaftlichen Diskurs zu Themen der IT-Sicherheit fortführen, um auch weiterhin Cyber-Sicherheit mit der Gesellschaft für die Gesellschaft zu gestalten.


Herzlich Willkommen!
Bundesamt für Sicherheit in der Informationstechnik
Schwieriges Thema
Ziel für morgen
Versuch:
Thesenpapier
Keine Schere im Kopf
Vertrauen!
Warum Denkwerkstatt?
IT
in den Fokus
IT SICHERHEIT
Wir sind mittendrin!
AUFBRUCH
Haben wir ein digitales Immunsystem?
Haben wir einen digitalen Gesellschaftsvertrag?
Wer ist „wir"?
Was ist Digitalisierung?
Mehr Möglichkeiten – mehr Gefahren
Vertrauen
Transparenz
Wie unsicher ist sicher genug?
Wir kennen es nicht
Restrisiko
(schlimmes Wort)
1 Technische Entwicklungen
2 Nutzungsmuster
3 Andere Denkansätze
Perspektiv-wechsel
Das tut man nicht unter Freunden!
Computerisierte Allgegenwart
Verschiebung vom öffentlichen und privatem
Entgrenzungen
Abhängigkeiten
Sicherheitskultur
Macht uns die Digitalisierung verwundbar und wenn ja inwiefern?
IT SICHERHEIT ist Vertrauensfrage
da lang
Interessen zur Beeinflussung der Gesellschaft
Sichere Kommunikation
kein Ende!
privat wirtschaftlich
für politische Debatten
führt zu Innovation
Verschlüsselung
Kryptografie
verbieten?
Code ist freie Meinungs-äußerung
führt ins Leere
Sicherheit als demokratisches Dilemma
Überleben
politische Strategie
SICHERHEIT
ist ein kaleidoskopischer Begriff
geschlossene Diskursgruppen zusammen-bringen
Vertrauen
Schmierstoff der Gesellschaft
Informations-sicherheit
lässt sich nicht isoliert betrachten


6.+7. April 2016
Denkwerkstatt
Sichere Informationsgesellschaft
Der Internetnutzer – mit Paradoxien im Dauer-dilemma
Matthias Kammer
Intellektuelles Dessert
„ googlen ist wie denken – nur krasser !"
Ich will spielen
Ich bin krank
SICHERHEIT
Paradoxie
Volks-zähler (damals)
Was ist gut ?
Was ist böse ?
Medienkompetenz
Umbruch
Wie leben Menschen ?
öh.
Was haben Sie wegen der Enthüllungen von Edward Snowden an Ihrem Verhalten geändert ?
Paradoxie
Convenience vs Sicherheit ?
Wir sind nicht in der Lage, Risiken abzuschätzen
Wir wollen es nicht wissen
Im Privaten nehme ich eher Risiken in Kauf
Kosten-Nutzen-Szenarien
Autonomie des Individuums ist genug
Ja, wir sind durch Digitalisierung verwundbar (und erpressbar)
In welchen Bereichen unseres digitalisierten Lebens sind wir bereit Risiken mitzutragen und in welchen nicht ?
Sicherheitsbedürfnis, Risikobereitschaft und Digitale Praxis. Ambivalente Vergesellschaftungs-tendenzen
Prof. Dr. Martin Endreß
Sicherheits-bedürfnis
subjektives Sicherheits-gefühl
Unsicherheit
Risiko-bereitschaft
Sicherheits-versprechen
Intransparenz vs. Offenheit
Verschlüsselung nicht für alle erreichbar
Das große Unbekannte
Erfahrung fehlt
Prozess spielt sich nicht im Großhirn ab
Biologische Entwicklung des Menschen hält nicht mit der technologischen Schritt → ungewisser Ausgang
Autorität
Autorität fehlt
Gehirn ist nicht geeignet, zu digitalisieren
Kann Informationssicherheit die durch die Digitalisierung auftretenden Verwundbarkeiten in der Gesellschaft abmildern ?
Ja, ...
... wenn der Faktor „Mensch" berücksichtigt wird
... aber von Anfang an
... vielleicht
Wirtschaft
Staat
Bürger
Medienkompetenzvermittlung im deutschen Schulsystem
Philipp Kalweit
Zukunft: mündige Bürger mit Grundkompetenz
Schule sollte großer Bruder sein
AGB
Wer liest die ?
Was wollte ich sagen ?
Ich weiß es nicht.
Entwicklung:
Jeder ist verdächtig (Umkehr der Unschulds-vermutung)
Politik kündigt Vertrauen gegenüber Bürgern auf
VISUAL FACILITATORS
Marcus Frey

