Bundesamt
für Sicherheit in der
Informationstechnik

Die Lage der IT-Sicherheit in Deutschland 2015

Inhaltsverzeichnis

Vorwort

Mit dem Bericht zur Lage der IT-Sicherheit in Deutschland 2015 informiert das Bundesamt für Sicherheit in der Informationstechnik (BSI) über Art und Umfang der einschlägigen IT-Gefährdungen und daraus resultierende Risiken. Grundlage sind die vom BSI ausgewerteten Informationen über Schwachstellen und Verwundbarkeiten der heute genutzten Informationstechnik sowie über Angriffe auf IT-Systeme und Netze.

Der Bericht zeigt, dass die Anzahl der Schwachstellen und Verwundbarkeiten in IT-Systemen weiterhin auf einem sehr hohen Niveau liegt. Einige dieser Schwachstellen offenbaren schwerwiegende Sicherheitslücken. Die asymmetrische Bedrohungslage im Cyber-Raum spitzt sich weiter zu. Das bedeutet: Der Schutz der IT-Systeme durch die Anwender kann mit den oft hoch entwickelten Werkzeugen zur Ausnutzung von Sicherheitslücken nicht immer Schritt halten.

Folgende Entwicklungen fallen bei der Lektüre des Lageberichts darüber hinaus besonders auf:

Erstens: Angesichts der hohen Zahl von erkannten Schwachstellen tendieren einige IT-Hersteller dazu, für die aus ihrer Sicht weniger schwerwiegenden Sicherheitslücken in ihren Produkten keine Sicherheitsupdates mehr bereitzustellen. Das verschärft die Gefährdungslage unnötig.

Zweitens: Die Zahl der Angriffe auf industrielle Produktionsanlagen steigt. Hierdurch entstehen neue betriebs- und volkswirtschaftliche Risiken.

Und drittens: Aspekte der IT-Sicherheit werden bei der Digitalisierung nicht immer ausreichend berücksichtigt, und zwar auch dann nicht, wenn ein Ausfall der betreffenden Systeme zu weitreichenden persönlichen oder gesellschaftlichen Folgen führen kann.

Das Ende Juli 2015 in Kraft getretene IT-Sicherheitsgesetz ist ein erster wichtiger Schritt, damit die IT-Systeme und digitalen Infrastrukturen in unserem Land besser geschützt werden. Wir wollen, dass sie zu den sichersten weltweit gehören. Mit dem BSI als staatlichem Kompetenzzentrum für Fragen der IT-Sicherheit ist Deutschland hier gut aufgestellt. Trotzdem: Weder Staat noch Wirtschaft können die IT-Sicherheit in unserem Land allein erreichen. Jeder muss seinen Teil dazu beitragen. Wir müssen daher die Zusammenarbeit zwischen Wirtschaft und Staat intensivieren und auch neue Formen der Zusammenarbeit finden. Wir müssen gemeinsam einen Beitrag leisten, um Bürgerinnen und Bürger für die Risiken zu sensibilisieren und ihnen Wege zum sicheren Handeln im Netz aufzeigen. Je sicherer sich jeder Einzelne im Netz bewegt, umso besser können Staat und Gesellschaft im Netz geschützt werden.

Die digitalen Verwundbarkeiten unserer Gesellschaft werden uns in den kommenden Jahren weiter fordern. Der vorliegende Bericht des BSI zur Lage der IT-Sicherheit in Deutschland bietet die Grundlage für Entscheider in Staat, Wirtschaft und Gesellschaft, um den mit der Digitalisierung einhergehenden Risiken für unser Land angemessen begegnen zu können. Deshalb wünsche ich diesem Bericht zahlreiche Leserinnen und Leser, die erkennen, wo sie betroffen sind, und dann auch danach handeln.

Dr. Thomas de Maizière
Bundesminister des Innern

1 IT-Sicherheit im Spannungsfeld von Innovation, Globalisierung und Komplexität

1 IT-Sicherheit im Spannungsfeld von Innovation, Globalisierung und Komplexität

Ausdruck der ungebrochen hohen Innovationsgeschwindigkeit der Informationstechnologie ist ihre enorme Veränderungskraft und rasante Durchdringung aller Lebens- und Wirtschaftsbereiche. Der Sättigungsbereich des möglichen Einsatzes von IT ist noch nicht erreicht. Im Gegenteil: Mit der weiteren Miniaturisierung und Vernetzung von intelligenten Systemen sind noch deutlich höhere Steigerungsraten zu erwarten. Entwicklungen wie „Internet der Dinge“ und „Industrie 4.0“ sind dabei nur Beispiele. In einer Phase, in der Unternehmen ihre Geschäftsmodelle weiterentwickeln oder sogar neu erfinden, sind Industrie und Wirtschaft ebenso wie die Konsumenten von der weiter voranschreitenden Digitalisierung betroffen. Für Deutschland ergeben sich dadurch ökonomische und gesellschaftliche Perspektiven. Allerdings ist zu beobachten, dass die fortschreitende Digitalisierung im Wesentlichen durch funktionale und ökonomische Faktoren bestimmt wird. Mit der gleichzeitig voranschreitenden Globalisierung nimmt dabei der wirtschaftliche Erfolgsdruck auf alle Akteure zu. IT-Sicherheit kommt in diesem Spannungsfeld oft zu kurz.

Anbieter, die bei Innovationen und Wettbewerbsfähigkeit zurückliegen, laufen dabei Gefahr, sehr schnell aus dem Markt zu fallen. Dies resultiert in einem Druck, schneller und funktional besser die Bedürfnisse einer weltweit steigenden Anzahl an Kunden zu bedienen als die Wettbewerber. Aspekte der IT-Sicherheit werden häufig weder von den Nutzern noch von den Anbietern gleichrangig mitbetrachtet. Es ist daher nicht verwunderlich, dass die Anforderungen hinsichtlich der Sicherheit von IT-Systemen, Applikationen und Software hinter ökonomischen Überlegungen zurücktreten. Solange Nutzer von Lieferanten, Dienstleistern und Herstellern neben der Funktionalität nicht auch gleichzeitig Sicherheit einfordern, wird es keine durchgreifenden Veränderungen zugunsten von IT-Sicherheit geben. IT-Sicherheit scheidet damit abseits von Spezialmärkten in den hochskalierenden Geschäftsfeldern, insbesondere dem Endkundenbereich, als geeignetes Differenzierungsmerkmal im Wettbewerb aus. Im Ergebnis wird nicht das notwendige Maß an Sicherheit produziert.

Dies hat schwerwiegende Folgen für die Sicherheit der eingesetzten IT, die durch die Anzahl von veröffentlichten Schwachstellen, Verwundbarkeiten und Angriffen sichtbar werden. Die IT-Risikolage bleibt damit angespannt. Die Regulierung der Kritischen Infrastrukturen durch das IT-Sicherheitsgesetz ist daher ein Schritt in die richtige Richtung. Es bleibt abzuwarten, wie sich die IT-Risikosituation in anderen Anwendungsbereichen außerhalb der Kritischen Infrastrukturen entwickelt. Auch hier kann, wenn sich durch Marktmechanismen kein angemessenes IT-Sicherheitsniveau einstellt, eine weitere IT-Sicherheitsgesetzgebung sinnvoll sein.

Im Folgenden werden einige technologische Veränderungen und ihre Bedeutung für die IT-Sicherheit dargestellt. Es wird dabei deutlich, wie schnell man sich als Hersteller und Anwender in dem oben dargestellten Spannungsfeld wiederfindet.

Software-defined Everything versus Separation

Der aktuelle Trend zum Software-defined Everything illustriert das Spannungsfeld zwischen Funktionalität und IT-Sicherheit. Der Begriff beschreibt die Entwicklung hin zu Architekturen, bei denen Systeme, Netze, Speicher und - je nach Auslegung - auch andere Elemente der Informationsverarbeitung nicht mehr statisch durch die eingesetzte Hardware definiert werden, sondern dynamisch konfiguriert werden können (beispielsweise Software-defined Network, Software-defined Data Center, Software-defined Storage). Die Vorteile liegen auf der Hand: Ressourcen können schneller und mit geringeren Kosten dorthin verlagert werden, wo sie gerade benötigt werden. Auch organisatorische Änderungen, etwa bei Fusionen oder Akquisitionen, lassen sich leichter abbilden. Software-defined Everything steht aber in Konkurrenz zur Grundforderung der Informationssicherheit nach Separation von wichtigen Prozessen und Systemen. Die Trennung unterschiedlicher Kundendaten, betrieblicher und technischer Prozesse sowie Systeme und Netze mit unterschiedlichen Sicherheitsniveaus ist eine etablierte und bewährte Strategie, um angemessene IT-Sicherheit zu erreichen. In einer dynamischen, softwarekonfigurierten Umgebung kann diese Trennung nicht in der gleichen technischen Tiefe erfolgen wie in klassischen Architekturen.
Hier gilt es, einerseits die notwendige Separation auch auf virtueller Ebene zu verankern und andererseits sichere Plattformen einzusetzen, damit die virtuelle Trennung nicht unterlaufen werden kann.

Mobile Computing versus Schutz geschäftskritischer Informationen

Der Trend zur Nutzung mobiler IT ist ungebrochen. Im Privatanwenderbereich drängen neben den etablierten Smartphones und Tablets bereits neue Geräteklassen auf den Markt, beispielsweise als Armbanduhren und Brillen („Wearable Computing"). Auch im geschäftlichen Einsatz gehören Smartphones und Tablets zur Standardausstattung. Damit wächst der Wunsch, geschäftskritische Informationen auf solchen Geräten bearbeiten zu können. Andererseits haben viele Institutionen angesichts der zunehmenden Gefahr durch gezielte Cyber-Spionage erkannt, dass sie bestimmte Informationen besonders schützen müssen. Dieses Vorgehen ist darin begründet, dass ein einheitliches hohes Sicherheitsniveau für die gesamte Institution meist nicht wirtschaftlich und nicht praktikabel ist. Stattdessen werden die geschäftskritischen Daten, die „Kronjuwelen", besonders geschützt, während in allen anderen Bereichen bewährte Standardsicherheitsmaßnahmen umgesetzt werden. Für viele Institutionen stellt sich daher die Frage, ob – und wenn ja, wie – von mobilen Geräten aus auf geschäftskritische Daten zugegriffen werden kann. Hier sind zum einen die verfügbaren modernen Sicherheitslösungen und zum anderen die individuellen Risiken zu berücksichtigen.

Betriebssicherheit versus Schutz vor Angriffen

In der industriellen Steuerungs- und Automatisierungstechnik ist Sicherheit eine wesentliche Grundforderung. Auch bei Fehlfunktionen und abweichenden Betriebszuständen darf von Maschinen und Anlagen keine inakzeptable Gefahr für Menschen und Umwelt ausgehen. Anforderungen an diese Betriebssicherheit, im Englischen „Safety" genannt, sind seit vielen Jahren in Normen und Standards festgelegt, die ständig aktualisiert und weiterentwickelt werden. Im Unterschied zur Betriebssicherheit wird mit dem Begriff „Security" der Schutz vor Angriffen, vor absichtlichen schädlichen Handlungen, bezeichnet.

Vor dem Hintergrund der zunehmenden Digitalisierung entstehen organisatorische und technische Wechselwirkungen zwischen Safety und Security. Einerseits gibt es viele Synergien, beispielsweise bei der klaren Strukturierung von Netzen und bei der Überwachung von Komponenten. Andererseits können Verschlüsselungs- und Filtermechanismen die Signallaufzeit und somit unter Umständen auch Safety-Eigenschaften der Anlage beeinflussen. Solche möglichen Wechselwirkungen müssen bei der Planung von Safety- und Security-Maßnahmen systematisch berücksichtigt werden.

Kompatibilität versus Informationssicherheit

Bei der Einführung moderner und sicherer Lösungen kann die berechtigte Forderung nach Kompatibilität mit bereits bestehenden Lösungen zum Hemmnis werden. Es dauert mitunter sehr lange, bis sich sicherheitstechnisch verbesserte Technologien durchsetzen und veraltete, unsichere Lösungen abgeschaltet werden können. Ein Beispiel hierfür ist das Protokoll TLS/SSL, das im Internet und in anderen Netzen zur Verschlüsselung des Datenverkehrs eingesetzt wird. Viele Server im Internet sind so konfiguriert, dass auch veraltete und unsichere kryptografische Verfahren zugelassen werden, damit auch Internetnutzer mit älteren Browsern auf das jeweilige Internetangebot zugreifen können. Ein weiteres Beispiel ist der Einsatz veralteter Betriebssysteme, die nicht mehr vom Hersteller mit Sicherheitsupdates versorgt werden. Im Bereich der industriellen Steuerungs- und Automatisierungstechnik können IT-Systeme oft nicht ohne Weiteres auf ein neueres Betriebssystem umgerüstet werden, etwa weil der Hersteller dies nicht unterstützt oder weil die Kompatibilität nicht gegeben ist.

2 Gefährdungslage

2 Gefährdungslage

Kapitel 2 beschreibt die aktuelle Gefährdungslage anhand von Rahmenbedingungen, Ursachen und Angriffsmethoden. Dabei wird auch grafisch eine Bewertung der einzelnen Gefährdungen im Berichtszeitraum vorgenommen.

(niedrig, durchschnittlich, hoch) 

2.1 Ursachen und Rahmenbedingungen

2.1.1 Cloud Computing

Einleitung

Cloud Computing ist ein sich verstetigender Trend, der die gesamte IKT-Branche umwälzt und dessen Auswirkungen einen großen Einfluss auf die IT-Sicherheit haben. Die fundamentale Veränderung in der IKT-Branche durch Cloud Computing ist, Cloud-Dienste zu mieten anstatt Softwareprodukte zu kaufen. Somit steigt die Abhängigkeit vom Cloud-Diensteanbieter, die bis zum Verlust der Prozess- und Datenhoheit reichen kann. Der Einsatz von Cloud-Lösungen erfordert ein größeres Vertrauen in die Anbieter am Markt. Denn es bedeutet einen großen Unterschied, ob Software klassisch von einem Anbieter beschafft und in der eigenen Institution betrieben wird oder ob dem Anbieter alle Daten mit übergeben werden und die Bereitstellung von Software nur noch als Dienstleistung vom Anbieter bezogen wird. Bei einem Eigenbetrieb der IT bestimmt der Betreiber selbst, welche Verfahren des IT-Sicherheitsmanagements zum Einsatz kommen. Bei Inanspruchnahme von Cloud-Lösungen liegt die Verantwortung für den IT-Betrieb beim Anbieter und mit ihm sind nur bestimmte Service Level Agreements (SLA) verhandelbar. Der sichere Einsatz von Cloud-Anwendungen stellt IT-Sicherheitsexperten somit weiter vor große Herausforderungen.

Lage

Cloud Computing und Cloud Security bringen zahlreiche Anforderungen für Einsatzszenarien hervor, die Verantwortliche vor immer neue Aufgaben stellen. In Bezug auf die IT-Sicherheit sind die folgenden Aspekte relevant:

- **Vertraulichkeit von Kundendaten:** Mehrstufige Vorkehrungen um Kundenbereiche voneinander zu trennen, sind Voraussetzung für sicheres Cloud Computing, aber mitunter mit hohen Kosten verbunden. Schlagen diese Maßnahmen fehl, sind in der Regel viele Kunden betroffen. Der finanzielle Schaden durch abgeflossene Kundendaten ist schwer zu beziffern. Entsprechend anspruchsvoll ist es, vorab vertraglich einen angemessenen Schadensersatz zu vereinbaren. Die Problematik scheint noch nicht flächendeckend in Cloud-Verträgen berücksichtigt zu sein.

- **Cloud-Dienstleister als Ziel von Angriffen:** Cloud-Dienstleister stellen in mehrfacher Hinsicht ein lukratives Ziel für Angreifer dar. Einerseits können mit einem erfolgreichen Angriff auf einen Dienstleister zugleich Daten mehrerer Kunden abgegriffen werden. Andererseits ist eine Cloud-Infrastruktur selbst für Angreifer interessant, da sie große Ressourcen (Rechenleistung, Speicherplatz) vorfinden, um etwa Passwörter zu knacken oder DoS-Angriffe auf Dritte auszuführen. Dieser Trend wird sich mit zunehmender Cloud-Nutzung weiter verstärken. Cloud-Dienstleister müssen künftig noch mehr Aufwand betreiben, um ihre eigenen Systeme – und damit die Daten und Betriebsfähigkeit ihrer Kunden – zu schützen.

- **Behandlung von Sicherheitsvorfällen:** Cloud-Dienstleister arbeiten häufig mit Unterauftragnehmern oder kompletten Supply Chains. Kommt es zu einem Vorfall, müssen über mehrere Dienstleister hinweg zeitnah Maßnahmen ergriffen sowie alle Kunden in die Vorfallsbewältigung integriert werden. Bislang ließ sich das Spannungsfeld zwischen dem Anliegen des Cloud-Anbieters, seine Kunden nicht übermäßig zu beunruhigen, und dem Anliegen des Kunden, rasch und präzise über Vorfälle informiert zu werden, nicht auflösen. Aus Sicht der IT-Sicherheit müssen die Cloud-Dienstleister dafür Prozesse definieren und umsetzen.

- **Vorteile für die IT-Sicherheit durch Cloud Computing:** Den aktuellen Herausforderungen stehen deutliche Vorteile der Cloud-Technik gegenüber. Ein Cloud-Anbieter kann – sofern er viele Kunden hat – Sicherheitsmaßnahmen kostengünstiger für alle Kunden umsetzen, als dies ein Unternehmen für sich könnte. Dies gilt für klassische Maßnahmen der Informationssicherheit, wie zum Beispiel Backup und georedundante Spiegelung von Daten, aber auch im Bereich der Cyber-Sicherheit, da ein Cloud-Dienstleister meist mehr Ressourcen einsetzen kann, um sich gegen DDoS-Attacken zu schützen. Davon können besonders kleine und mittelständische Unternehmen profitieren.