4.3.2 Die Bürger-Services des BSI

Gemäß seinem gesetzlichen Auftrag gehört es zu den Aufgaben des BSI, die Bürgerinnen und Bürger für einen sicheren Umgang mit Informationstechnologie, mobilen Kommunikationsmitteln und dem Internet zu informieren und zu sensibilisieren. Über die Risiken Bescheid zu wissen ist der erste Schritt, diese zu bewältigen. Das BSI bietet daher unter *www.bsi-fuer-buerger.de* ein speziell für die Bürger zugeschnittenes Internetangebot. Die vielfältigen Themen und Informationen rund um das Thema IT- und Internet-Sicherheit werden dort so behandelt, dass sie auch für technische Laien verständlich sind. Neben der reinen Information bietet das BSI auch konkrete und umsetzbare Handlungsempfehlungen an, beispielsweise zu Themen wie E-Mail-Verschlüsselung, Smartphone-Sicherheit, Smart Home oder Soziale Netzwerke.

Im November 2015 erfolgte der Relaunch der Webauftritte des BSI. Das Bürger-Angebot *www.bsi-fuer-buerger.de* zeichnet sich nun ebenso wie die BSI-Webseiten *www.bsi.bund.de* und *www.allianz-fuer-cybersicherheit.de* durch eine höhere Aktualität, moderne Gestaltung und nutzerfreundliche Struktur aus. Die vormalige Trennung zwischen stationärem und mobilem Internet ist aufgehoben, die Informationen und Empfehlungen lassen sich leichter finden. Mit ihrem Responsive Design passen sich alle Webseiten automatisch der Bildschirmgröße des jeweiligen Geräts an. Das neu gestaltete Webangebot wird von den Internetnutzern sehr gut angenommen: Seit dem Relaunch ist ein erheblicher Anstieg der Seitenaufrufe des Bürger-Informationsangebots zu verzeichnen, von durchschnittlich 151.072 Besuchern pro Monat im Zeitraum Juli 2014 bis Juni 2015 auf durchschnittlich 172.592 Besucher pro Monat im Zeitraum Juli 2015 bis Juni 2016.

Darüber hinaus bietet das BSI mit dem „Bürger-CERT“ einen kostenlosen Warn- und Informationsdienst, mit dem sich derzeit 102.137 Abonnenten schnell und kompetent über Schwachstellen, Sicherheitslücken und andere Risiken informieren. Die Experten des BSI analysieren rund um die Uhr die Sicherheitslage im Internet und verschicken bei Handlungsbedarf Warnmeldungen und Sicherheitshinweise per E-Mail.

Auch über die Facebook-Seite (*www.facebook.com/bsi.fuer.buerger*) und den seit März 2016 aktiven Twitter-Kanal (*www.twitter.com/BSI_Presse*) des BSI haben Internetnutzer die Möglichkeit, sich über IT-Sicherheit zu informieren und zu aktuellen Themen und Fragestellungen der IT-Sicherheit mit dem BSI in den Dialog zu treten. Zum Stichtag 30. Juni 2016 taten dies 25.983 Fans (Facebook) und 1.871 Follower (Twitter). Auch telefonisch oder per E-Mail steht das BSI für Anfragen der Bürgerinnen und Bürger zu Themen der IT- und Internetsicherheit zur Verfügung. Das Service-Center des BSI nimmt jeden Monat durchschnittlich rund 400 Anfragen von Privatanwendern entgegen.

4.3.3 Kooperativ für mehr IT-Sicherheit

Die Herausforderungen der Cyber-Sicherheit kann niemand allein lösen. Daher verfolgt das BSI auch im Bereich der Sensibilisierung der Öffentlichkeit für die Risiken und Möglichkeiten der Informationstechnologie einen kooperativen Ansatz und arbeitet mit einer Reihe von Einrichtungen zusammen. Eine dauerhafte Zusammenarbeit hat sich beispielsweise mit „Deutschland – Sicher im Netz“ oder bei bürgerbezogenen Aktivitäten mit der ENISA (Europäische Agentur für Netz- und Informationssicherheit) etabliert. Darüber hinaus gibt es anlassbezogene Aktivitäten mit Einrichtungen wie der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK), dem Bundeskriminalamt, klicksafe oder den Verbraucherzentralen. Diese Kooperationen werden zukünftig weiter intensiviert und ausgebaut.

Im Oktober 2015 fungierte das BSI als nationaler Hauptakteur bei der Gestaltung des Europäischen Cyber-Sicherheits-Monats (ECSM) mit weitreichenden Sensibilisierungs- und Informationsangeboten für Bürger und KMU. Das BSI ist dabei sowohl nationale Koordinierungsstelle zur Gewinnung von Partnern für den Aktionsmonat als auch Akteur mit eigenen Aktionen und Angeboten. Auf Initiative des BSI beteiligten sich 2015 20 Partner mit Sensibilisierungsmaßnahmen am ECSM in Deutschland. Das BSI erstellte unter anderem ein Quiz, mit dem Anwender auf *www.bsi-fuer-buerger.de* ihr Wissen über IT-Sicherheit testen konnten, und startete auf seiner Facebook-Seite ein Beratungsangebot, bei dem Fachleute die Fragen von Privatanwendern beantworteten. Gemeinsam mit der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK) führte das BSI während des Aktionsmonats eine Online-Umfrage durch, die unter anderem die von Privatanwendern genutzten Schutzmaßnahmen und ihre Erfahrungen mit Cyber-Kriminalität erhob.

4.3.4 Verschlüsselung schafft Vertrauen

Im Rahmen des Nationalen IT-Gipfels 2015 wurde die auf Initiative des Bundesinnenministeriums erstellte „Charta zur Stärkung der vertrauenswürdigen Kommunikation“ vorgestellt. Neben dem BMI und einigen namhaften Unternehmen und Institutionen gehört auch das BSI zu den Unterzeichnern der Charta. Erklärtes Ziel der Unterzeichner ist es, die vertrauenswürdige Kommunikation insbesondere durch Förderung und Umsetzung von Ende-zu-Ende-Verschlüsselung zu stärken. Die Charta enthält eine Reihe von entsprechenden Bekenntnissen und kann dabei helfen, Rahmenbedingungen zu formulieren, die die bereits zahlreich vorhandenen Aktivitäten bündeln und fokussieren.

Die von der Bundesregierung beschlossene Digitale Agenda gibt das Ziel aus, Deutschland zum „Verschlüsselungsstandort Nr. 1“ zu machen, zum Schutz der Bürger, der Wirtschaft und der Verwaltung. Zur sicheren Kommunikation im Internet treibt das BSI daher uneingeschränkt den Einsatz von Verschlüsselungslösungen voran. Im Einklang mit der Digitalen Agenda empfiehlt das BSI Bürgerinnen und Bürgern ebenso wie Wirtschaftsunternehmen, zum Schutz der Privatsphäre bzw. zum Schutz geschäftlich relevanter Informationen vor Ausspähung Verschlüsselung einzusetzen. Aus informationstechnischer Sicht ist insbesondere die Entwicklung, Bereitstellung und durchgängige Anwendung vertrauenswürdiger Krypto- und Cyber-Technologien für Unternehmen, Verwaltung und Bürger von entscheidender Bedeutung, um die aus der kritischen Gefährdungslage resultierenden Risiken zu minimieren. Grundvoraussetzung für die Gewährleistung von Informationssicherheit sind effektive und vertrauenswürdige Sicherheitsmechanismen auf technischer Ebene.