Bewertung

Derzeit scheint das Bewusstsein der Verantwortlichen für die Chancen und Risiken durch Cloud Computing im Bereich der Informationssicherheit noch recht gering zu sein. Bedingt durch die geringe Nachfrage der Kunden nach IT-Sicherheitsmaßnahmen von Cloud-Lösungen investieren die Anbieter bislang in diesem Bereich zu wenig. Es ist erforderlich, dass auch Kunden durch Nachfrage hoher IT-Sicherheitsniveaus dazu beitragen, dass Sicherheit ein wichtiges Differenzierungsmerkmal auf dem Markt der Cloud-Angebote wird.

Gefährdung 2015

2.1.2 Software-Schwachstellen

Einleitung

Software beinhaltet Schwachstellen, die Voraussetzung und Wegbereiter für erfolgreiche Cyber-Angriffe sind. Angesichts der zunehmenden Größe, gemessen in Anzahl Codezeilen, und Komplexität heutiger Software ist es unvermeidlich, dass bei der Entwicklung Fehler unterlaufen. Die Ausnutzung von Architektur-, Implementierungs- und Konfigurationsfehlern ermöglicht es, den Systemzustand gegen den Willen des Nutzers zu verändern. Beispiele sind die automatische Ausführung von regulär eingebettetem schädlichem Code beim Öffnen eines Dokuments (Architekturfehler), die Möglichkeit der Umgehung einer Passwortabfrage (Implementierungsfehler) oder die Nutzung öffentlich bekannter Standardpasswörter (Konfigurationsfehler).

Lage

- Die Anzahl kritischer Schwachstellen in Standard-IT-Produkten hat sich gegenüber den bereits hohen Werten in den Vorjahren im Jahr 2015 noch einmal massiv erhöht (Abb. 1). Allein für die 11 verbreitetsten in der BSI-Schwachstellenampel erfassten Softwareprodukte (Abb. 2) wurden im Jahr 2015 bis Ende September 847 kritische Schwachstellen bekannt.

- Aus Sicht der Angreifer sind Webbrowser und die darin enthaltenen Plug-ins die exponierteste Software. Schwachstellen in diesen Anwendungen werden deshalb bevorzugt für Angriffe verwendet. Bei den in der Schwachstellenampel aufgeführten Microsoft-Produkten betrafen mehr als 45 Prozent der Schwachstellen bis Juli 2015 den Webbrowser. Die mit Abstand höchste Anzahl kritischer Schwachstellen hatte das Browser-Plug-in Adobe Flash Player.

- Entwicklungsmethoden, die Sicherheitsaspekte durchgängig im gesamten Lebenszyklus einer

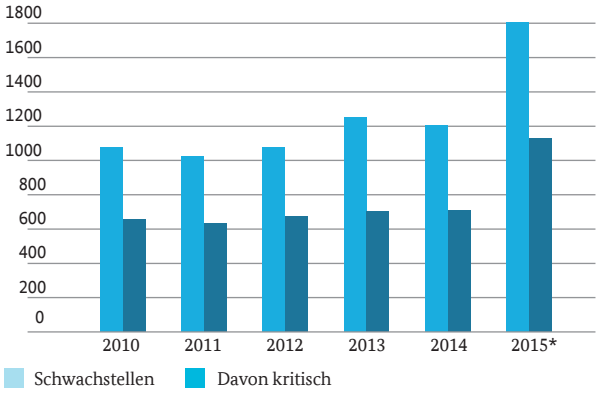

Abbildung 1: Anzahl aller Schwachstellen der in der BSI-Schwachstellenampel erfassten Softwareprodukte. * Zahlen für 2015 sind aus den bis Ende September 2015 entdeckten Schwachstellen hochgerechnet

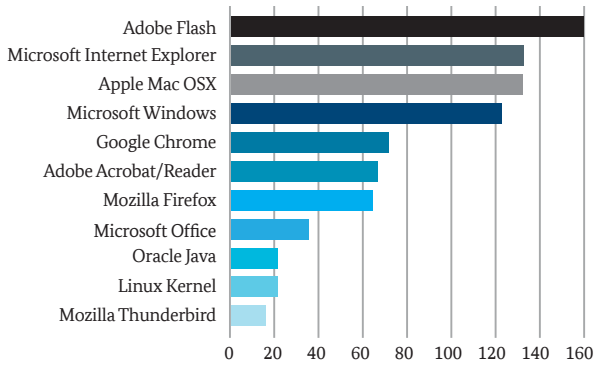

Abbildung 2: Kritische Schwachstellen der in der BSI-Schwachstellenampel erfassten Softwareprodukte bis September 2015

Software berücksichtigen, liefern einen wichtigen Beitrag zur Reduzierung der Anzahl Schwachstellen und damit zur Verbesserung der Sicherheit von Software (zum Beispiel Quellcodeanalysetools oder Tests mittels Fuzzing).

- Große Bedeutung haben auch Techniken zur Eindämmung der Ausnutzbarkeit bzw. der Auswirkungen von Schwachstellen wie ASLR (Address Space Layout Randomization) und NX/DEP (No eXecute / Data Execution Prevention). In aktueller Software werden ASLR und NX/DEP flächendeckend eingesetzt, sofern die Mechanismen von der Hardware unterstützt werden. Auch Sandbox-Mechanismen, also der Isolation von einzelnen Programmbestandteilen, kommt bei der Abwehr von Infektionen eine herausgehobene Bedeutung zu. Browser mit Sandbox-Technologie isolieren die Inhalte einer Webseite vom Rest des Browsers und vom Betriebssystem und reduzieren damit die Auswirkungen eines Angriffs beim Besuch einer infizierten Webseite.

- Der Patch-Politik kommt ebenfalls eine große Bedeutung zu. Hersteller sind in der Verantwortung, eine wirkungsvolle Patch-Politik mit kurzen Reaktionszeiten umzusetzen. Einige Hersteller sind jedoch – meist aus Ressourcengründen – dazu übergegangen, für weniger kritische Schwachstellen kaum noch Patches zur Verfügung zu stellen. Im Ergebnis kann dies dazu führen, dass Schwachstellen erst mit

Erpressungsversuch nach Kompromittierung des Webservers

Sachverhalt: Ein Unternehmen erhielt ein Erpresserschreiben per E-Mail, in dem die Zahlung von zwei Bitcoins mit einer Frist von 24 Stunden gefordert wurde. Falls das Unternehmen nicht auf die Forderung einginge, drohe die Veröffentlichung der zuvor über die Kompromittierung der Webseite des Unternehmens ausgespähten Kundendaten. Als Beleg für die Kompromittierung wurden dem Erpresseranschreiben die Datenbankstruktur der Webanwendung sowie Screenshots beigefügt.

Ursache/Auslöser: Die Kompromittierung der Webseite des Unternehmens war durch die Ausnutzung einer bekannten Schwachstelle in dem eingesetzten Content-Management-System (CMS) möglich. Nach Eingang des Erpresseranschreibens wurde ein bereits verfügbares Sicherheitsupdate für das CMS installiert.

Methode: Um eine große Anzahl von Webanwendungen zu kompromittieren, suchen die Angreifer nach bereits bekannten Schwachstellen in weit verbreiteten Webanwendungen. Diese erfolgt mithilfe von spezifischen Suchmaschinenparametern (z. B. bekannte Pfade bzw. Dateien der Webanwendung) und präparierten Angriffsskripten zur Ausnutzung der Schwachstellen weitgehend automatisiert.
Die Verwendung von Krypto-Währungen wie etwa Bitcoin für die Lösegeldforderungen wurde neben dem aufgezeigten Fall im Jahre 2015 auch verstärkt bei DDoS-Erpressungen und Krypto-Ransomware beobachtet.

Schadenswirkung: Dem Unternehmen entstand durch den Cyber-Angriff zunächst ein Reputationsverlust durch die Offenlegung der vertraulichen Kundendaten. Des Weiteren erzeugte die sichere Wiederherstellung der Webseite personelle und finanzielle Aufwände. Die Verwendung der ausgespähten Informationen für weitere Cyber-Angriffe - etwa gegen die Kunden des Unternehmens - ist denkbar, sie wurde allerdings im konkreten Fall nicht beobachtet. Kompromittierungen von Webseiten können generell verschiedene Schäden auslösen. Neben dem dargestellten Ausspähen von sensiblen Informationen und deren Verwendung für ein Erpressungsszenario können die Angreifer auch Schadprogramme über die Webseite verteilen oder den Webserver u. a. für DoS-Angriffe oder den Spam-Versand missbrauchen.

Zielgruppen: Im Jahre 2015 berichteten dem BSI vorrangig kleine und mittelständische Unternehmen über kompromittierte Webseiten und ähnlich gelagerte Erpressungsszenarien.

Technische Fähigkeiten: Die Ausnutzung von bekannten Schwachstellen in weit verbreiteten Webanwendungen kann durch Angreifer erfolgen, die keine tiefgehenden IT-Sicherheitskenntnisse aufweisen. Selbst unbekannte Schwachstellen in Webanwendungen können mithilfe von Schwachstellen-Scannern entdeckt und anschließend ausgenutzt werden.

wochen- oder monatelanger Verzögerung behoben werden oder eine Behebung sogar unterbleibt.

- Grundsätzlich ist eine unverzügliche Einspielung von Sicherheitsupdates direkt nach Verfügbarkeit zwingend, um das Zeitfenster, in dem die Systeme verwundbar sind, so klein wie möglich zu halten. Werden Detailinformationen oder gar Exploits für eine bestimmte Schwachstelle vor der Bereitstellung eines Sicherheitsupdates öffentlich, ist vom Einsatz der betroffenen Software nach Möglichkeit abzusehen bzw. sollte er nur mit höchster Vorsicht stattfinden. 2015 gab es bis Ende September allein neun öffentlich bekannte Vorfälle, in denen Zero-Day-Exploits verwendet wurden. Auch aus der Cyber-Sicherheitsumfrage 2015[1] geht hervor, dass erfolgreiche Angriffe häufig auf Angriffe über unbekannte Schwachstellen und auf fehlendes Patch-Management zurückzuführen sind.

Bewertung

Die Bedrohungslage durch Schwachstellen ist unverändert hoch. Es zeichnet sich jedoch in der Softwareindustrie stellenweise ein Umdenken ab, welches durch verbesserte Softwareentwicklung, verstärkte Eindämmung von Schwachstellen und kürzere Reaktionszeiten langfristig zu einer Erhöhung der IT-Sicherheit führen könnte. Die Hersteller müssen ihrer besonderen Verantwortung über den gesamten Lebenszyklus eines Produktes gerecht werden, der die regelmäßige und kurzfristige Behebung von Schwachstellen genauso umfasst wie die Verwendung verfügbarer Schutzmaßnahmen sowie aktueller Softwareentwicklungsprozesse. Um die Sicherheit beschaffter Hard- und Software in diesem Kontext zu erhöhen, könnten Großkunden im Zuge der Verhandlung von Lieferverträgen gegenüber den Herstellern verbindliche Fristen einfordern, innerhalb derer ein Hersteller nach öffentlichem Bekanntwerden einer Schwachstelle diese für Produkte im Rahmenvertrag beheben muss. Das BSI hat bereits damit begonnen, dies in einigen Rahmenverträgen zur IT-Beschaffung des Bundes umzusetzen.

Das BSI sieht in der engen Zusammenarbeit zwischen dem Entdecker einer Schwachstelle und dem Hersteller der betroffenen Software den richtigen Weg, um Schwachstellen zu beheben. Dieses als Coordinated oder Responsible Disclosure bezeichnete Vorgehen ermöglicht es dem Hersteller, Sicherheitsupdates zur Verfügung zu stellen, ohne dass Details zur Ausnutzung einer Schwachstelle vorab bekannt und für Angriffe ausgenutzt werden

[1] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Micro/Umfrage/umfrage2015.html

können. Trotzdem kommt es nicht selten vor, dass Entdecker Informationen über eine Schwachstelle öffentlich machen, auch wenn der Hersteller die Schwachstelle noch nicht geschlossen hat. Der Grund hierfür ist häufig, dass die Hersteller aus Sicht der Entdecker entweder zu viel Zeit zum Schließen einer Schwachstelle benötigen oder die Schwachstelle nicht schließen wollen. Informationen für Hersteller zur Handhabung von Schwachstellen hat das BSI veröffentlicht[2].

Gefährdung 2015

IT-Sicherheitszertifizierung: Vertrauen und Sicherheitsgestaltung

Da Deutschland und Europa in der globalen Informations- und Kommunikationstechnologie Nachfrage- und nur in Teilsegmenten signifikante Anbietermärkte für Software- und Hardwareprodukte sind, spielt die IT-Sicherheitszertifizierung eine wichtige Rolle: 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. Insbesondere der „High Assurance"-Ansatz liegt nicht immer im Interesse von Herstellern und Vertreibern, die an die im IT-Bereich vorherrschenden kurzlebigen Produktzyklen gebunden sind und sich (zeit-)aufwendige Zertifizierungsverfahren ersparen wollen. Wegen der Globalität des Marktes sind nur IT-Sicherheitsstandards und IT-Sicherheitszertifizierungen nach internationalen Standards („Common Criteria") geeignet, um die Sicherheit und damit das Vertrauen in Hard- und Softwareprodukte zu gewährleisten. Nur auf Basis internationaler Standards sind die Global Player in der IKT-Branche bereit, in Prüfaufwände und Zertifizierung zu investieren.

Durch Schwachstellen in IT-Produkten stellt sich die Herausforderung, Produkte sicherer zu entwickeln sowie durch unabhängige Prüfinstitutionen Evaluierungen mit Schwachstellenanalysen durchzuführen. Im Rahmen der Common-Criteria-Zertifizierung sind in Deutschland neun Evaluierungsstellen vom BSI anerkannt.

Eine wichtige Grundlage für die Zertifizierung bilden Technische Richtlinien und Schutzprofile (Protection Profiles), mit denen für bestimmte Produktgruppen oder Techniksysteme Sicherheitsvorgaben getroffen werden, deren Einhaltung durch die Zertifizierung gewährleistet wird. In den letzten Jahren wurde eine große Anzahl von Schutzprofilen – teilweise auch durch das BSI - erstellt. Diese Schutzprofile schaffen in den verschiedenen Produktklassen eine Vergleichbarkeit für den Anwender. Insbesondere machen die unterschiedlichen Prüftiefen transparent, ob und wie das Produkt im Rahmen der Evaluierung auf Schwachstellen hin analysiert worden ist.

Im Rahmen der 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 zum Beispiel

- 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-SchwachstellenInformationen durch Prüflabore und Hersteller, etwa bei der Simulation von Seitenkanalangriffen

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

Schutzprofile und „High Assurance"-Zertifikate sind wichtige sicherheitstechnische Eckpfeiler für Großprojekte der Bundesregierung im Rahmen von gesetzlichen Initiativen, die jede Bürgerin und jeden Bürger erreichen, sei es in Form des neuen Personalausweises, des elektronischen Reisepasses, der elektronischen Gesundheitskarte oder in Zukunft der intelligenten Messsysteme wie etwa Stromzähler. Nur über die Zertifizierung lässt sich gewährleisten, dass das vom Gesetzgeber vorgegebene Sicherheitsniveau sich tatsächlich in den eingesetzten Produkten wiederfindet. Das BSI vertritt hierbei den Ansatz, dass eine hohe Prüftiefe für die Beurteilung der Sicherheit moderner und in der Regel komplexer IT unverzichtbar ist. Besonders wenn IT-Systeme an wichtigen Schaltstellen kritischer Infrastrukturen eingesetzt werden, geht angesichts der damit verbundenen Risiken an einer umfassenden, in die Tiefe gehenden Sicherheitszertifizierung kein Weg vorbei.

Gegenwärtig ist insbesondere im internationalen, eher außereuropäischen Umfeld eine Tendenz zu verzeichnen, dass diese Position nicht von allen Staaten so vertreten wird. Es gibt viele Stimmen, die eine schnelle, leichte Prüfung und Zertifizierung fordern. Auch bei den sich gegenwärtig in Verhandlung befindlichen internationalen Handelsabkommen (TTIP, TiSA u.a.) besteht die grundsätzliche Gefahr, dass IT-Sicherheitsbelange nicht adäquat berücksichtigt werden. Hier ist es wichtig, dass die in Deutschland und Europa etablierten hohen Standards nicht gefährdet werden.

[2] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/programmierung/BSI-CS_019.pdf

2.1.3 Hardware-Schwachstellen

Einleitung

Die Bedrohung durch Hardware-Schwachstellen in elektronischen Geräten ist in der Fachwelt schon lange Gegenstand vieler IT-Sicherheitsbetrachtungen. Hardware-Manipulationen können auf verschiedenen Ebenen stattfinden. Im Wesentlichen kann man folgende Angriffsvektoren unterscheiden:

- Modifikationen durch zusätzliche Baugruppen
- Änderungen bestehender Schaltungen
- Manipulationen auf Chipebene
- Softwaremodifikationen auf Firmware-Ebene

Mit Ausnahme von Firmware-Manipulationen aus dem Betriebssystem heraus ist für diese Art von Angriffen der physikalische Zugriff auf das Gerät notwendig. Angesichts in der Industrie üblicher verteilter Produktionsstätten und globaler Lieferketten gehen die Bauteile durch viele Hände, wodurch sich die Möglichkeit einer Manipulation signifikant erhöht.

Lage

- Hardware-Manipulationen sind über die Integration von Bauteilen in Geräte oder durch die Schwächung bestehender elektronischer Schaltkreise (Verdünnen von Drähten oder Bestrahlung von Bauteilen) möglich. Beispielsweise kann durch den Einbau zusätzlicher Baugruppen erreicht werden, dass eine Tastatur neben ihrer eigentlichen Funktionalität Daten über Funkfrequenzen versendet. Beliebige USB-Geräte können in ähnlicher Weise manipuliert werden und somit erwünschte Nebeneffekte mit sich bringen. Die Detektion zusätzlicher Bauteile ist grundsätzlich möglich, oft jedoch mit sehr hohem Aufwand verbunden.

- Praktisch nicht zu detektieren sind Eingriffe, die auf Chipebene vorgenommen werden. Ziel dieser Angriffe ist zum Beispiel der Zufallsgenerator im Prozessor, der für kryptografische Verfahren elementar ist. Durch Dotierungsänderungen des Halbleitermaterials kann dieser Zufallsgenerator so geschwächt werden, dass die Zufallszahlen vorhersehbar werden. Die Auswirkungen auf kryptografischen Verfahren sind schwerwiegend: Eine Verschlüsselung kann ausgehebelt bzw. um ein Vielfaches leichter gebrochen werden[3]. Eine derartige Manipulation ist kaum zu entdecken, da sich an der internen Struktur und den Bauteilen des Chips nichts ändert. Auch eine Funktionsprüfung würde die Vorhersehbarkeit der Zufallszahlen nicht offenlegen.

- Moderne Hardware ist oft untrennbar mit Softwarebestandteilen verbunden. Veröffentlichungen zur NSA-Affäre beziehen sich auf Hintertüren, die dauerhaft ins BIOS oder in Firmware implantiert werden[4]. Da sich diese Programme außerhalb der Kontrolle des Betriebssystems befinden, werden sie oft den Hardware-Trojanern zugeordnet. Die Gefährdung durch solche Implantate beruht darauf, dass sie im System Management Mode (SMM) von x86-Prozessoren oder in der noch darunter liegenden Management-Engine (Intel ME, Apple SMC) laufen und somit vollen Zugriff auf den Hauptspeicher und/oder weitere wichtige Komponenten des Systems haben. Ein Angreifer kann den Rechner auf diesem Wege komplett übernehmen oder zumindest schädigen. Auch hier ist es mit sehr hohem Aufwand verbunden, ein solches Schadprogramm zu finden.

- Viele Angriffstechniken auf Hardware sind in grundsätzlicher Form allgemein verfügbar geworden und können kostengünstig umgesetzt werden. Dies umfasst Seitenkanalanalysen und die absichtliche Erzeugung von Fehlern oder Fehlzuständen (Glitches). Ohne Verletzung der Geräte oder Zugriff auf Debug-Schnittstellen können so interne Informationen, wie etwa Schlüssel zum Schutz der Kommunikation, erlangt werden.

Bewertung

Die besondere Bedrohung durch Hardware-Angriffe besteht darin, dass sie nur mit großem Aufwand entdeckt werden können. Gleiches gilt für Hardware-Trojaner, die die meiste Zeit passiv sind und nur nach Aktivierung ihre Schadfunktionen ausführen. Bestehende Testverfahren sind nicht ausreichend oder zu aufwendig, wobei die kurzen Produktinnovationszyklen in der Informationstechnik Analysen zusätzlich erschweren oder obsolet machen. Wirksamen Schutz gegen Manipulationen kann man allein dadurch erreichen, dass Komponenten in vertrauenswürdiger Umgebung produziert und mittels einer sicheren Lieferkette distribuiert werden.

Gefährdung 2015

[3] http://people.umass.edu/gbecker/BeckerChes13.pdf
[4] http://mjg59.dreamwidth.org/35110.html

Verwundbarkeit von Intel-Management-Systemen

Sachverhalt
Intel bietet für PCs mit der bereits im Chipsatz des Mainboards implementierten Management-Lösung AMT (auch als vPro beworben) eine Fernwartungsfunktion, mit deren Hilfe Rechner selbst aus dem ausgeschalteten Zustand heraus aktiviert und vollständig konfiguriert werden können. AMT ist Teil der Intel Management Engine. Im Auslieferungszustand ist das System typischerweise unkonfiguriert und mit einem Standardpasswort versehen. Wird diese Funktion nicht verwendet, bleibt dieser unkonfigurierte Zustand meist bestehen.

Im Juli 2015 wurde eine Verwundbarkeit bei einigen Gerätetypen verschiedener Hersteller bekannt: Angreifer haben die Möglichkeit, mit einem speziell präparierten USB-Stick einen unkonfigurierten Rechner unabhängig von eventuell eingerichteten Sicherheitsmaßnahmen durch Nutzung des herstellerspezifischen Standard-AMT-Passworts umzukonfigurieren. Von der Schwachstelle sind in der Regel nur Businesssysteme verschiedener Hersteller betroffen.

Bewertung
Hat ein Angreifer nur wenige Sekunden lang physikalischen Zugriff auf ein verwundbares System und schließt einen präparierten USB-Stick an, kann er den Rechner anschließend vollständig fernsteuern, Daten lesen und modifizieren. Schutzmechanismen auf Betriebssystemebene können den Angriff nicht verhindern, sondern nur unter spezifischen Randbedingungen detektieren. Besonders gefährdet sind mobile Systeme, da diese in der Regel nicht ständig unter der Kontrolle des Besitzers sind.

Maßnahmen
Das AMT-Subsystem sollte, unabhängig von der späteren Verwendung von AMT, vor Beginn der Nutzung mit einem neuen, gerätespezifischen sicheren AMT-Passwort versehen werden. Danach kann das AMT-Subsystem in den BIOS-Settings deaktiviert werden. Das Deaktivieren von AMT in den BIOS-Settings allein genügt nicht.

2.1.4 Nutzerverhalten und Herstellerverantwortung

Einleitung

Mit der zunehmenden Verbreitung von Informationstechnik rückt auch der Mensch immer mehr in den Mittelpunkt von IT-Sicherheitsfragen. Einerseits ist er für die IT- und Informationssicherheit verantwortlich, andererseits ist er häufig das schwächste Glied in der Verteidigungskette. Neben technischen und organisatorischen Maßnahmen sind Sensibilisierung, Awareness sowie ein gesundes Maß an Misstrauen aufseiten der Anwender für die IT-Sicherheit unerlässlich.

Lage

- Die Digitalisierung prägt viele Bereiche des Alltags. Derzeit erfreuen sich beispielsweise sogenannte Fitness-Tracker, die diverse Körperfunktionen und Trainingseinheiten messen können, steigender Beliebtheit[5]. Die digitalen Helfer übertragen auch sensible Gesundheitsdaten an zentrale Dienstleister zur Speicherung oder Auswertung. Es ist davon auszugehen, dass die Verwundbarkeit der Technik oder die Datennutzung durch die Betreiber kaum hinterfragt werden. Bestehende und neue Angebote im Social Web vermitteln scheinbar kostenlose oder preiswerte soziale Vernetzung und Zugehörigkeit und führen zu weiter steigenden Mitgliederzahlen[6].

- Persönliche Daten oder digitale Identitäten sind gefährdet, wenn fehlendes Technikverständnis auf unzureichende Transparenz der Angebote trifft. Desinteresse und Überforderung verleiten den Nutzer zum sorglosen Handeln in der digitalen Welt.

- Awareness-Kampagnen und die zunehmende Zahl an Medienberichten tragen zu einer höheren Aufmerksamkeit für die Risiken beim Einsatz von IT und der Nutzung des Internets bei. Viele Anwender entscheiden sich jedoch aufgrund von Komfort und einfacher Bedienbarkeit für bestimmte Geräte, Dienste und Anwendungen, während IT-Sicherheitsaspekte häufig keine Rolle bei der Auswahl spielen.

- Laut einer IBM-Studie hängen über die Hälfte aller erfolgreichen Cyber-Angriffe mit dem Nutzer zusammen. Unabhängig von Cyber-Angriffen durch externe Angreifer können (ehemalige) Mitarbeiter oder Dienstleister wissentlich oder durch unbedarftes Handeln gravierende Sicherheitsprobleme auslösen[7, 8]. Beispiele sind vermeidbare Anwenderfehler, die Nutzung von Social-Web-Angeboten sowie die zunehmende Anbindung – auch privater – Mobilgeräte an das Unternehmensnetz. Unbefugte Zugriffe führen in der Studie die Rangliste der Sicherheitsvorfälle an, in den Vorjahren lagen detektierte Angriffe durch schadhaften Code und Ausspionieren von Systemen durch externe Angreifer vorn.

[5] http://www.connect.de/news/smartwatch-fitness-armbaender-wearables-apple-watch-verkaufszahlen-2897622.html
[6] WhatsApp mit 800 Millionen aktiven Nutzern: http://www.heise.de/newsticker/meldung/WhatsApp-mit-800-Millionen-aktiven-Nutzern-2612236.html
[7] http://www.heise.de/ix/meldung/IBM-Sicherheitsstudien-Cyberattacken-aus-den-eigenen-Reihen-am-haeufigsten-2715977.html
[8] 2015 Cyber Security Intelligence Index; http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03073USEN&attachment=SEW03073USEN.PDF

Bewertung

Der Weg von digitaler Sorglosigkeit zum digitalen verantwortungsbewussten Handeln ist keine isolierte Leistung eines einzelnen Anwenders. Die Verantwortung für die digitale Sicherheit tragen alle Beteiligten: Nutzer, Management in Unternehmen und Behörden, Hersteller, Provider und Diensteanbieter. Für ein hohes Sicherheitsniveau der IT in Unternehmen trägt das Management entscheidende Verantwortung. IT-Sicherheitskonzepte müssen auf Geschäftsführer- oder Vorstandsebene adressiert, entschieden und in die Organisation kommuniziert werden. Damit lässt sich die erforderliche Grundlage schaffen, auf der die Anwender verantwortungsbewusst handeln können.

Hersteller sollten IT-Sicherheitskonzepte frühzeitig in die Produktentwicklung integrieren und eine intuitive Nutzbarkeit sowie Beherrschbarkeit von Software und Prozessen auch für technisch weniger versierte Anwender berücksichtigen (Sicherheitsergonomie). Hersteller sollten zudem bei der Produktentwicklung dem Security-by-design-Ansatz folgen. Hersteller können in der Entwicklung von sicheren IT-Produkten eine solide Grundlage schaffen, auf die Administratoren und Mitarbeiter im Unternehmen aufbauen können.

Aufgrund ihrer zentralen und vorgelagerten Stellung können Provider einen wichtigen Beitrag zu mehr IT-Sicherheit leisten, indem sie sich im Hinblick auf IT-Sicherheitsaspekte technisch und personell so aufstellen, dass sie frühzeitig Anomalien oder Sicherheitsvorfälle detektieren und analysieren können und ihre Kunden bei IT-Sicherheitsvorfällen frühzeitig und effizient informieren und unterstützen. Zur konkreten Hilfe gehören Warndienste ebenso wie die Bereitstellung von Abwehrtools.

Eine wichtige Rolle spielt jedoch trotz aller Hersteller- und Providerverantwortung auch der Nutzer. Nachfrage erzeugt Angebot, auch in Bezug auf IT-Sicherheit. Es bleibt abzuwarten, ob Nutzer künftig – zum Beispiel nach Inkrafttreten der neuen EU-Datenschutzregelung – vermehrt Informationen und Transparenz bei den Anbietern einfordern, ihr „Recht auf Vergessen“ in Anspruch nehmen und damit eine Digitale Verantwortung an die Stelle der Digitalen Sorglosigkeit treten kann.

Gefährdung 2015

2.1.5 Kryptografie

Einleitung

Mathematische Kryptografie ist der zentrale und stärkste Grundbaustein für IT-Sicherheitsmechanismen zur Wahrung von Vertraulichkeit, Integrität und Authentizität digitaler Informationen. Sie dient zudem der Authentisierung und dem Integritätsschutz von Software sowie zur Absicherung von physikalischen Systemen wie etwa Schließsystemen. Kryptografie ist zudem ein wichtiges und dynamisches Forschungsfeld, das häufig neue Herausforderungen an die Experten stellt, die sich beispielsweise aus neuen Anwendungsfällen wie dem Cloud Computing ergeben. Die Zahl möglicher Einsatzzwecke von kryptografischen Verfahren ist sehr hoch und das Potenzial der Kryptografie noch lange nicht ausgeschöpft.

Lage

- In den letzten Jahren bzw. Jahrzehnten sind zahlreiche kryptografische Verfahren entwickelt worden: Block- und Stromchiffren zur Verschlüsselung, Verfahren zum Austausch von Schlüsseln oder zur Erstellung von digitalen Signaturen sowie Hashfunktionen und Zufallszahlengeneratoren.
- Diese Verfahren werden als Grundbausteine in kryptografischen Protokollen wie dem Transport Layer Security (TLS)-Protokoll verwendet, die beispielsweise der Absicherung mobiler Kommunikation sowie von Transaktionen beim Online-Shopping dienen.
- Gängige Krypto-Algorithmen können – bis auf RC4 – nach heutigem Stand als sicher angesehen werden. Voraussetzung dafür ist eine hinreichende Wahl der Parameter- und Schlüssellängen (vgl. BSI Technische Richtlinie TR-02102).
- In der Forschung ist die Entwicklung von quantencomputerresistenten Verfahren ein wichtiges Thema. Viele gängige Verfahren sind bei Existenz eines hinreichend leistungsfähigen Quantencomputers nicht mehr sicher. Diese Entwicklung ist besonders für die Übermittlung von Informationen mit hohem und langfristigem Schutzbedarf bedeutsam.
- Sicherheitsprobleme ergeben sich durch die mitunter fehlerhafte Verwendung von kryptografischen Verfahren in kryptografischen Protokollen bzw. Fehler in Implementierungen von kryptografischen Protokollen.
- Seitenkanalangriffe erlauben es, Implementierungen von an sich sicheren Algorithmen anzugreifen. Diese nutzen beispielsweise Zeitverhalten oder Stromverbrauch von Geräten aus, um an Informationen über geheime Schlüssel zu gelangen.

Aktuelle Angriffe auf kryptografische Verfahren

Seit Dezember 2014 gab es zwei neue schwerwiegende Angriffe auf das TLS-Protokoll: die FREAK-Attacke und die Logjam-Attacke. Beide Angriffe nutzen die Existenz von schwachen TLS-Parametern (sogenannte Export-Verfahren) aus. Während die FREAK-Attacke auf einem Implementierungsfehler in OpenSSL beruht, ermöglicht bei Logjam eine Schwäche im Protokoll, dass ein Angreifer als „Man-in-the-middle" zwischen den beiden Kommunikationspartnern fungieren kann. Die Logjam-Attacke richtet sich gegen ein Verfahren zum Schlüsselaustausch, dem das Diskreter-Logarithmus-Problem (DLP) zugrunde liegt. Forscher des französischen INRIA haben sich für den Logjam-Angriff[9] zunutze gemacht, dass sich bei schwachen Export-Verfahren das DLP mithilfe von Vorberechnungen relativ leicht lösen lässt. Sie konnten dadurch die beim TLS-Verbindungsaufbau ausgetauschten geheimen Schlüssel nahezu in Echtzeit berechnen. Die Ergebnisse sind auch auf andere Einsatzbereiche dieses Schlüsselaustauschverfahrens übertragbar. Mit einem höheren Aufwand für die Vorberechnungen lassen sich zudem potenziell auch DLP-Fälle lösen, die eher dem Stand der Technik entsprechen. Die französischen Forscher geben beispielsweise Argumente dafür, dass die NSA in der Lage sei, das DLP auf ausgewählten Gruppen zu 1.024 Bit Primzahlen schnell zu lösen.

Schwächen in RC4

Die Stromchiffre RC4 ist trotz bekannter Schwächen noch weit verbreitet. In den letzten Monaten sind noch einmal verbesserte Angriffe auf RC4 veröffentlicht worden, die besonders auf die Verwendung von RC4 in TLS abzielen. Diese Angriffe sind bislang nur theoretisch möglich, dennoch hat die für Internet-Standards verantwortliche Internet Engineering Task Force die Nutzung von RC4 für TLS inzwischen zurückgezogen[10].

Bewertung

Kryptografie ist ein sehr aktives und wichtiges Forschungsfeld. Das BSI bewertet kryptografische Algorithmen bzw. Standards, untersucht Implementierungen dieser Algorithmen und wertet Messungen zur Seitenkanalresistenz von Implementierungen aus. Aufgrund des hohen Potenzials kryptografischer Lösungen ist davon auszugehen, dass sie weiterhin in zahlreiche alltagsnahe Anwendungen Eingang finden und dort zum Schutz von Daten beitragen werden.

Gefährdung 2015

2.1.6 Internet-Protokolle

Einleitung

Ein Grundgedanke des Internets ist seine Offenheit, die es allen Nutzern ermöglicht, das Internet zur Information und zum Austausch von Daten zu nutzen. Gleichzeitig hat das Internet eine sehr komplexe Struktur. Selbst bei einfachen Aktionen wie dem Abrufen einer Webseite sind zahlreiche Komponenten und Protokolle involviert. Offenheit und Anonymität sind für viele Nutzer wünschenswerte Attribute des Internets. Zusammen mit der technischen Komplexität sind sie aber auch Ursache dafür, dass das Internet als Angriffsplattform missbraucht wird.

Lage

- Beim Design des Internets ging man von kooperativen Nutzern in einer vertraulichen Umgebung aus. Dementsprechend war Sicherheit kein Kriterium bei der Entwicklung der Protokolle. Die Protokolle aus den Anfängen, wie IP, UDP, TCP, DNS, SMTP, HTTP, SSL und BGP, werden jedoch bis heute verwendet.
- Da das Internet elementarer Bestandteil der heutigen Kommunikation ist, wiegen Schwachstellen in den Protokollen oder in den verwendeten Referenzimplementierungen besonders schwer. Milliarden von Geräten unterstützen diese und sind somit prinzipiell angreifbar.
- Protokollerweiterungen, die bisher fehlende Schutzmechanismen ergänzen, setzen sich oft nur langsam durch.
- So steht für den Verzeichnisdienst DNS nach einer gemeinsamen Testbed-Initiative durch BSI, DENIC und den eco-Verband die Sicherheitserweiterung DNSSEC seit 2010 für die in Deutschland übliche Top-Level-Domain .de zur Verfügung. Die Second-Level-Domain .bund.de ist seither mit DNSSEC signiert. Verschiedene BSI-Veröffentlichungen zu Themen der Internetsicherheit referenzieren und empfehlen den Einsatz. Anfang 2015 waren jedoch nur 0,25 Prozent der registrierten .de-Domains mit DNSSEC signiert. In der Folge können auch auf DNSSEC aufbauende Sicherheitsverfahren wie DNS-DANE nicht eingeführt werden.