4.3.5 Flächendeckend sicherer E-Mail-Transport

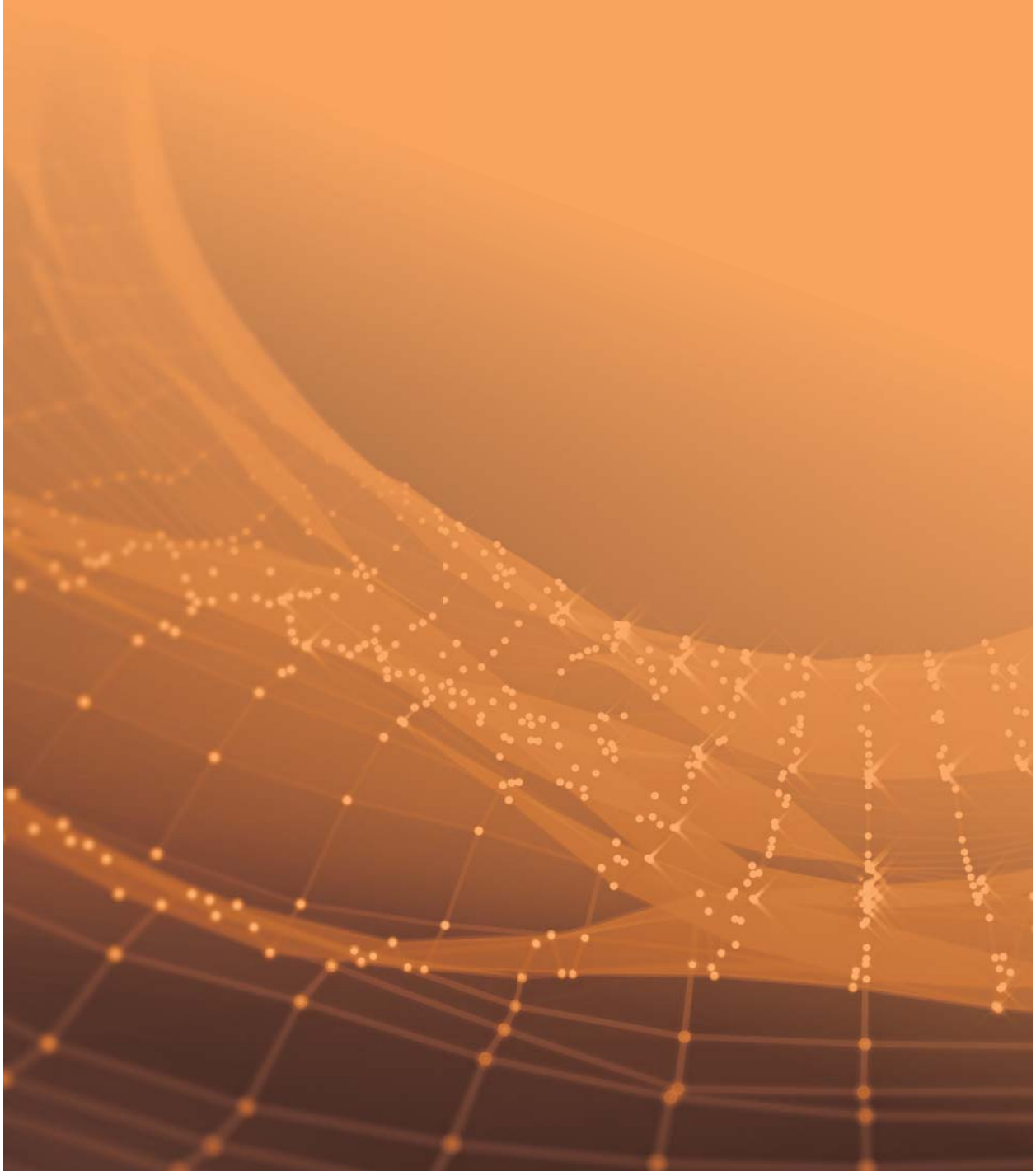
Ein Großteil der digitalen Kommunikation findet heute immer noch schnell und komfortabel per E-Mail statt. Vernachlässigt wird in der Praxis jedoch häufig die konsequente Anwendung von IT-Sicherheit. Um dem entgegenzuwirken, hat das BSI mit der Technischen Richtlinie „Secure E-Mail Transport (BSI TR-03108)“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