[9] Imperfect Forward Secrecy: How Diffie-Hellman Fail in Practice, D. Adrian et. al., abrufbar unter weakdh.org

[10] RFC 7465: Prohibiting RC4 Cipher Suites, A. Popov, Februar 2015

- Bei der Kommunikation per E-Mail ist sowohl der gesicherte Austausch von E-Mails als auch die Prüfung der Absender-Authentizität eine Herausforderung. Ein standardisiertes Verfahren zur gegenseitigen Feststellung der Authentizität des jeweiligen E-Mail-Servers nutzt zur Überprüfung im DNS hinterlegte Signaturen (DNS-DANE). Eine Hürde für die Umsetzung ist hier die bisher mangelnde Akzeptanz von DNSSEC, sodass nach wie vor ein Großteil der E-Mails unverschlüsselt übertragen wird.

- In vielen Bereichen der Internetkommunikation hat es sich inzwischen durchgesetzt, Protokolle (wie HTTP) mit TLS zu verschlüsseln. Dabei werden jedoch oftmals veraltete Verschlüsselungsalgorithmen verwendet. Auch Schwachstellen in Implementierungen, wie die 2014 bekannt gewordene Heartbleed-Schwachstelle, ermöglichen Angreifern die Auslesung der verschlüsselten Kommunikation.

- Das Internet ist ein Zusammenschluss vieler einzelner Systeme. Die Erreichbarkeiten untereinander - die sogenannten Routing-Prefixe - werden über das Border Gateway Protokoll (BGP) zwischen den einzelnen Systemen ausgetauscht. Das Prefix-Hijacking ermöglicht die Umleitung ganzer IP-Adressbereiche im Internet mit der Folge, dass die Kommunikation gestört oder Datenspionage ermöglicht wird. Ursache für diese Angriffe auf das Internetrouting sind Schwachstellen im Routing-Protokoll BGP. Mit der Resource-Public-Key-Infrastruktur (RPKI) steht ein Schutzmechanismus zur Verfügung, der aber seine vollständige Wirkung erst entfalten wird, wenn eine flächendeckende Verbreitung stattgefunden hat.

- Neben der Ausnutzung von Protokollschwachstellen sind vermehrt auch Angriffe auf die zum Datenaustausch verwendeten Geräte und Komponenten festzustellen. Hierzu gehören neben den Milliarden von Geräten der Internetnutzer auch Router, DNS-Resolver, DNS-Server oder Webserver. Insbesondere die Entdeckung von Schwachstellen in Routern und Angriffe auf diese und ähnliche Komponenten haben stark zugenommen. Hier liegt eine besondere Verantwortung bei den Herstellern dieser Komponenten, Schwachstellen zu erkennen und schnellstmöglich Sicherheitsupdates zur Verfügung zu stellen. Leider erfolgt diese Reaktion oftmals gar nicht oder nur sehr verzögert. Nutzer und Betreiber können so der Verantwortung, ihre Netzkomponenten sicherheitstechnisch auf dem aktuellen Stand zu halten, nur erschwert nachkommen.

Bewertung

Den strukturellen Schwächen der Internetarchitektur liegen vielfach Designentscheidungen aus der Vergangenheit zugrunde, die ohne Beachtung von Sicherheitsaspekten getroffen worden sind, aber nicht ohne Weiteres rückgängig gemacht werden können. Zur Verbesserung der Sicherheit ist es daher notwendig, dass zumindest die zur Verfügung stehenden Verbesserungen, beispielsweise im Bereich der Protokollerweiterungen, schnellstmöglich in die Praxis umgesetzt werden. Hersteller von Komponenten sind mehr als bisher gefordert, auch nach dem Verkauf der Geräte Verantwortung zu übernehmen und Softwareaktualisierungen bei Bekanntwerden von Schwachstellen rasch zur Verfügung zu stellen.

Gefährdung 2015

2.1.7 Mobilkommunikation

Einleitung

Mobile Geräte wie Smartphones und Tablets sowie zunehmend auch Smart Watches haben sich zu ständigen Begleitern in Beruf und Privatleben entwickelt. Viele Nutzer speichern persönliche Informationen darauf oder wickeln sensible Vorgänge über diese Geräte ab. Dies macht die Geräte zu einem lohnenden Angriffsziel für Kriminelle.

Lage

- Die Produktentwicklung im Mobilbereich ist nach wie vor rasant. Dadurch entsteht eine große Vielfalt von Gerätetypen, sowohl auf Hardware- als auch auf Softwareebene. Eine schnelle und lückenlose Bereitstellung von Software-Aktualisierungen zur Beseitigung von Sicherheitslücken ist unter diesen Bedingungen nicht gewährleistet: Updates werden manchmal gar nicht, oft nur für eine kurze Zeitspanne nach dem Kauf oder nur mit erheblicher Verspätung bereitgestellt.

- Viele der persönlichen Informationen, die man mit Mobilgeräten handhabt, werden in einer Cloud gespeichert. Der Nutzer vertraut somit dem Anbieter seine Daten an. Falls der Zugriff auf die Cloud nicht ausreichend geschützt ist, können sowohl die Nutzerdaten als auch die Zugriffsdaten für die Cloud selbst, wie Passwörter, schnell in die falschen Hände geraten.

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

- Die Ortung von Mobilgeräten und damit auch ihrer Besitzer ist für die Betreiber des Mobilfunknetzwerks, für App-Anbieter, aber auch für Cyber-Kriminelle, die Zugriff auf das Gerät haben, jederzeit möglich. In Kombination mit anderen ausgespähten Informationen können Angreifer dadurch ein umfassendes Bewegungsprofil des Opfers anlegen.

- Telefonate, die über die Mobilfunktechnologie der zweiten Generation (2G/GSM) getätigt werden, können 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 oben beschriebenen Faktoren, kombiniert mit der unüberschaubaren Masse von verfügbaren und teils Schadcode enthaltenden Apps, werden auch in absehbarer Zukunft ein hohes Gefahrenpotenzial im Bereich der Mobilkommunikation darstellen.

Am Beispiel der Mobilkommunikation wird deutlich, welchen Einfluss bestimmte Geschäftsmodelle auf die Informationssicherheit haben können. So verwendet Apple große Sorgfalt darauf, sein Betriebssystem geschlossen zu halten und die Kontrolle darüber zu behalten, welche Software auf mobilen Apple-Geräten installiert werden kann. Ausnahmen gibt es lediglich bei der Softwareverteilung innerhalb von Institutionen.

Google hingegen erlaubt auch das Installieren von Android-Apps aus fremden Quellen, was von den Anwendern auch häufig genutzt wird. Aus Sicht der Informationssicherheit haben beide Ansätze Vor- und Nachteile: Während es inzwischen mehrere Millionen verschiedener Schadprogrammvarianten für Android gibt, sind für iOS vergleichsweise wenige bekannt. Andererseits haben iOS-Benutzer deutlich weniger Kontrolle darüber, welche Programme auf ihren Geräten ablaufen und was mit ihren Informationen tatsächlich geschieht. Zumindest im Unternehmens- und Behördenkontext müssen beide Gefährdungen, Schadprogramme und Kontrollverlust, im Zuge der Risikoanalyse berücksichtigt werden.

Gefährdung 2015

Stagefright-Lücke in Android: Nachlässiges Update-Verhalten der Hersteller

Der Umgang mit der Stagefright-Lücke in Android ist ein prominentes Beispiel für das schleppende, teilweise nachlässige Update-Verhalten der Gerätehersteller. Nach Angaben des Entdeckers zLabs existierte die Lücke zum Zeitpunkt der Entdeckung auf 95 Prozent aller Android-Geräte[11]. Stagefright ist die Bezeichnung für die im Android-Betriebssystem integrierte Multimedia-Schnittstelle (Media Playback Engine). Das Android-Betriebssystem sowie installierte Apps können die Schnittstelle nutzen, um Audio- und Videoinhalte zu verarbeiten. In dieser Schnittstelle wurden insgesamt sieben verschiedene Verwundbarkeiten entdeckt, die zur Berechtigungserhöhung und zur Codeausführung genutzt werden können. Beispielsweise kann eine vom Smartphone empfangene MMS mit Multimedia-Inhalten oder der Besuch einer präparierten Webseite für einen - vom Benutzer unbemerkten - Angriff verwendet werden.

Neue Versionen von Android, die in der Regel diverse Sicherheitslücken schließen, werden von den verschiedenen Geräteherstellern oftmals mit monatelanger Verzögerung an die Smartphones ausgeliefert. Ältere Geräte werden teilweise gar nicht mehr mit Updates versorgt, sodass Sicherheitslücken offen bleiben. Nach einer Untersuchung des Online-Portals Heise[12] sind sowohl die Update-Häufigkeit wie auch die Update-Geschwindigkeit sehr unterschiedlich. Am schnellsten werden die Google-eigenen Nexusgeräte versorgt. Bei anderen Herstellern besteht jedoch eine Update-Verspätung von bis zu zehn Monaten. Auch der Gerätepreis spielt bei der Versorgung mit Updates eine Rolle. Hochwertige, teure Smartphones werden in der Regel häufiger aktualisiert als günstige Geräte.

2.1.8 Sicherheit von Apps

Einleitung

Für viele Menschen sind Smartphones und Tablets zum Dreh- und Angelpunkt ihrer digitalen Existenz geworden. Mittlerweile stehen den Nutzern Millionen von Anwendungsprogrammen – Apps – zur Verfügung, mit denen sie ihren beruflichen und privaten Alltag jederzeit und allerorts organisieren und gestalten können. Die meisten Apps aber erheben und verwerten im Hintergrund auch Informationen über den Nutzer selbst. Präferenzen, Standortdaten, die Historie der Suchanfragen, aber auch persönliche Daten über die Gesundheit wie Trainingsdauer und -intensität oder die Herzfrequenz werden im Zusammenspiel der Apps mit der Cloud zu umfassenden Nutzerprofilen verarbeitet und ggf. mit weiteren Datenquellen abgeglichen und verknüpft. Die kombinierte Nutzung

[11] http://blog.zimperium.com/experts-found-a-unicorn-in-the-last-heart-of-android/
[12] http://heise.de/-2237972

vieler Smartphones und Tablets sowohl privat als auch geschäftlich erschwert den Überblick und die Kontrolle des Anwenders über die Datenströme zusätzlich.

Lage

- Die App-Stores der großen Firmen wie Google, Apple und Microsoft bedienen ein weltweites Publikum. Bei der App-Auswahl spielen Sicherheit und Datenschutz jedoch meist eine untergeordnete Rolle. Der Wettbewerb findet vielmehr über die „User Experience" statt, die Kombination von Nützlichkeit und Bequemlichkeit sowie den Kosten einer App.

- Mobile Betriebs- und Ökosysteme[13] sind mit unterschiedlichen Sicherheitsmechanismen ausgestattet: Googles Android hat eine andere Rechteverwaltung als Apples iOS. App-Entwickler sind von den Ökosystemen der Firmen abhängig und müssen zudem in einem sehr dynamischen Umfeld agieren, in dem ihre Produkte ständig an neue Versionen und Endgerätetypen angepasst werden müssen, während die Nutzer immer mehr und ausgefeiltere Funktionalität einfordern. App-Sicherheit und Datenschutz finden deswegen oft nicht die benötigte Beachtung, die Sicherheitseigenschaften einer App können je nach Betriebssystem unterschiedlich ausfallen.

- Die Sicherheit einer App hängt vom Umgang der App mit sensitiven Informationen ab. Apps, die für die eigentliche Anwendung unnötige Rechte einfordern, sind keine Seltenheit. Anwender haben kaum die Möglichkeit, die eingeforderten Rechte manuell und individuell einzuschränken, um die App nutzen zu können. Vielfach räumen die Nutzer daher der App diese eigentlich unnötigen Rechte ein, um die App überhaupt verwenden zu können.

- Viele Apps binden Werbenetzwerke ein, um personalisierte Werbung, entweder in der App selbst oder an anderer Stelle, zu ermöglichen. Dies erweitert die mögliche Angriffsfläche.

- Die traditionellen Methoden aus dem Bereich der PC-Virenscanner können aufgrund der Isolierung der Apps untereinander (Sandboxing) nicht direkt übernommen werden. Stattdessen werden Regelwerke und Kriterien zur Bewertung der App-Sicherheit definiert, spezialisierte Firmen unterziehen Apps verschiedenen Prüfverfahren. Diese sind nur zum Teil automatisiert und wichtige Teile der Untersuchung müssen manuell durchführt werden, was sich negativ auf die Kosten und die Skalierbarkeit dieser Prüfungen auswirkt.

- Das BSI hat seit 2014 rund 100 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. Keine App kam dabei ohne einen Befund durch die Prüfung. Dabei wurde eine große Bandbreite potenzieller Probleme deutlich. Während einige Apps nur wenige der definierten Sicherheitskriterien verletzen, gehen andere höchst sorglos mit den ihnen anvertrauten Daten um. Besonders häufig sind bei den bisherigen Prüfungen die Einbindung sogenannter Tracking-Netzwerke, welche sich nicht abschalten lassen, die Erhebung von Geodaten sowie das Fehlen von entsprechenden Datenschutzerklärungen aufgefallen. In Bereichen mit hohen Sicherheitsanforderungen ist es erforderlich, alle eingesetzten Apps zu überprüfen und vor der Nutzung freizugeben.

- Mobile Device Management (MDM)-Systeme haben sich in den vergangenen Monaten weiterentwickelt. In Kooperation mit den Herstellern der mobilen Betriebssysteme werden mittlerweile Lösungen angeboten, die es ermöglichen, Regelwerke zu definieren, mit denen geschäftlich genutzte Mobilgeräte zentral verwaltet und eingeschränkt werden können. Dabei kann auch vorgegeben werden, welche Apps installiert werden dürfen. Auch Szenarien mit kombinierter privater und geschäftlicher Nutzung werden von MDM-Systemen adressiert.

Bewertung

Im privaten Umfeld müssen Anwender oftmals weiterhin Aspekte der Nützlichkeit und Bequemlichkeit von Apps mit den bereitgestellten Funktionen zu Datensicherheit und Datenschutz abwägen. Die meisten Apps lassen sich nur nutzen, wenn man alle geforderten Rechte akzeptiert, auch wenn diese nichts mit der eigentlichen Funktion der App zu tun haben. Hier sind App-Entwickler und App-Store-Betreiber gefordert, mehr Augenmerk auf Sicherheitsaspekte zu legen und dem Anwender zumindest die Wahl zu lassen, welche Rechte er akzeptiert. Im geschäftlichen Umfeld zeichnen sich Initiativen ab, MDM-Systeme stärker mit den App-Prüfungen zu integrieren. Der Markt ist noch jung: Systemübergreifende Standards für die Prüfungen sowie zur systematischen Erfassung der Sicherheitseigenschaften von Apps, auch in Hinblick auf Themen wie mobiles Bezahlen, Home Automation und mobiles Gesundheitsmanagement, müssen sich noch etablieren.

Eine gut vorbereitete Integration eines MDM-Systems, verbunden mit kontinuierlicher Überwachung und Wartung, kann entscheidende Vorteile

[13] Als Ökosystem wird in diesem Kontext die enge Verknüpfung zwischen Geräten, Betriebssystemen und Dienstleistungsangeboten eines Herstellers bezeichnet.

im Bereich der Sicherheit mobiler Geräte mit sich bringen. Es ist jedoch unwahrscheinlich, dass sich in absehbarer Zeit eine einzelne Lösung für die Trennung zwischen geschäftlichem und privatem Bereich in Mobilgeräten (Bring Your Own Device - BYOD) durchsetzt. Auch die Lösungsansätze einzelner Firmen werden in einer Vielfalt von Ausprägungen je nach Bedarf angeboten, um der Komplexität des Umfelds gerecht zu werden. Das Spannungsfeld zwischen privater und geschäftlicher Nutzung der Geräte wird somit Wirtschaft und Behördenwelt nach wie vor die Herausforderung stellen, geeignete Lösungen speziell für die jeweiligen Gegebenheiten anzupassen. Dieser Herausforderung wird sich das BSI auch in den kommenden Jahren weiterhin stellen.

Gefährdung 2015

2.1.9 Sicherheit von Industriellen Steuerungsanlagen

Einleitung

Industrielle Steuerungsanlagen (engl. Industrial Control Systems, ICS) sind nicht nur elementarer Bestandteil vieler Kritischer Infrastrukturen. Auch in vielen anderen Anwendungsgebieten der Fabrikautomation und Prozesssteuerung ist deren Verfügbarkeit und Integrität essenziell, um die dort stattfindenden physikalischen Prozesse zu steuern. Dies stellt eine große Herausforderung dar, wenn die Zukunftsvision von Industrie 4.0 mit einer vollumfänglichen Vernetzung auch über Unternehmensgrenzen hinaus tatsächlich Realität werden soll. Die Sicherheitsrisiken in ICS sind – entgegen der öffentlichen Wahrnehmung – nicht auf die Unsicherheit einzelner Komponenten zurückzuführen. Eine hinreichend sichere Fabrikautomation oder Prozesssteuerung bedarf neben geeigneter Komponenten auch einer nach einem Sicherheitskonzept konzipierten und integrierten Maschine bzw. Anlage sowie geeigneter Maßnahmen in der Betriebsphase als Teil eines Sicherheitsmanagements. Es sind also neben Herstellern von Komponenten auch Maschinenbauer und Integratoren sowie die Betreiber gefordert.

Lage

- Mit dem zunehmenden Einsatz von Komponenten der Standard-IT im industriellen Umfeld hat es in der Vergangenheit häufig Produktionsausfälle durch nicht zielgerichtete Schadsoftware gegeben. Bei diesen Kollateralschäden wurden beispielsweise Steuerungskomponenten oder Bedienterminals mit einer allgemeinen Schadsoftware infiziert und zum Absturz gebracht. Hierbei waren in vielen Fällen nicht einzelne Rechner, sondern gesamte Produktionsstandorte betroffen. Auch Fälle von Ransomware oder Spyware wurden im industriellen Umfeld beobachtet. Bei Fällen mit Ransomware verschlüsselte die Schadsoftware nicht nur lokale Daten auf dem betroffenen PC, sondern auch die Daten auf zugreifbaren zentralen Dateiablagen. Ein Grund hierfür sind ICS-Systeme, die nicht mit Updates versorgt wurden und somit zum Teil offene Schwachstellen enthalten, die bereits seit mehreren Jahren bekannt sind. Die Infektion erfolgte beispielsweise über die Office-IT, die nur unzureichend vom Produktionsnetz getrennt war, über direkt mit dem Internet verbundene ICS-Komponenten oder über USB-Sticks (die beispielsweise für Updates genutzt werden), auf denen Schadsoftware enthalten war.

- Zielgerichtete Angriffe nehmen meist ihren Anfang über die Office-IT oder auf Engineering Workstations, wo eine Infektion über Spear Phishing oder manipulierte Webseiten erfolgt. Dabei stellt sich im industriellen Umfeld häufig heraus, dass eine

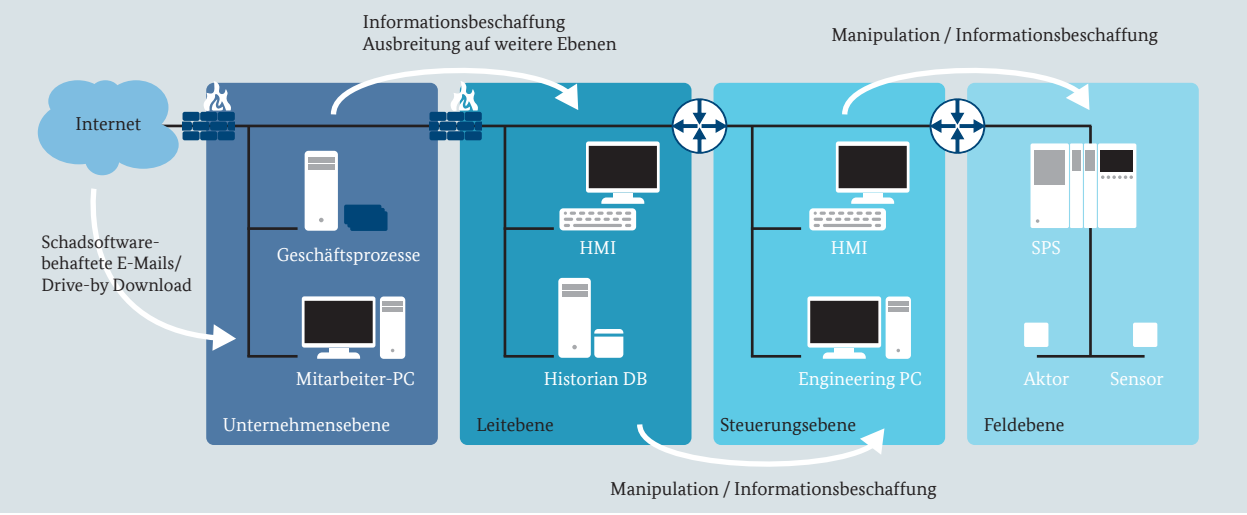

Abbildung 3: Ablauf mehrstufiger Angriffe auf eine typische ICS-Infrastruktur

Ausbreitung der Angreifer im Unternehmen bis in die Produktionsnetze hinein nicht hinreichend verhindert wird. So ist es in solchen Fällen mitunter mit geringem Aufwand möglich, kritische Daten zu stehlen oder Produktionsanlagen zu manipulieren – also an die Kronjuwelen des Unternehmens zu gelangen. Die Ursache sind fehlendes Bewusstsein für die Risiken, mangelhafte organisatorische Prozesse und eine aus IT-Sicherheitssicht unzureichende technische Umsetzung. Über gezielte Angriffe wird insbesondere im industriellen Umfeld noch sehr viel zurückhaltender berichtet als in der klassischen IT. Das BSI sichert in solchen Fällen ein maximales Maß an Vertraulichkeit zu, weshalb an dieser Stelle keine solchen Angriffe auf deutsche Unternehmen konkret genannt werden.

- Es stellt sich auch die Frage der Cyber-Sicherheit von Komponenten der funktionalen Sicherheit, die Mensch und Umwelt im Falle einer Fehlfunktion vor der Maschine oder Anlage schützen sollen. Es ist zu beobachten, dass diese Komponenten in verstärktem Maße über die allgemeinen Produktionsnetze und mit operativen Steuerkomponenten kommunizieren. Somit sind Angriffe möglich, bei denen sämtliche Schutzfunktionen übergangen werden können.

Bewertung

Im Jahr 2015 ist eine steigende Sensibilität für das Thema IT-Sicherheit in ICS zu erkennen. Dies führt in einzelnen Unternehmen zu erheblichen Fortschritten bei der IT-Sicherheit. Dieser Trend muss fortgesetzt und signifikant gesteigert werden, um den bestehenden und neuen Gefahren etwas entgegensetzen zu können. Hierzu sind sowohl Hersteller von Komponenten als auch Maschinenbauer und Integratoren sowie Betreiber gefordert.

Hersteller müssen Sicherheit als integralen Bestandteil und Entwurfsziel verstehen und dies u.a. durch Entwicklungsrichtlinien oder sicherheitsspezifische Tests umsetzen. Besonders wichtig ist ein zeitnahes Bereitstellen von Informationen zu Schwachstellen.

Für Maschinenbauer und Integratoren gelten vergleichbare Anforderungen, da die konzipierte Maschine bzw. Anlage als eigenes Produkt verstanden und deren Sicherheit ganzheitlich umgesetzt werden muss. Besonders wichtig ist dabei ein hinreichender Informationsfluss zwischen Herstellern und Betreibern.

Betreiber müssen Sicherheit als fortlaufenden Prozess verstehen und dies in einem Sicherheitsmanagement umsetzen. Hierzu gehören nicht nur organisatorische Prozesse, sondern auch technische Maßnahmen wie beispielsweise die Segmentierung der Netze.

Im industriellen Umfeld müssen dringend die bewährten Best Practices in der Fläche umgesetzt werden. Dabei muss auch die funktionale Sicherheit berücksichtigt werden. Für das industrielle Umfeld sollte – wie heute auch schon in der konventionellen IT – zudem das Paradigma „Assume the Breach“ gelten und im Rahmen des ganzheitlichen Sicherheitsmanagements berücksichtigt werden. Ein rein präventiver Ansatz am Netzübergang (Perimeter) ist daher nicht mehr zielführend. Vielmehr gilt es, Angreifer im eigenen Produktionsumfeld zu erkennen und zeitnah zu reagieren.

Gefährdung 2015

US-Forscher hacken Geländewagen

Im Sommer 2015 gelang es US-Computerexperten, über das Internet durch eine Schwachstelle in das Infotainmentsystem eines Geländewagens kabellos einzudringen. Die Forscher konnten den Zugriff vom Infotainmentsystem auf das CAN-Bussystem des Fahrzeugs ausweiten und so die Kontrolle über die daran angeschlossenen elektronischen Steuergeräte bis hin zur Gas- und Bremsregulierung übernehmen. Mit der Manipulation der digitalen Systeme gelang somit ein Übergriff auf die mechanischen Systeme des Fahrzeugs. Der Fahrer verlor in dem Versuchsszenario während der Fahrt die Kontrolle über den Wagen und die vermeintlichen Angreifer manövrierten den Geländewagen in einen Graben. Zum Zeitpunkt des Angriffes befanden sich die Angreifer mehrere Kilometer entfernt vom Fahrzeug. Das Infotainmentsystem des betroffenen Fahrzeugs bündelt zahlreiche wichtige Funktionen und ist in der Regel als mobiler WLAN-Hotspot die Schnittstelle zu den Smartphones oder Tablets der Insassen. Neben diesem Angriff auf die Fahrzeug-IT, die im Ernstfall gravierende Folgen für die Sicherheit auf den Straßen hätte, gab es weitere Versuche, bei denen Forscher Schwächen in der Bordelektronik von Fahrzeugen belegen konnten. So konnte unter anderem bei einem deutschen Automobilhersteller das Verriegelungssystem per Mobilfunk ausgehebelt werden.
Die Versuche zeigen eindrücklich die Möglichkeiten und Einfallstore, die Angreifer bereits heute im Bereich der Fahrzeug-IT vorfinden und die sich auf die Sicherheit im Straßenverkehr erheblich auswirken können. Automobilhersteller und Zulieferer sind daher aufgefordert, die digitalen Bestandteile eines Steuergeräts vor unbefugtem Zugriff oder Veränderung zu schützen und die IT-Sicherheit bereits im Rahmen des Produktionsprozesses mit zu bedenken. Durch die Digitalisierung der Fahrzeuge werden künftig auch Automobilhersteller wie klassische Software-Hersteller, Herausforderungen in den Bereichen Softwareentwicklung, Reaktion auf Schwachstellen und Patchverfahren angehen müssen. Zum Aufbau und Betrieb maximal sicherer Fahrzeug-IT müssen künftig Sicherheitsstandards vergleichbar den in anderen Bereichen bewährten Schutzprofilen oder Technischen Richtlinien entwickelt werden. Automobilhersteller könnten damit einen wichtigen Nachweis zur Sicherheit ihrer IT-Systeme in den Fahrzeugen liefern.

2.2 Angriffsmethoden und -mittel

2.2.1 Schadsoftware

Einleitung

Als Schadsoftware, Schadprogramme oder Malware werden Computerprogramme bezeichnet, die unerwünschte oder schädliche Funktionen auf einem infizierten Computer ausführen. Die früher übliche eindeutige Klassifizierung von Schadsoftware ist heute oft nicht mehr möglich, da moderne Schadprogramme meist aus mehreren Komponenten bestehen, die unterschiedliche Funktionen haben und bei Bedarf weitere Module mit anderen Funktionen nachladen können. Zu den häufigsten Infektionswegen gehören E-Mail-Anhänge sowie die vom Anwender unbemerkte Infektion beim Besuch von Webseiten.

Lage

- Die Gesamtzahl der Schadprogrammvarianten für PCs liegt nach Schätzungen derzeit bei über 439 Millionen mit einem Anstieg der individuellen Verbreitung von immer neuen, automatisch generierten Schadprogrammvarianten. Aufgrund seines hohen Marktanteils ist hauptsächlich das Betriebssystem Windows betroffen.

- Die Anzahl der Varianten von Schadsoftware für mobile Plattformen nimmt weiterhin rasant zu. Rund 96 Prozent der Schadsoftware trifft aufgrund seines Verbreitungsgrads das Betriebssystem Android. Auf mobilen Computern werden Schadprogramme überwiegend als legitime Apps oder Updates getarnt, bei deren Installation die Benutzer unwissentlich eine Infektion herbeiführen. Die größte Gefahr geht von Software in App-Stores aus, die nicht von großen Betreibern wie Apple, Microsoft oder Google bereitgestellt werden und keine Überprüfung von Apps beinhalten.

- 59 Prozent der bis September 2015 von AV-Produkten detektierten schadhaften Android-Apps sind Trojanische Pferde. 2014 lag der Anteil bei 51 Prozent. Die Anzahl von Adware-Detektionen sank dagegen im gleichen Zeitraum von 26 Prozent auf 10 Prozent.

- Ransomware verbreitet sich im Jahr 2015 noch stärker als 2014. Dieser Schadprogrammtyp verschlüsselt Dateien oder verhindert den Zugriff auf den Computer, um Lösegeld zu erpressen, das häufig in Krypto-Währungen wie Bitcoin gezahlt werden soll. Neuere Versionen wie beispielsweise „Cryptowall 3.0“ verbreiten sich über Drive-by-Exploits und Exploit-Kits. Dabei werden moderne kryptografische Verfahren verwendet, um die Dokumente auf dem infizierten Computer zu verschlüsseln. Vor der Infektion angelegte Backups sind häufig die einzige Möglichkeit, die Daten wiederherzustellen.

- Durch die Vielzahl automatisch generierter Schadprogrammvarianten bietet der klassische signaturbasierte AV-Ansatz immer weniger Schutz, weil die neuen Varianten schneller erzeugt als analysiert werden können oder die Dauer der Schadprogramm-Verteilwellen (Spam) nicht mehr zur Erstellung/Einspeisung geeigneter Abwehrmaßnahmen (AV-Signaturen) reicht. Dies erschwert die Erkennung und Abwehr und führt zu einem größeren Zeitfenster, in dem der Nutzer ungeschützt ist. Zudem wird die Analyse von Schadprogrammen häufig durch die Erkennung von Analyse-Tools und virtuellen Maschinen oder durch eine verzögerte Ausführung erschwert. Um die Entdeckung der Kommunikation eines Schadprogramms zu erschweren, werden zunehmend 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.

- Schadsoftware-Infektionen nach ungezielten Angriffen wurden auch in der Cyber-Sicherheitsumfrage 2015[14] der Allianz für Cyber-Sicherheit als häufigste Angriffsart benannt.

- Die Verbreitungswege von Schadprogrammen sind vielfältig: Drive-by-Exploits, Spam-E-Mails, Links auf Schadprogramme. Schadsoftware installiert zunehmend Root-Zertifikate eigener Zertifizierungsstellen, um Man-in-the-Middleangriffe auszuführen.

- Der im Jahr 2014 festgestellte Trend, Makro-Viren für Microsoft-Office-Produkte einzusetzen, hält an. Dabei wird der Schadcode zunehmend verschleiert, um die Erkennung und Analyse zu erschweren. Dem Anwender wird suggeriert, das vermeintliche Dokument könne nur richtig angezeigt werden, wenn er die Makro-Funktionen erlaubt und so die Ausführung des Schadprogramms ermöglicht.

Bewertung

Schadprogramme sind weiterhin eine der größten Bedrohungen sowohl für private Anwender als auch für Unternehmen und Behörden. Gegenüber 2014 haben sich die Schadprogramme weiterentwickelt und die klassischen Abwehrmaßnahmen werden zunehmend umgangen. Mobile und

[14] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Micro/Umfrage/umfrage2015.html

Ransomware im Krankenhaus

Sachverhalt: Unter Einsatz der Schadsoftware Cryptowall (Ransomware/Cryptoware) infizieren Kriminelle Rechner und verschlüsseln darauf liegende Daten. Daraufhin erpressen die Angreifer vom Opfer Lösegeld, bei dessen Zahlung die Verschlüsselung rückgängig gemacht werden soll. Im April 2015 war ein System eines Klinikkonsortiums von der Ransomware betroffen, die dort Gesundheitsdaten wie Arztbriefe und Abrechnungen verschlüsselte.

Ursache: Die Infektion mit der Schadsoftware ist vermutlich auf Anwendungssoftware zurückzuführen, die nicht auf dem aktuellen Stand in Bezug auf Sicherheitsupdates war.

Methode: Der genaue Angriffsvektor wurde in diesem Fall nicht ermittelt. Die Infektion mit der Schadsoftware erfolgte wahrscheinlich über einen Drive-by-Exploit auf einer Webseite, nachdem ein Link in einer E-Mail aufgerufen wurde.

Schadenswirkung: Nach der Detektion konnte ein Backup eingespielt werden, wodurch sich der Datenverlust auf eine Zeitspanne von zwölf Stunden begrenzen ließ. Ein weiterer finanzieller Schaden ist jedoch nicht ausgeschlossen, da Abrechnungen ggf. nicht mehr nachvollzogen werden können und die erneute Erstellung von Arztbriefen und die Aktualisierung der medizinischen Dokumentation zusätzlichen Aufwand generiert.

Zielgruppen: Bei Cryptowall handelt es sich um eine Schadsoftware, die von Cyber-Kriminellen ungezielt eingesetzt wird, um Geld zu erpressen. Alle Anwendergruppen können folglich davon betroffen sein. Dass im konkreten Fall ein Unternehmen aus dem KRITIS-Sektor Gesundheit betroffen war, zeigt, dass auch KRITIS-Unternehmen für alltägliche Angriffe von Cyber-Kriminellen anfällig sind.

Technische Fähigkeiten: Cyber-Angriffe mit Ransomware zur Erpressung von Geld sind heute Alltag und gehören zum typischen Angriffsspektrum von Cyber-Kriminellen.

alternative Plattformen geraten zunehmend in den Fokus der Angreifer. Schadprogramme werden oft durch Mitwirkung des Nutzers installiert, wodurch technische Schutzmaßnahmen umgangen werden und Angreifer in abgesicherte Netze eindringen können. Zum Schutz reichen klassische AV-Lösungen und Firewalls nicht mehr aus, vielmehr muss IT-Sicherheit als Gesamtkonzept verstanden und umgesetzt werden, wozu auch die Einbeziehung des Nutzers gehört.

Gefährdung 2015

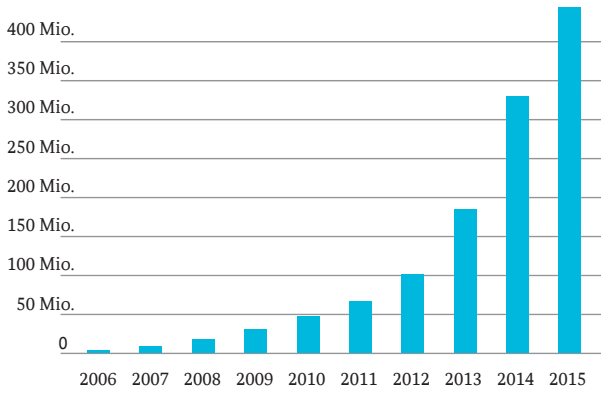

Abbildung 4: Anzahl bekannter Windows-Schadprogrammvarianten

2.2.2 Social Engineering

Einleitung

Beim Social Engineering wird die „Schwachstelle Mensch“ gezielt ausgenutzt. Angreifer verleiten ihre Opfer dazu, Schutzmechanismen zu umgehen oder unbewusst Schadprogramme zu installieren, um so an schützenswerte Daten und Informationen zu gelangen. Dazu spionieren die Täter das persönliche Umfeld aus und nutzen dieses Wissen über das Opfer, um dessen Vertrauen zu gewinnen. Dabei nutzen sie menschliche Schwächen wie Vertrauen, Neugier, Respekt vor Autorität, Zugehörigkeitsgefühl oder Hilfsbereitschaft aus. Die Opfer handeln meist aus Unwissenheit, aus einer Stresssituation heraus oder aus Höflichkeit und werden so zu einem Werkzeug des Angreifers. Angriffe durch Social Engineering geschehen oft mehrstufig, wobei die Resultate der einzelnen Stufen sukzessive in den fortlaufenden Angriffsoperationen verwertet werden.