Marktbewährte Anforderungen, kooperative Lösung

Bereits der 2015 veröffentlichte Entwurf der Technischen Richtlinie wurde im Dialog mit am Markt tätigen E-Mail-Diensteanbietern erstellt. Das dem Entwurf zugrunde liegende Konzept wurde dabei stetig weiterentwickelt, wobei die IT-Sicherheit, Praxistauglichkeit und Nutzerakzeptanz im Vordergrund standen. Kern des Konzepts ist, dass durch die Technische Richtlinie kein neues in sich geschlossenes System entsteht, sondern die IT-Sicherheit der bereits existierenden offenen E-Mail-Infrastruktur angehoben wird. In einer vom BSI gegründeten Arbeitsgruppe mit mehr als 20 Mitgliedern wurde der Entwurf kooperativ fortentwickelt und finalisiert. Bemerkenswert ist dabei, dass die Anforderungen der Technischen Richtlinie nicht nur präzisiert, sondern in Abstimmung mit der Arbeitsgruppe erhöht wurden, sodass ehemals als optional markierte Anforderungen in der finalen Version verpflichtend geworden sind. Neben der Verwendung hochwertiger Kryptoverfahren zeichnen signierte DNS-Abfragen, obligatorische Verschlüsselung und vertrauenswürdige Zertifikate die Anforderungen der Technischen Richtlinie aus.

Schon jetzt erfreut sich die Technische Richtlinie großer Akzeptanz; erste Anbieter haben bekundet, die Anforderungen der TR bereits umzusetzen. Das BSI entwickelt derzeit ein Zertifizierungsverfahren für die Technische Richtlinie, sodass solche Bekundungen zukünftig auch gegenüber Dritten nachweisbar sein werden. Ziel ist, dass die Technische Richtlinie künftig auch in Branchen akzeptiert und umgesetzt wird, in denen der Versand von E-Mails nicht zum Kerngeschäft, aber zum Alltag gehört, beispielsweise bei Versicherungen, Banken und Behörden. Entsprechendes Interesse wurde dem BSI bereits von verschiedenen Stellen signalisiert und auch international wird die Technische Richtlinie mit großem Interesse verfolgt.

5 Gesamtbewertung und Fazit



5 Gesamtbewertung und Fazit

Aus dem vorliegenden Lagebericht des Bundesamts für Sicherheit in der Informationstechnik wird unumwunden deutlich, dass die Komplexität der Bedrohungslage ebenso wie die damit einhergehenden Gefahren für die fortschreitende Digitalisierung zunimmt. Die Frage der Sicherheit der eingesetzten Informationstechnik stellt sich damit nicht mehr nur nebenbei. Sie stellt sich auch nicht länger nur einem eingeweihten Kreis der IT-Spezialisten. Vielmehr ist die Informationssicherheit wesentliche Vorbedingung für das Gelingen der Digitalisierung in Deutschland geworden.

Die Gefährdungslage ist weiterhin angespannt. Zusätzlich zu bereits bekannten Phänomenen kann das BSI aber auch eine neue Qualität in der Bedrohung feststellen. Die bekannten Einfallstore für Cyber-Angriffe bleiben im Wesentlichen unverändert kritisch:

- In den am häufigsten eingesetzten Soft- und teilweise auch Hardwareprodukten finden sich Schwachstellen, welche es Angreifern erlauben, Informationen abfließen zu lassen oder die Kontrolle über die Systeme zu erlangen.
- Organisiert aufgebaute und betriebene Botnetze stehen für die Angreifer zur Verfügung, um Schadsoftware oder Spam-E-Mails massenhaft zu verteilen. Ebenso können diese Botnetze für Angriffe auf die Verfügbarkeit von Diensten erfolgreich eingesetzt werden.
- Anwender setzen auch gängige und einfache Sicherheitsmaßnahmen häufig nicht oder nicht hinreichend um.
- Durch anonyme Zahlungsmethoden wie beispielsweise Bitcoin ergeben sich neue Möglichkeiten für Cyber-Kriminelle in der Vermarktung von Angriffswerkzeugen, aber auch in der Erpressung.

Die sprunghaft angestiegenen Fälle von Ransomware verdeutlichen eindrucksvoll, wie verwundbar mittlerweile das alltägliche Leben für Cyber-Angriffe geworden ist. Der Zugriff auf die eigenen Daten wird zunehmend essenziell – nicht nur für Unternehmen, sondern auch für den einzelnen Bürger. Diesen Umstand nutzen Cyber-Kriminelle aus und halten die Daten des Opfers und die digitale Identität als Geisel. Wenn sogar Krankenhäuser mit ihren vernetzten Systemen betroffen sind und ihr Betrieb hierdurch beeinträchtigt wird, sind Cyber-Angriffe endgültig in der realen Welt angekommen.

Ebenso muss das BSI feststellen, dass die Bedrohung für Staat und Wirtschaft durch professionelle und vermutlich staatlich gelenkte Angreifergruppen weiterhin hoch ist. Die einschlägigen Beispiele – wie etwa noch 2015 der Angriff auf die IT-Systeme des Deutschen Bundestages oder aktuell Angriffe auf die im Bundestag vertretenen Parteien – illustrieren die politische Dimension und Wirkrichtung der Cyber-Angriffe.

Cyber-Sicherheit: Voraussetzung für erfolgreiche Digitalisierung

Ein automatisiertes Auto wird ohne höchste Sicherheitsgarantien niemals allein fahren können. Die Versorgung der Bevölkerung mit wesentlichen Gütern kann industriellen Steuerungssystemen ohne funktionierende Absicherung nicht überantwortet werden. Die Wertschöpfung der deutschen Wirtschaft durch Vorsprung in Know-how und Technik darf nicht durch Industriespionage gefährdet werden. Jeder Einzelne will in den Genuss der Verheißungen der immer komplexeren Informationstechnik kommen – sei es durch unbegrenzten Zugang zu Informationen, zur Steuerung der heimischen IT oder schlicht der Unterhaltung. Die Sicherheit der eingesetzten Systeme muss dabei von vornherein gewährleistet sein.

Den hieraus erwachsenden großen Herausforderungen begegnen die Mitarbeiterinnen und Mitarbeiter des BSI in der täglichen Arbeit im Zusammenwirken mit vielen weiteren Partnern. Das BSI hat auch im Berichtszeitraum von Juli 2015 bis Juni 2016 unter Beweis gestellt, dass es handlungsfähig im Angesicht der Bedrohung ist und diese wirksam bekämpft:

- Das BSI hat die Regierungsnetze erfolgreich geschützt. Auch hochspezialisierte Angriffe konnten frühzeitig entdeckt und abgewehrt werden. Selbst zunächst erfolgreiche Infektionen mit Schadsoftware auf Systemen der Bundesverwaltung wurden durch die zahlreichen Abwehr- und Erkennungsmaßnahmen frühzeitig aufgedeckt und bereinigt.
- Betroffene außerhalb der Regierungsnetze wurden durch das BSI vor aktuellen Bedrohungen gewarnt und bei der Ergreifung von Gegenmaßnahmen unterstützt. Im Falle erfolgreicher Angriffe hat das BSI vor Ort Unterstützung geleistet – eine Leistung, die angesichts der geringen Größe des BSI mit etwa 660 Mitarbeitern nur der Start für künftige Bemühungen sein wird.

- Im international wichtigen Bereich der Standardisierung und Zertifizierung nimmt das BSI eine herausgehobene Rolle ein. Bei der IT-Sicherheitszertifizierung ist das BSI die weltweit führende Stelle.

- Für die Sicherheit der Kritischen Infrastrukturen in Deutschland hat das BSI durch das IT-Sicherheitsgesetz eine neue Aufgabe übertragen bekommen. In enger Kooperation mit den jetzt im Fokus stehenden Branchen und Unternehmen werden sinnvolle und umsetzbare Maßnahmen entwickelt, um die Versorgung der Bevölkerung sicherzustellen. Das BSI steht bereit, um seine Rolle als Aufsichtsbehörde über diesen Bereich der Wirtschaft zu erfüllen.

Ebenso hat das BSI im abgelaufenen Berichtszeitraum wesentliche Grundsteine für die jetzt kommenden weiteren Entwicklungen gelegt. Zu Recht wird an das BSI vermehrt die Erwartung herangetragen, sich jenseits eines engen Aufgabenverständnisses mehr gegenüber Verwaltung, Unternehmen sowie den Bürgern zu öffnen und Angebote zu machen. Das BSI hat dies mit seinem Leitsatz: „Das BSI als die nationale Cyber-Sicherheitsbehörde gestaltet die Informationssicherheit in der Digitalisierung für Staat, Wirtschaft und Gesellschaft“ aufgegriffen und konnte im Berichtszeitraum bereits erste Grundsteine zur Umsetzung dieses Anspruchs legen.