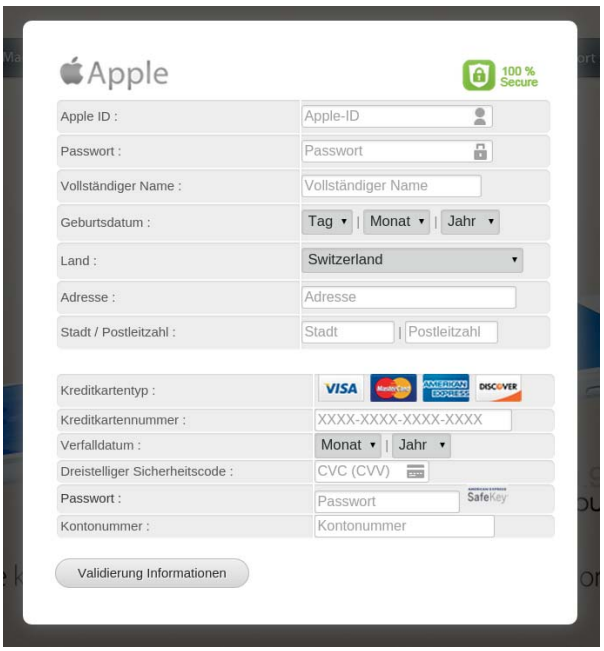

Abbildung 5: Apple-ID Phishing-Webseite

Lage

- Über eine Milliarde Menschen sind in Sozialen Netzwerken miteinander verbunden. Angreifer haben über diese große Datenansammlung die Möglichkeit, schnell und anonym persönliche Daten von bestimmten Personen für ihre Angriffe zu erhalten. Je mehr persönliche Informationen jeder Nutzer preisgibt, desto einfacher haben es die Angreifer. Diese suchen in Sozialen Netzwerken gezielt nach Personen einer bestimmten Organisation und nutzen die so gewonnenen Informationen, um über diese Zielpersonen das Unternehmen anzugreifen.

- Fast täglich passieren Phishing-Angriffe, die als Massen-E-Mail vorgeblich von bekannten und vertrauenswürdigen Organisationen wie Banken, Telefongesellschaften oder Online-Shops versendet werden. Mit fiktiven Sicherheitsproblemen, hohen Rechnungsbeträgen oder Statusmeldungen zu Aufträgen werden die Nutzer verleitet, persönliche Informationen wie Zugangsdaten, Konto- oder Kreditkartennummern oder andere Kundendaten auf gefälschten Webseiten einzutragen, die an die Angreifer übermittelt werden.

- Auf gleiche Weise werden Nutzer dazu verleitet, Anhänge in E-Mails zu öffnen oder Links in E-Mails aufzurufen, was in beiden Fällen die Installation eines Schadprogramms zur Folge haben kann.

- Bei gezielten Angriffen wird Social Engineering in der ersten Phase des Angriffs eingesetzt. Der Angreifer sammelt zuerst Informationen über sein Opfer und nutzt diese, um Angriffsmöglichkeiten zu entwickeln:
  - Anhand der Profildaten kann er das Passwort des Opfers erraten, wenn dieses schlecht gewählt ist (Brute-Force-Angriff)
  - Mithilfe der Informationen über das Opfer kann er Vertrauen aufbauen, um vertrauliche Informationen zu erlangen (Social Hacking)
  - Durch den Versand einer personalisierten E-Mail (Spear-Phishing-Angriff) kann er ein Schadprogramm auf dem Rechner des Opfers installieren und auszuführen.

- Seit Anfang 2015 kommt es vermehrt zu Anrufen von angeblichen Microsoft-Mitarbeitern, die die Opfer über eine vorgebliche Schadprogramminfektion des Rechners oder über Probleme mit der Windows-Lizenz informieren. Die Anrufer bieten den Betroffenen an, das System zu bereinigen und verleiten die Opfer dazu, eine Fernwartungs-Software zu installieren, über die Schadsoftware nachgeladen oder sensible Daten entwendet werden können.

- Lukrativ im geschäftlichen Umfeld ist der „Fake-President-Angriff“. Dabei gibt sich ein Angreifer 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. Allen Fake-President-Angriffen ist gemein, dass die Betrüger ihre Opfer vorab ausführlich ausspioniert haben und dadurch unter anderem der Stil der Kommunikation im Unternehmen authentisch nachgestellt werden konnte.

- In Anbetracht des Risikos, das durch Social Engineering entsteht, sind die Schutzmaßnahmen eher mäßig: Der Cyber-Sicherheitsumfrage 2015[15] des BSI zufolge führen nur 50 Prozent der befragten Unternehmen regelmäßig Sensibilisierungsmaßnahmen durch. Es mangelt in weiten Teilen an Awareness auf allen Hierarchieebenen.

Bewertung

Social Engineering ist weiterhin ein beliebtes Mittel, um Cyber-Angriffe erfolgreich auszuführen oder zu unterstützen. Selbst sehr hohe technische Absicherungen lassen sich durch die Schwachstelle Mensch umgehen. Für den Angreifer ist es einfacher, das schwächste Glied Mensch anzugreifen, anstatt komplexe technische Sicherheitsmaßnahmen mit viel Aufwand zu umgehen. Schulungs- und Sensibilisierungsmaßnahmen sind daher regelmäßig erforderlich, um die Nutzer gegen diese Angriffsmethoden zu wappnen. Je mehr Sicherheitsbewusstsein und Digitale Bildung bei Anwendern aller Hierarchieebenen vorhanden ist, desto schwerer wird es für Angreifer, menschliche Schwächen auszunutzen.

Gefährdung 2015

Social Engineering per Telefon

Sachverhalt: Wie im Vorjahr gab es auch im aktuellen Berichtszeitraum immer wieder Wellen von Social-Engineering-Angriffen, bei denen sich Kriminelle am Telefon als Support-Mitarbeiter der Firma Microsoft ausgaben und versuchten, unter Vorspiegelung angeblicher Lizenzprobleme oder Schadsoftware-Infektionen die Angerufenen dazu zu bewegen, persönliche Daten preiszugeben oder dem Anrufer einen Zugang zu ihrem Rechner zu ermöglichen.

Methode: Die Täter geben sich bei ihren Anrufen als Microsoft-Support-Mitarbeiter aus, die ein angebliches Problem mit der Betriebssystemlizenz des Opfers oder eine Schadsoftware-Infektion festgestellt haben und dies in Zusammenarbeit mit dem Kunden beheben wollen. Im Verlauf des Gespräches werden die Opfer überzeugt, eine Fernwartungssoftware zu installieren, damit der vorgebliche Support-Mitarbeiter Zugriff auf das System erhält, um das angebliche Problem direkt zu lösen. Mithilfe dieser Software hat der Angreifer vollständigen Zugriff auf das System und alle darauf gespeicherten Daten. In manchen Fällen werden am Telefon auch die Kreditkartendaten des Kunden erfragt, um damit den angeblich geleisteten Support zu bezahlen.

Schadenswirkung: Der Fernzugriff auf die Systeme und die Daten der Opfer erlaubt es den Angreifern, beliebige Schadprogramme auf den Computern auszuführen oder direkt nach Informationen zu suchen, die sich für kriminelle Zwecke verwerten lassen. Ein solcher Eingriff stellt eine Verletzung der Privatsphäre dar. Schafft es der Angreifer, dem Opfer Konto- oder Kreditkartendaten zu entlocken, so entstehen Letzterem durch Abbuchungen unmittelbare finanzielle Schäden.

Zielgruppen: Die Telefonanrufe erfolgen weitgehend wahllos. Aufgrund der sehr hohen Verbreitung des Betriebssystems Windows und anderer Microsoft-Software und der damit verbundenen Erfolgswahrscheinlichkeit, einen Microsoft-Kunden am Telefon zu erreichen, geben sich die Angreifer als Microsoft-Mitarbeiter aus. Besonders häufig sind Privatanwender Opfer dieser Betrugsversuche, da viele für diese Art von Angriff nicht sensibilisiert sind und häufig von einem tatsächlichen Problem ausgehen.

Technische Fähigkeiten: Bei diesem Angriff werden keine besonderen technischen Fähigkeiten angewandt. Bedeutsam ist vielmehr der Organisationsgrad der Täter, die vermutlich ganze Callcenter für diese Form des Social Engineerings einsetzen.

[15] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Micro/Umfrage/umfrage2015.html

2.2.3 Gezielte Angriffe - APT

Einleitung

Ein Advanced Persistent Threat (APT)-Angriff zeichnet sich im Gegensatz zu üblichen Cyber-Angriffen meist dadurch aus, dass dem Angreifer sowohl Zeit als auch Mittel in Form von Geld, Informationen und Entwicklungskapazitäten in großer Menge zur Verfügung stehen. Ein APT verfolgt langfristige Ziele. Die Angreifer nutzen zur Infektion individuell zugeschnittene Angriffsvektoren und stellen sicher, dass sie dauerhafte Zugriffsmöglichkeiten auf infizierte Systeme haben. Eine Netzwerkkompromittierung wird daher nicht aufgrund der Nutzung einer komplexen Schadsoftware als APT klassifiziert. Stattdessen fußt eine solche Bewertung meist auf dem verwendeten Angriffsvektor und der Tatsache, dass sich die Täter im internen Netz festgesetzt und auf mehrere Systeme – typischerweise zentrale Server – ausgebreitet haben.

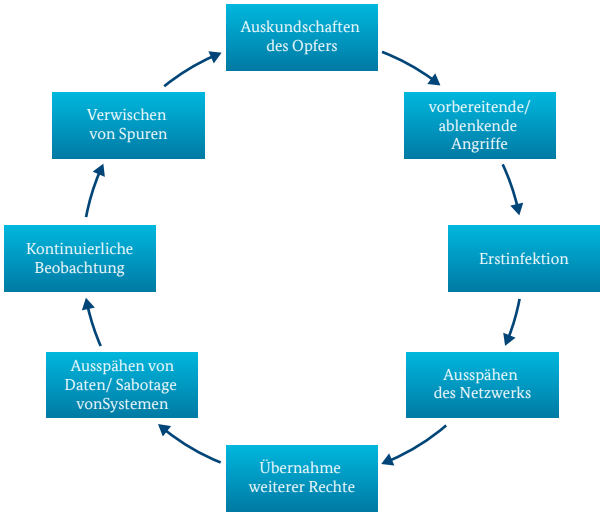

Abbildung 6: Vorgehensweise bei einem APT-Angriff

Lage

- Nur wenige APT-Angriffe werden öffentlich bekannt, valide Zahlen und Statistiken liegen kaum vor oder zeigen nur einen Ausschnitt der Gesamtlage. Die Dunkelziffer ist hoch, weil die meisten Opfer für sich behalten, dass sie Opfer wurden.
- Die Zeitspanne zwischen Infektion und Entdeckung eines APT-Angriffs beträgt in den meisten Fällen mehrere Monate. Viel Zeit, in der sich Angreifer ungehindert in den Netzen des Opfers bewegen und Informationen ausspionieren können.

Cyber-Angriff auf den Deutschen Bundestag

Anfang Mai 2015 informierte das Bundesamt für Verfassungsschutz den Deutschen Bundestag und das BSI über Hinweise, dass mindestens zwei Rechner aus dem Netz des Deutschen Bundestages kompromittiert wurden. Das BSI nahm daraufhin mit dem Deutschen Bundestag Kontakt auf, wo man ebenfalls bereits Anomalien im Netz festgestellt hatte. Diese Auffälligkeiten im Netz des Deutschen Bundestags deuteten bereits zu diesem Zeitpunkt darauf hin, dass zentrale Systeme des internen Bundestagsnetzes kompromittiert waren. Gemeinsam mit einem externen Dienstleister untersuchte das BSI daraufhin im Auftrag des Deutschen Bundestags den Vorfall, um das Ausmaß der Kompromittierung festzustellen.

Es stellte sich heraus, dass die Täter anhand der klassischen APT-Methode vorgegangen waren, bei der zunächst einzelne Arbeitsplatzrechner mit einer Schadsoftware infiziert werden. Diese Erstinfektion erlaubt es typischerweise, Dateien hoch- und herunterzuladen. Die genaue Analyse der Erstinfektion in den Logdateien war durch die kurze Speicherfrist von maximal sieben Tagen nicht möglich. Die Täter nutzten diese Funktionalität, um auf dem infizierten System weitere Tools nachzuladen, darunter auch öffentlich verfügbare und von vielen Tätergruppen genutzte Werkzeuge. Die nachgeladene Software diente unter anderem dazu, die Zugangsdaten eines Systemkontos für die Softwareverteilung herauszufinden und dies für die weitere Ausbreitung im internen Netz zu verwenden. Die Analyse ergab, dass auf einzelnen Systemen ein Backdoor-Schadprogramm installiert worden war, das den Angreifern jederzeit erlaubt, auf das System zuzugreifen. Daneben wurden weitere Angriffstools und Schadprogramme wie Keylogger, die Tastatureingaben mitschneiden und Bildschirmfotos erstellen, sowie selbst geschriebene Skripte zum Sammeln von Dokumenten bestimmter Dateitypen gefunden. Aufgrund der Analyse des Vorfalls ist davon auszugehen, dass es die Täter unter anderem auf ausgewählte E-Mail-Postfächer abgesehen hatten.

Der Angriff entspricht dem klassischen APT-Muster, das von nahezu allen bekannten Cyber-Spionagegruppen angewandt wird. Bei der Ausbreitung im internen Netz („Lateral Movement“) setzten die Angreifer auf gängige Methoden und öffentlich verfügbare Tools, wie sie auch von weniger professionellen Tätern verwendet werden. Dies kann dadurch begründet sein, dass man eine Zuordnung des Angriffs erschweren wollte. Allerdings führten einige Fehler der Angreifer dazu, dass ihre Aktivitäten im Netz nachzuvollziehen und zu detektieren waren.

- Wie schon 2014, so waren auch 2015 insbesondere die Branchen Rüstung, Hochtechnologie (Auto, Schiffbau, Raumfahrt), Forschungseinrichtungen sowie die Öffentliche Verwaltung Ziel von APT-Angriffen.

- Die Erstinfektion erfolgt nach wie vor oft durch „Watering Hole"-Angriffe sowie durch das Versenden von E-Mails mit einem präparierten Dokumentenanhang und einem Beitext mit gutem Social Engineering, durch welchen das Opfer dazu gebracht wird, das Schaddokument zu öffnen. Die E-Mail ist häufig so gestaltet, dass es für das Opfer beinahe unmöglich ist, die Fälschung zu erkennen.

- Die Angreifer verankern sich meist tief im System des Opfers und nutzen alle denkbaren technischen Möglichkeiten, um es dem Opfer sehr schwer zu machen, den Angreifer wieder aus dem Netzwerk zu entfernen. Neben den bisher durchgeführten Spionageaktivitäten gehen die Angreifer auch in Einzelfällen dazu über, die erbeuteten Privilegien zur Störung des Betriebes oder zu Propagandazwecken zu missbrauchen. Für das Opfer ist die Bereinigung des Netzwerkes mit hohen personellen und finanziellen Aufwänden verbunden.

- Aus der Kombination von meist nicht adäquaten Schutzmaßnahmen – häufig sind nicht einmal grundlegende IT-Sicherheitsmaßnahmen umgesetzt – und der großen Persistenz der Angreifer entsteht durch APT-Angriffe häufig ein großer Schaden. Dies schließt einerseits die Kosten zum Entfernen der Angriffswerkzeuge und notwendige Säuberungsarbeiten ein, auf der anderen Seite sind dies die Kosten durch abhanden gekommene Daten sowie mögliche geschäftliche Einbußen aufgrund des Datenabflusses.

- Hochwertige Angriffe werden nicht mehr nur von Nachrichtendiensten durchgeführt, sondern zunehmend auch von kriminellen Organisationen.

- Aufgrund der zunehmenden Zahl von APT-Akteuren und -Angriffen ist in Bezug auf die Abwehr und Analyse dieser Angriffe inzwischen ein Markt entstanden. Veröffentlichungen von Dienstleistern und Sicherheitsfirmen zu diesem Thema sollten stets auch im Bewusstsein gelesen werden, dass es sich dabei auch um die eigene Positionierung im Wettbewerb handelt. Dennoch sollte man Veröffentlichungen zu großen APT-Kampagnen nicht als Hype abtun, da sie dokumentieren, dass diese Angriffe weiter verbreitet sind, als landläufig angenommen wird.

Umgang mit einem APT-Angriff

APT-Angriffe sind zielgerichtete Cyber-Angriffe auf sehr stark eingegrenzte Systeme und Netzwerke. Die Angreifer verfügen in der Regel über hohe finanzielle und personelle Ressourcen. APT-Angriffe können nur sehr schwer verhindert werden, da sie oft mit großem Aufwand so entworfen wurden, dass die Standardschutzmaßnahmen umgangen werden können. Bei einem APT-Angriff muss möglichst rasch eine ganze Reihe von Maßnahmen ergriffen werden. Diese dienen einerseits der Begrenzung des Aktionsradius des Angreifers, dürfen aber andererseits den Angreifer nicht zu früh alarmieren, damit dieser keine Spuren verwischen kann und die Aufklärung des Vorfalls dadurch nicht erschwert oder unmöglich wird. Folgende grundlegende Schritte sollten beachtet werden:

1. Analyse: genutzte Angriffswerkzeuge, erkennbare Angriffsmuster, Ausmaß des Angriffs
2. Kontrolle: Aktivitäten des Angreifers unter Kontrolle halten, Aktionsradius des Angreifers einschränken
3. Bereinigung: Bereinigung infizierter Systeme und Netze, ggf. Neuaufsetzung
4. Härtung des Systems: Erfahrungen und Lehren aus dem aktuellen APT-Angriff nutzen, um das System besser abzuschotten und zukünftige Angriffe besser abwehren zu können.