So hat das BSI seine Zusammenarbeit mit Staat und Wirtschaft intensiviert. Hierzu wurden nicht nur bereits bestehende Kooperationsplattformen wie UP KRITIS und die Allianz für Cyber-icherheit erweitert und gestärkt. Darüber hinaus prägt das BSI die entscheidenden Standards der Informationssicherheit mit besonderer Beachtung der Umsetzbarkeit in der Wirtschaft – von der Neuausrichtung des IT-Grundschutzes bis hin zu besonderen Standards der Industrie 4.0. Weiterhin bietet das BSI die Sicherheitszertifizierung an, mit der die Wirtschaft im Markt den Nachweis der umgesetzten Sicherheitsstandards führen kann.

In den großen Digitalisierungsprojekten in Deutschland bringt sich das BSI verstärkt ein und wird hier übergreifend für staatliche und private Akteure im Sinne der Gewährleistung der Sicherheit tätig. So leistet das BSI seinen Beitrag zum Gelingen der Energiewende durch die Erarbeitung von Sicherheitskriterien für die Infrastruktur der intelligenten Stromzähler und es unterstützt bei der Erarbeitung der Sicherheitsaspekte einer Verkehrsinfrastruktur, in der autonome oder hochautomatisierte Fahrzeuge Realität werden. Darüber hinaus hat das BSI die wesentlichen Sicherheitsanker der elektronischen Gesundheitskarte und der dazu notwendigen Systeme mitgestaltet und zertifiziert. Gleichzeitig konnte das BSI auch Standards und Empfehlungen für die Wirtschaft herausgeben, wie etwa Empfehlungen für eine sichere E-Mail-Infrastruktur, die bereits aufgegriffen werden.

Für Bürgerinnen und Bürger unterhält das BSI darüber hinaus ständig aktualisierte Informationsangebote – von Hinweisen und Tipps zum Umgang mit IT bis hin zu Konfigurationsanleitungen für den heimischen PC. Erweitert werden die Bürgerservices um Angebote zur Sensibilisierung und Hilfestellung. Diesen Bereich werden wir künftig noch weiter stärken.

Das IT-Sicherheitsgesetz in der Umsetzung

Das IT-Sicherheitsgesetz ist seit Juli 2015 in Kraft getreten. Zur Umsetzung des Gesetzes sind Verordnungen erforderlich, welche die vom Gesetz erfassten Bereiche der Kritischen Infrastrukturen konkretisieren. Eine erste Verordnung hierzu ist im Mai 2016 in Kraft getreten. Sie erfasst die KRITIS-Sektoren Energie, Informationstechnik und Telekommunikation, Wasser und Ernährung. Die nächste Verordnung wird für das Frühjahr 2017 erwartet und wird die Sektoren Finanzen, Transport und Verkehr sowie Gesundheit abdecken. Die betroffenen Branchen müssen jeweils sechs Monate nach Inkrafttreten der Verordnungen ihre Pflichten aus dem Gesetz erfüllen – erstmals also ab November 2016.

Der Erlass des IT-Sicherheitsgesetzes entfaltet bereits erste Wirkungen. So erfüllen einzelne Unternehmen in den erfassten Bereichen bereits im Vorgriff auf den Stichtag ihre gesetzlichen Verpflichtungen zur Meldung von IT-Sicherheitsvorfällen und zur Absicherung ihrer IT-Systeme entsprechend dem Stand der Technik. Ebenso wurden bereits branchenspezifische Arbeitskreise unter dem UP KRITIS gebildet. Die Teilnehmerzahl des UP KRITIS hat sich zwischenzeitlich verdoppelt auf aktuell 380 Organisationen.

BSI gestaltet Informationssicherheit in der Digitalisierung

Die von Cyber-Angriffen und sonstigen IT-Sicherheitsvorfällen besonders betroffenen Gruppen müssen sich besser aufstellen, um den künftigen Herausforderungen gerecht zu werden. Das BSI wird hierzu seine Unterstützungsangebote in der Fläche ausbauen.