Bewertung

APT-Angriffe sind aktuell und zukünftig eine große Bedrohung für Unternehmen und Verwaltungseinrichtungen. APT-Angriffe zum Zweck der Wirtschaftsspionage oder Konkurrenzausspähung werden auch in Zukunft von verschiedenen Gruppen durchgeführt werden. Insbesondere Unternehmen, die international aktiv und sichtbar sind, sollten APT-Angriffe in ihr unternehmerisches Risikomanagement einbeziehen und IT-Sicherheitsmaßnahmen im Bereich Detektion und Monitoring sowie im Bereich der Vorfallsbearbeitung vornehmen.

Gefährdung 2015

2.2.4 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 ermöglicht. 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 Seite mit Drive-by-Exploits verweist.

Lage

- Nach einem Anstieg im Jahr 2014 hat die Spamaktivität 2015 auf circa 30 Prozent des Volumens im Vergleich zum Vorjahr abgenommen (Abb. 7). Der Rückgang ist hauptsächlich im Bereich des klassischen Spams zu verzeichnen. Die beliebtesten Themen waren 2015 bislang Partnervermittlung, Medikamente und dubiose Jobangebote.

- Die Anzahl von Spamnachrichten mit Schadsoftware im Anhang ging auf ca. 75 Prozent des Vorjahresniveaus zurück.

- Dabei stieg der Anteil von Schadprogramm-Spam, für die zuvor auf anderen infizierten Systemen gesammelte aktuelle E-Mail-Adressen verwendet werden. Verantwortlich dafür sind oft Schadprogramme aus der Geodo-Familie.

- In Spamnachrichten werden die Empfänger häufig mit korrektem Namen angesprochen, was die Chance erhöht, dass die schadhaften Inhalte angeklickt werden.

- Die seit Mitte 2014 versendeten Office-Dokumente, die Makros zum automatischen Schadsoftware-Download beinhalten, sind nach wie vor unterwegs und wurden von den Tätern weiterentwickelt. Dazu verschleiern und variieren diese zunehmend den Makro-Code. Teilweise wurden Schadprogramme als unsichtbarer Text im Dokument kodiert eingebettet, sodass kein nachträglicher Download mehr nötig war. Vereinzelt wurde auch mit eingebetteten Download-Skripten gearbeitet, die beim Doppelklick innerhalb des Dokuments ausgeführt werden.

- Die Angreifer versenden statt eines schadhaften Anhangs häufig einen Link zum Herunterladen der Schadsoftware. Dieser wird in entsprechenden Mail-Anschreiben als Link zu Rechnungen, Mahnungen, Paketversand-Benachrichtigungen oder Ähnlichem getarnt. Kriminelle ahmen dafür E-Mail-Vorlagen namhafter und bekannter Firmen nach. Die Links werden in einigen Fällen in angehängten Dokumenten versendet, wahrscheinlich mit dem Ziel, die Erkennung zu erschweren.

- Der Versand von Schadsoftware variiert zeitlich sehr stark (Abb. 8). Im Vergleich zum letzten Jahr hat der Versand an Donnerstagen und Freitagen zugenommen, der Schwerpunkt hat sich insgesamt leicht auf die Vormittagsstunden verlagert. Wahrscheinlich erfolgt diese zeitliche Steuerung seitens der Angreifer mit Absicht, damit möglichst viele Spamnachrichten während der normalen Arbeitszeit direkt geöffnet werden.

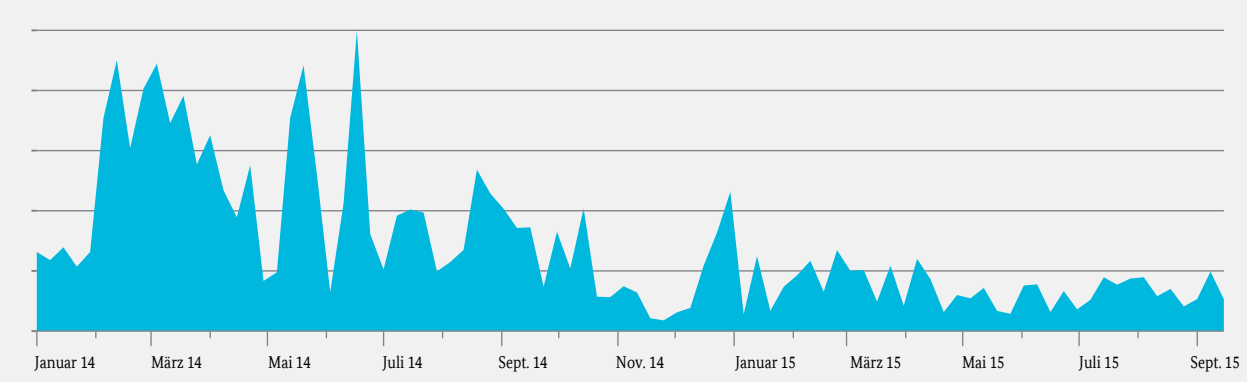

Abbildung 7: Spamverlauf pro Woche in Deutschland seit 1.1.2014

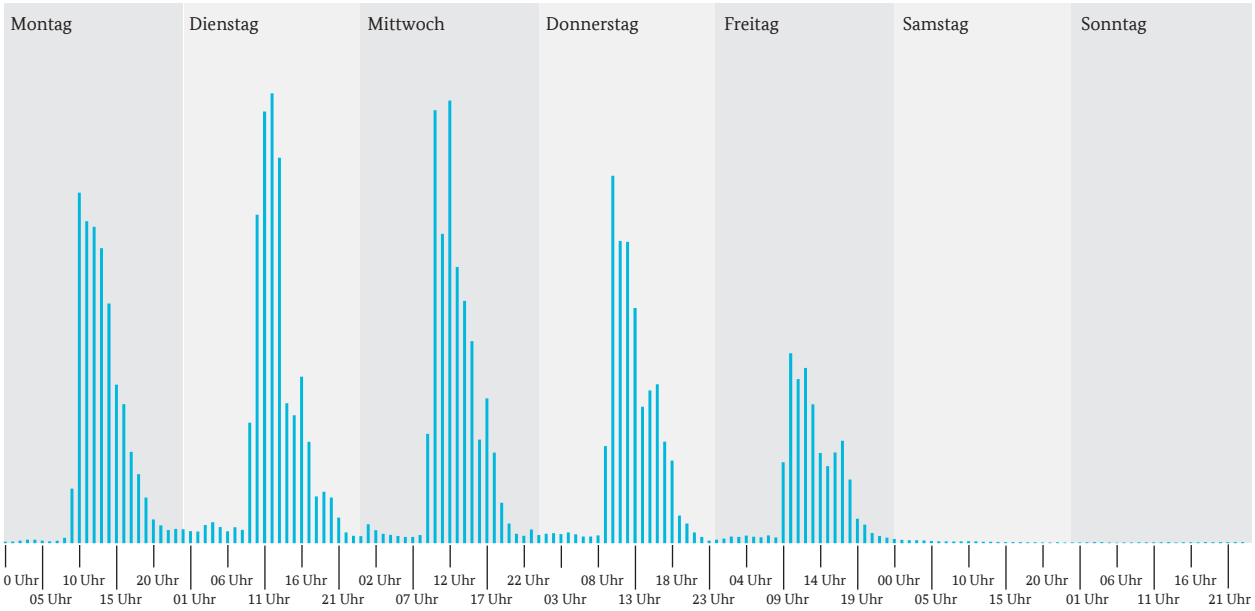

Abbildung 8: Verteilung des Versands von Schadsoftware-Spam auf die Wochentage seit Anfang 2015

Bewertung

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. Fortgeschrittene Verschleierungstechniken, individuelle Varianten bei den versendeten 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.

Klassischer Spam hat heute kaum noch Auswirkungen auf die Verfügbarkeit der Mail-Systeme. Schadsoftware-Spam ist weiterhin eine der Hauptquellen von Infektionen. Als Gegenmaßnahme ist vor allem der aufmerksame Benutzer gefordert, der mit gesundem Misstrauen E-Mails bearbeitet, die von unbekannten Absendern stammen oder bei denen etwas nicht in Ordnung zu sein scheint. Eine gute technische Gegenmaßnahme bietet das sogenannte Whitelisting von Verzeichnissen, aus denen ausführbare Dateien gestartet werden dürfen.

Gefährdung 2015

2.2.5 Botnetze

Einleitung

Als Botnetz wird ein Verbund von Systemen bezeichnet, die von einem fernsteuerbaren Schadprogramm befallen sind. Dies können Computersysteme, aber auch mobile Geräte wie beispielsweise Smartphones oder Tablet-Computer sein. Aufgrund ihrer hohen Verfügbarkeit und breitbandigen Anbindung werden zunehmend auch Webserver kompromittiert oder gezielt über Cloud-Dienste angemietet. Aus Internetroutern bestehende Botnetze verdeutlichen, dass jedes internetfähige System zum Teil eines Botnetzes werden kann.

Alle befallenen Systeme einer speziellen Schadprogrammvariante werden von einer bzw. mehreren übergeordneten Einheiten gesteuert, die vom Botnetz-Betreiber kontrolliert werden. In vielen Fällen handelt es sich dabei um Server, die auch als Command-and-Control-Server (C&C-Server) bezeichnet werden.

Lage

- Im Berichtszeitraum wurden zwei Botnetze abgeschaltet, die auch in Deutschland aktiv waren. Das Dropperbot-Botnetz bestand aus circa 11.000 Bots und wurde im Dezember 2014 deaktiviert; das Ramnit-Botnetz mit weltweit circa 3,2 Millionen Infektionen im Februar 2015. Betroffene Nutzer wurden durch die Internetprovider und das BSI informiert.

- In der ersten Jahreshälfte 2015 wurden von Sicherheitsforschern täglich bis zu 60.000 Infektionen deutscher Systeme registriert und über das BSI an die deutschen Internetanbieter gemeldet. Diese informieren ihre Kunden, einige bieten auch Unterstützung bei der Bereinigung.

- Aufgrund des hohen Marktanteils sind überwiegend Windows-Systeme von Bot-Infektionen betroffen. Aber auch Mac OS X und Android-Geräte rücken zunehmend in den Fokus der Cyber-Kriminellen. Weiterhin hält der Trend an, kompromittierte Webserver zum Betrieb von C&C-Servern zu missbrauchen.

- Es ist davon auszugehen, dass im Tagesdurchschnitt mehrere Hundert C&C-Server in Deutschland aktiv sind. Aufgrund von Gegenmaßnahmen durch die Betreiber ist eine hohe Fluktuation der Systeme zu beobachten.

Bewertung

Botnetze werden von Kriminellen im großen Stil zum Informationsdiebstahl, Online-Banking-Betrug, für Angriffe auf die Verfügbarkeit von Computersystemen sowie zum Versand von Spam genutzt. Aktuelle Schadprogramme sind aufgrund ihrer Nachladefunktionalität flexibel einsetzbar. Botnetz-Infrastrukturen bieten Internetkriminellen 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 weiterhin kritisch und tendenziell steigend. Dies resultiert einerseits aus der Vielzahl verwundbarer Internetsysteme, die als potenzielle Bots verwendet werden können, sowie andererseits der niedrigen Einstiegshürde für Cyber-Kriminelle.

Gefährdung 2015

2.2.6 Distributed Denial-of-Service (DDoS)-Angriffe

Einleitung

Denial-of-Service (DoS)- oder Distributed Denial-of-Service (DDoS)-Angriffe werden von Angreifern durchgeführt, deren Motivation hauptsächlich im Bereich der Erpressung, aber auch im Bereich des Hacktivismus liegt. Die Angriffe auf die Verfügbarkeit von Diensten oder Systemen können den Opfern unmittelbaren Schaden zufügen, etwa dadurch, dass geschäftskritische Prozesse nicht mehr funktionieren oder Dienstleistungen nicht mehr angeboten werden können. DDoS-Angriffe oder die Drohung damit können das Opfer aber auch dazu bewegen, auf bestimmte Forderungen der Angreifer einzugehen.

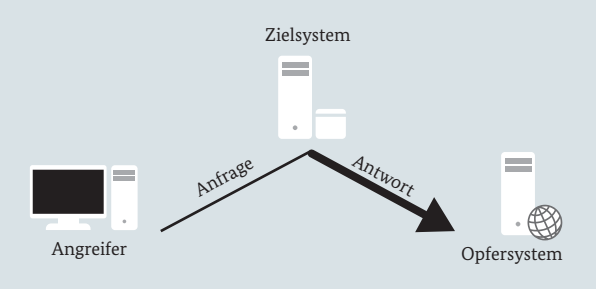

Abbildung 9: Illustration eines Reflection-Angriffs

Eine verbreitete Angriffsart sind Reflection-Angriffe. Hierbei werden öffentlich erreichbare Server (z. B. NTP-Server) missbraucht, um einen Angriff zu verstärken. Die Betreiber solcher Server werden somit ungewollt zu Mittätern. Bei dieser Art von Angriff lässt sich mit wesentlich weniger

Systemen eine vergleichbare Wirkung wie bei einem Angriff über ein klassisches Botnetz erzielen.

Lage

- Immer wieder sind Webangebote aufgrund von DDoS-Angriffen nicht erreichbar. Auch Webseiten innerhalb der Bundesverwaltung werden gelegentlich zum Ziel von Angriffen.
- Im ersten Halbjahr 2015 wurden 29.437 Angriffe in Deutschland registriert. Im ersten Halbjahr 2014 waren es 25.113 Angriffe. Das entspricht einem Zuwachs von etwa 17 Prozent. Gleichzeitig ist in Deutschland die durchschnittliche Angriffsbandbreite von 1,315 auf 1,435 Gbps, die durchschnittliche Paketrate der Angriffe von 469,889 auf 665,691 Kpps (42 Prozent) gestiegen. Diese Steigerung ist durch die stark erhöhte durchschnittliche Paketrate im zweiten Quartal 2015 bedingt. Hier lag sie bei rund 919 Kpps - im Vergleich zu etwa 486 Kpps im ersten Quartal 2015.
- Die in 2013 und Anfang 2014 beobachteten Reflection-Angriffe über NTP haben im Verlauf des Jahres 2014 anteilig abgenommen, während Reflection-Angriffe über SSDP (Simple Service Discovery Protocol) zugenommen haben. Insgesamt hat der Anteil der Reflection-Angriffe an der Menge der DDoS-Angriffe zugenommen. Bei dieser Art von Angriff sind wesentlich weniger Systeme notwendig als bei einem Angriff über ein klassisches Botnetz, um eine vergleichbare Wirkung zu erzielen.

Bewertung

- Deutschland ist weder als Quelle noch als Ziel von Angriffen besonders auffällig. Auffällig ist jedoch die im zweiten Quartal 2015 stark angestiegene durchschnittliche Paketrate bei Angriffen. Die durchschnittliche Paketrate ist damit nach einem „ruhigen" Jahr 2014 wieder auf einem zu 2013 vergleichbaren Wert angelangt. Bei Angriffen mit hohen Paketraten können vorgelagerte Komponenten wie Load-Balancer oder Firewalls zum Flaschenhals werden.
- Deutschland ist weiterhin noch in den Top10 der Länder mit den meisten offenen NTP-Servern vertreten. Da die Zahl der offenen NTP-Server in Deutschland rückläufig ist, werden Angreifer auf andere Protokolle – etwa SSDP – ausweichen, sodass die Gesamtsituation weitestgehend unverändert bleiben wird.

Gefährdung 2015

DDoS-Angriffe auf Webseiten der Bundesregierung und des Deutschen Bundestages

Sachverhalt: Am Mittwoch, den 7. Januar 2015 konnten die Webseiten www.bundeskanzlerin.de, www.bundesregierung.de und www.bundestag.de ab ca. 10:00 Uhr nicht mehr aufgerufen werden. Der Ausfall wurde initial im Lagezentrum des BSI festgestellt. Ab etwa 14:00 Uhr war auch die Webseite des Auswärtigen Amtes www.auswaertiges-amt.de zeitweise nicht zu erreichen.

Ursache: Auslösendes Moment war ein DDoS-Angriff, zu dem sich die politisch motivierte Gruppierung „CyberBerkut" bekannte. Als Anlass für den Angriff nannte die Gruppe in einem Bekennerschreiben den in diesem Zeitraum stattfindenden Besuch des ukrainischen Ministerpräsidenten Arseni Jazenjuk in Deutschland. Ob die Gruppe tatsächlich hinter dem Angriff steckt, ist nicht bekannt.

Methode: Bei dem Angriff handelte es sich um verschiedene, vom Angreifer variierte DDoS-Angriffsformen, darunter TCP SYN-Flood, UDP Reflection sowie Angriffe auf Ebene der Webanwendung, mit einer signifikanten Bandbreite, die die Internetanbindung überlastete. Zeitweilig waren an dem Angriff Tausende weltweit verteilter Botnetz-Clients beteiligt.

Schadenswirkung: Mithilfe von Filterregeln und der Anbindung an eine dedizierte Internetleitung wurde die Verfügbarkeit der Webseite www.bundeskanzlerin.de kurzzeitig wiederhergestellt. Der Angriff weitete sich im Verlauf auf die Webseite des Deutschen Bundestages www.bundestag.de aus, ab ca. 18:00 Uhr war auch die Webseite www.bundesregierung.de beeinträchtigt. Der DDoS-Angriff setzte sich über Nacht fort, zeigte aber infolge der eingeleiteten Gegenmaßnahmen keine nach außen sichtbaren Auswirkungen mehr. Der DDoS-Angriff dauerte bis weit in den nächsten Tag. Andere Webseiten der Bundesverwaltung waren von dem Angriff nicht betroffen.