Dies entlässt jedoch die Wirtschaft nicht aus ihrer Verantwortung, auch die eigenen Maßnahmen zur Prävention und Sensibilisierung auszubauen. Das BSI steht bereit, um bei der Gestaltung der einzelnen Maßnahmen zu unterstützen. Ebenso besteht ein großer Bedarf an erweiterten Detektions- und Reaktionsfähigkeiten in der Wirtschaft. Das BSI wird Initiativen hierzu begleiten und wo sinnvoll selbst tätig werden. Im Bereich der Kritischen Infrastrukturen kann ein vordringlicher Bedarf hieran festgestellt werden, aber in der Fläche bei den kleinen und mittleren Unternehmen (KMU) muss sich ebenfalls etwas bewegen. Die im Berichtszeitraum schon angelegten Veränderungen wird das BSI in dieser Hinsicht fortführen. Erste Schritte zu mehr unmittelbarer Kooperation mit der Wirtschaft sind bereits erfolgt. So wurde kürzlich eine individuelle Kooperationsvereinbarung mit der Volkswagen AG abgeschlossen, Ähnliches ist auch mit der Continental AG geplant. Ebenso geht das BSI gesammelt auf alle DAX- und MDAX-Unternehmen zu, um die Zusammenarbeit zu intensivieren. Erste Ergebnisse dieser Kooperationen sind sehr vielversprechend.

Das Funktionieren der staatlichen Informationstechnik steht im besonderen Interesse des Gemeinwesens. Das BSI wird die Schutzmaßnahmen für das Regierungsnetz daher kontinuierlich der veränderten Bedrohungslage anpassen. Ebenso wird das BSI verstärkt mit den Ländern zusammenarbeiten und seine Unterstützungsangebote ausbauen. Durch die stetige Verbesserung der Lageinformationen kommt das BSI schnell in den Besitz der hierfür erforderlichen Informationen und kann seinen Auftrag erfüllen. Zur Verbesserung der Reaktionsfähigkeit des BSI bei besonderen Cyber-Lagen werden Mobile-Incident-Response-Teams (MIRT) zur Unterstützung akut betroffener Stellen eingerichtet.

Das BSI hat aktuell Angriffe auf Parteien, Medien und staatliche Einrichtungen beobachtet, welche die Sorge vor einer gezielten Manipulation der öffentlichen Meinung durch Dritte begründen. Das BSI beobachtet die Lage gerade diesbezüglich intensiv und wird sich für den Zeitraum der Bundestagswahl in besonderer Weise aufstellen, um möglichen Cyber-Angriffen begegnen zu können.

Den Herausforderungen der Digitalisierung stellt sich das BSI auch mit seinen internationalen Partnern. Da die Angriffe zumeist eine internationale Komponente aufweisen, ist dies eine essenzielle Informationsquelle für das BSI, die weiter ausgebaut werden wird.

Die Digitalisierung mit ihren Chancen und Risiken ist in vollem Gange. Die durch sie angestoßenen Veränderungen sind durchgreifend und werden Deutschland verändern. Das BSI stellt sich auch weiterhin der Aufgabe, die Informationssicherheit zu gestalten und somit zum Erfolg der Digitalisierung in Staat, Wirtschaft und Gesellschaft beizutragen. Eine erfolgreiche Digitalisierung von Staat, Wirtschaft und Gesellschaft wird es ohne Cyber-Sicherheit nicht geben.

6 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 dauerhaften Zugriff zu einem Netzwerk verschafft und diesen in der Folge auf weitere Systeme ausweitet. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten aufseiten der Angreifer aus und sind in der Regel schwierig zu detektieren.

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

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

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 Infrastrukturen (Rechenleistung, Speicherplatz), Plattformen und Software.

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

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

Drive-by-Exploits / Drive-by-Download
Drive-by-Exploits oder Drive-by-Downloads 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.

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.

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

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 Plugins zu finden und zur Installation von Schadprogrammen zu verwenden.

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

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

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

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.

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

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.

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

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

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).

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.

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

Impressum

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik (BSI)

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

E-Mail
bsi@bsi.bund.de

Telefon
+49 (0) 22899 9582-0

Telefax
+49 (0) 22899 9582-5400

Stand
Oktober 2016

Druck
Druck- und Verlagshaus Zarbock Frankfurt am Main

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

Bildnachweis
alle Bilder: iStock.com/jm1366

Grafiken
BSI

Artikelnummer
BSI-LB16/505

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

www.bsi.bund.de