Zielgruppen: Die reklamierte Urheberschaft des Angriffs sowie der zeitliche Zusammenhang mit politischen Gesprächen in Berlin untermauern, dass dieser DDoS-Angriff explizit gegen die Bundesregierung gerichtet war.

Technische Fähigkeiten: Im Gegensatz zu anderen, regelmäßig stattfindenden DDoS-Angriffen mit geringen Auswirkungen zeigten die Angreifer in diesem Fall fortgeschrittene technische Fähigkeiten. Dazu zählt insbesondere die sofortige Reaktion auf eingeleitete Gegenmaßnahmen. Sobald ein Angriffsvektor durch einen Filter geschlossen wurde, schwenkten die Angreifer auf einen neuen Vektor um.

2.2.7 Drive-by-Exploits und Exploit-Kits

Einleitung

Drive-by-Exploits sind ein tückisches Angriffsmittel, da sie ohne Zutun des Internetnutzers funktionieren. Um Schwachstellen im Webbrowser, in Browser-Plug-ins oder im Betriebssystem auszunutzen und Schadprogramme zu installieren, reicht es aus, eine entsprechend präparierte Webseite aufzurufen. Drive-by-Exploits werden einzeln oder gesammelt in sogenannten Exploit-Kits verwendet. Die Verbreitung erfolgt oftmals über manipulierte Werbebanner oder kompromittierte Webserver. Drive-by-Exploits oder Exploit-Kits, die in eine populäre, hochfrequentierte Webseite eingebunden sind, können in kürzester Zeit eine große Zahl verwundbarer Systeme mit Schadprogrammen infizieren. 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

- Drive-by-Exploits und Exploit-Kits kommen aktuell nicht nur auf dubiosen Webangeboten vor, sondern häufig auch auf unverdächtigen, legitimen Webseiten. Die Auswertung der Webseiten-Indexierung durch Google[16] zeigt, dass 2015 zwischen einem und zwei Prozent aller Webseiten in Deutschland Drive-by-Angriffe ausführen oder darauf verweisen. Im Juli 2015 konnte eine Angriffskampagne mittels eines Exploit-Kits gestoppt werden, von der ca. 5.000 Webseiten allein in Deutschland betroffen waren.
- Schädliche Werbebanner sind eine wesentliche Infektionsquelle, da die Werbebanner von Dritten bereitgestellt und in viele Seiten eingebunden werden. Die Einblendung der manipulierten Werbebanner reicht aus, um den Angriff zu starten. Sowohl große als auch kleine Werbenetzwerke waren 2015 Ausgangspunkt von Angriffen über Werbebanner.
- 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. 2015 wurde diese Methode durch die Kompromittierung der Webseite des Präsidenten von Myanmar eingesetzt, um Organisationen mit politischen oder geschäftlichen Beziehungen zu Myanmar anzugreifen[17].
- Gezielte Angriffe per Drive-by-Exploit erfolgen des Weiteren durch auf den Empfänger und dessen Tätigkeits- oder Interessengebiet zugeschnittene E-Mails, die Links auf präparierte Webseiten enthalten. Eine Tätergruppe setzte diese Methode der Link-Verteilung per E-Mail im Juni 2015 etwa gegen Unternehmen mehrerer Branchen wie Luft- und Raumfahrt, Rüstungsindustrie, Telekommunikation oder Logistik ein[18].
- Seit Anfang 2015 wurden die neuen Schwachstellen in Abbildung 10 erstmalig in Drive-by-Angriffen verwendet oder in Exploit-Kits integriert. Angriffsziel waren hauptsächlich neue Schwachstellen im Adobe Flash Player.

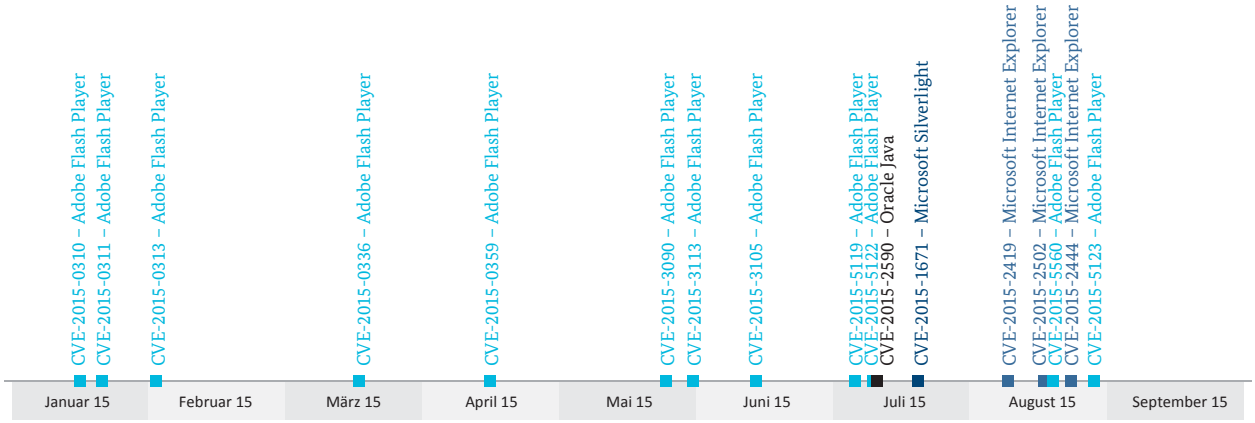

Abbildung 10: Ausnutzung neuer Schwachstellen in Drive-by-Angriffen und Exploit-Kits in 2015

[16] https://www.google.com/transparencyreport/safebrowsing/malware/?hl=de

[17] http://researchcenter.paloaltonetworks.com/2015/06/evilgrab-delivered-by-watering-hole-attack-on-president-of-myanmars-website

[18] https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html

- Im Vergleich zu 2014 hat sich die Lage im Bereich der Exploit-Kits geändert: Hauptangriffsziel 2015 ist der Adobe Flash Player. Allein im ersten Halbjahr 2015 wurden acht neue Exploits gegen Schwachstellen im Adobe Flash Player in Exploit-Kits integriert bzw. in einem Fall durch einen einzelnen Drive-by-Exploit genutzt. Bei fünf dieser Exploits handelte es sich um 0-Day-Schwachstellen, die vor Bereitstellung eines Sicherheitsupdates durch den Hersteller aktiv für Angriffe genutzt wurden. Auch die weiteren Exploits wurden zum Teil bereits wenige Tage nach Bereitstellung eines Sicherheitsupdates in Exploit-Kits integriert.
- Die Schadsoftware, die nach einem Angriff installiert wird, variiert und kann jederzeit angepasst werden. In ungezielten Angriffskampagnen wurden Opfer unter anderem mit verschiedenen Ransomware-Varianten wie CryptoWall 3.0 oder TeslaCrypt/AlphaCrypt, Schadsoftware zum Klickbetrug wie Kovter oder Bedep sowie generischen Droppern wie Pony Loader infiziert.

Bewertung

Im Vergleich zum Vorjahr hat sich die Bedrohungslage durch Drive-by-Exploits und vor allem durch Exploit-Kits verschärft: Neue Schwachstellen sowie 0-Day-Schwachstellen werden regelmäßig und binnen kürzester Zeit in Exploit-Kits integriert. Die aktuelle Lage zeigt, dass in neue Exploits und die Suche nach unbekannten Schwachstellen investiert wird, um das Potenzial von Drive-by-Exploit-Angriffen auszuschöpfen. Neben dem sofortigen Einspielen von Sicherheitsupdates kann auch die zumindest temporäre Deaktivierung betroffener Programme oder Plugins notwendig sein, um sich vor diesen Angriffen zu schützen.

Gefährdung 2015

Tausende Webseiten leiten Nutzer auf Exploit-Kit

Sachverhalt: Im Juli 2015 konnte eine Angriffskampagne mittels des Exploit-Kits „Angler“ durch Zusammenarbeit der internationalen CERT-Community gestoppt werden, von der allein in Deutschland rund 5.000 Webseiten betroffen waren.

Methode: Für den Angriff wurden mehr als 150.000 Webseiten weltweit kompromittiert. Hauptsächlich waren Webseiten betroffen, die das Contentmanagementsystem WordPress einsetzen. Die Angreifer manipulierten die Seiten, sodass Besucher der Webseiten im Hintergrund auf das Exploit-Kit umgeleitet wurden. Das Exploit-Kit versuchte im Anschluss, mittels unterschiedlicher Exploits Schwachstellen auf dem PC der Webseitenbesucher zur Installation von Schadsoftware auszunutzen.

Schadenswirkung: Allein in Deutschland wurden ca. 5.000 Webseiten kompromittiert. Durch den Angriff wurden weltweit 68 Millionen Seitenaufrufe von vier Millionen IP-Adressen auf das Exploit-Kit umgeleitet. Knapp fünf Prozent der Seitenaufrufe kamen aus Deutschland. Nach einem erfolgreichen Angriff wurden die Opfersysteme mit der Ransomware Cryptowall infiziert, um Lösegelder zu erpressen. Der Anteil tatsächlich erfolgreicher Angriffe und damit verbundener Schadsoftware-Infektionen ist nicht bekannt. Da Exploit-Kits jedoch seit Anfang 2015 vermehrt Zero-Day-Schwachstellen oder Schwachstellen im unmittelbaren Anschluss an die Veröffentlichung eines Sicherheitsupdates im Adobe Flash Player ausnutzen, ist von einer hohen Anzahl erfolgreicher Angriffe auszugehen.

Zielgruppen: Angriffe mittels Exploit-Kits sind ungezielt. Betroffen sind häufig private Anwender, aber auch Unternehmen, deren Systeme nicht auf dem aktuellen Stand an Sicherheitsupdates sind.

Technische Fähigkeiten: Bei diesem Angriff wurden keine besonderen technischen Fähigkeiten angewandt. Vielmehr sind Angriffe mittels Exploit-Kits und kriminellem Hintergrund heute Alltag. Die Masse an im Vorfeld kompromittierten Webseiten und die Vielzahl der umgeleiteten Nutzer zeigen das Potenzial eines solchen Angriffs.

2.2.8 Identitätsdiebstahl

Einleitung

Die Identität einer natürlichen Person wird durch eine Vielzahl unterschiedlicher Merkmale definiert, beispielsweise durch Name, Geburtsdatum, Adresse, Sozialversicherungsnummer oder Steuernummer. Im Kontext des Internets wird die Identität vielfach auf Identifikations- und Authentisierungsdaten eingeschränkt, meist auf die Kombination aus Nutzername und Passwort, Bank- oder Kreditkarteninformationen und E-Mail-Adressen. Verschafft sich ein Unberechtigter Zugang zu solchen Daten, so hat sich hierfür der Begriff „Identitätsdiebstahl" eingebürgert. Identitätsdiebstahl erfolgt vor allem mittels Social Engineering, durch die Installation von Schadprogrammen auf Endgeräten oder durch Datenabfluss nach dem Angriff auf Online-Angebote. Meist hat ein Angreifer kein Interesse an der Übernahme der reellen Identität der natürlichen Person, sondern nutzt diese Daten zum eigenen Vorteil, beispielsweise zur Realisierung von Gewinnabsichten. Nutzt ein Angreifer gestohlene digitale Identitäten, so bezeichnet man dies als Identitätsmissbrauch. In der Regel läuft dies arbeitsteilig ab: Während die digitalen Identitäten von dem einen Kriminellen gestohlen werden, missbraucht sie ein anderer für seine kriminellen Zwecke. Es existiert mittlerweile ein reger Onlinehandel mit digitalen Identitäten.

Lage

- Dem BSI sind durchgehend ca. 100.000 Infektionen durch mehrere Schadprogrammfamilien mit Identitätsdiebstahlfunktion in Deutschland bekannt. Es ist davon auszugehen, dass die Gesamtzahl der Infektionen durch diese Schadprogrammfamilien noch erheblich höher liegt, da mit der verwendeten Messmethode wahrscheinlich nur ein Bruchteil der Infektionen detektiert wird.

- Über die in der obigen Zählung erfassten Schadprogrammfamilien hinaus existieren noch weit mehr Schadprogramme mit Identitätsdiebstahlfunktion: Von Dezember 2014 bis September 2015 hat das BSI rund 168.000 neue Schadprogramme analysiert, die einen Bezug zum Identitätsdiebstahl in Deutschland aufweisen.

- Im Jahresverlauf ist in Deutschland nur ein Einbruch auf Server öffentlich bekannt geworden, der dem Diebstahl von Nutzernamen und Passwörtern diente. Auch international sind 2015 keine nennenswerten Passwortdiebstähle von Servern an die Öffentlichkeit gelangt. Es ist jedoch davon auszugehen, dass hier eine hohe Dunkelziffer existiert, denn ein betroffener Betreiber hat in der Regel kein Interesse daran, dass ein erfolgreicher Angriff öffentlich bekannt wird. In einigen Fällen wird zudem ein Angriff vom Betreiber möglicherweise nicht bemerkt. Schon ein einzelner erfolgreicher Angriff kann dabei in den Millionenbereich gehen: Aus der weiteren Vergangenheit ist bekannt, dass wesentlich mehr Identitäten von Servern als von Endgeräten gestohlen werden.

- Zum Missbrauch digitaler Identitäten sind nicht nur Nutzernamen und Passwörter geeignet, sondern auch andere gestohlene personenbezogene Daten. Im Berichtszeitraum sind als herausragende Beispiele für solche Angriffe eine Cyber-Attacke auf die Personaldatenverwaltung der US-Regierung, bei der personenbezogene Daten von 21,5 Mio. Regierungsangestellten oder Bewerbern[19] abgeflossen sind, sowie ein Angriff auf die US-Steuerbehörde bekannt geworden, bei dem mithilfe von entwendeten Steuerzahlerdaten 39 Mio. US-Dollar (Ermittlungsstand: Juli 2015) erbeutet werden konnten[20].

- Da bezüglich der Diebstahlszahlen eine hohe Dunkelziffer existiert, lässt sich der durch Identitätsmissbrauch entstandene Schaden nicht seriös beziffern.

Bewertung

Durch den Verkauf von gestohlenen Identitäten können Angreifer einen direkten monetären Gewinn erzielen. Da die Installation von Schadprogrammen demgegenüber mit relativ geringem Aufwand und Kosten zu bewerkstelligen ist, ergeben sich mitunter hohe Gewinnspannen. Deshalb ist davon auszugehen, dass der Diebstahl von Identitätsdaten gleich welcher Art auf dem aktuell hohen Niveau verbleibt.

Gefährdung 2015

[19] https://www.opm.gov/cybersecurity
[20] http://www.irs.gov/uac/Written-Testimony-of-Commissioner-Koskinen-on-Unauthorized-Attempts-to-Access-Taxpayer-Data-before-Senate-Finance-Committee

2.3 Cyber-Angriffe: Motivation und Ziele

Nachrichtendienste, Cyber-Kriminelle und Hacktivisten haben einen maßgeblichen Einfluss auf die technische Cyber-Sicherheit. Ihre Motive sind sehr unterschiedlich und können geostrategische, politisch-ideologische, religiös-ideologische, nachrichtendienstliche, wirtschaftliche oder destruktive Ziele verfolgen.

2.3.1 Nachrichtendienstliche Cyber-Angriffe

Viele Staaten haben mittlerweile das Potenzial von Cyber-Angriffen erkannt. Deutschland ist permanent Cyber-Angriffen ausgesetzt, die darauf zielen, informative und finanzielle Vorteile zu erlangen. Durch die kontinuierlich verbesserte Sensorik des BSI in den Regierungsnetzen, den Austausch von Erkenntnissen im Cyber-Abwehrzentrum mit anderen Behörden sowie weitere Veröffentlichungen aus dem Dokumentenfundus von Edward Snowden und durch Wikileaks haben sich die Zahl der konkreten Detektionen, die technischen Erkenntnisse und das allgemeine Wissen des BSI über nachrichtendienstliche Cyber-Angriffe sowie Cyber-Angriffsmethoden seit dem letzten Lagebericht von Dezember 2014 erneut erweitert.

Im Zeitraum 2014/2015 sind unter den international detektierten Cyber-Angriffen, die einen nachrichtendienstlichen Hintergrund vermuten lassen, vor allem die Angriffe unter der Bezeichnung „APT28“[21] und die Spionage-Software Regin[22] zu nennen. Mit erweiterten Detektionsmöglichkeiten in der Bundesverwaltung gemäß §5 des IT-Sicherheitsgesetzes (IT-SiG) sowie durch das zukünftige Meldungsaufkommen aus den Unternehmen der Kritischen Infrastrukturen gemäß §8b IT-SiG wird das BSI in den kommenden zwei Jahren seine Fähigkeiten erneut ausbauen und damit zu einer verbesserten Aussage über die Cyber-Sicherheitslage auch mit Bezug auf nachrichtendienstliche Angriffe im deutschen Cyber-Raum gelangen.

Die Analyse der oben genannten neuen Erkenntnisse des BSI zu nachrichtendienstlichen Angriffen bestätigt und vertieft die im Jahresbericht 2014 getroffenen Aussagen zu den vier Hauptangriffsvektoren von Nachrichtendiensten:

1. Angriffsvektor Strategische Aufklärung: An Internet- und Kommunikationsknotenpunkten können alle anfallenden Daten abgegriffen, gespeichert und analysiert werden. Hierbei sind insbesondere die (Verkehrs-)Daten beliebiger Internetnutzer betroffen. Unverschlüsselte Inhalte können mitgehört oder -gelesen werden. Alle diese Prozesse geschehen in der Regel vollautomatisch und sind in der Lage, sehr große Datenmengen zu verarbeiten.

2. Angriffsvektor Individuelle Angriffe im Kommunikations- und Cyber-Raum: Diese Angriffe zielen auf IT-Systeme interessanter Personen und Institutionen. In der strategischen Aufklärung identifizierte IT-Systeme werden mithilfe vorab gesammelter technischer, aber auch sozialer Informationen über den Nutzer mit spezifisch adaptierten Cyber-Angriffen attackiert und kontrolliert. Nutzt etwa die Zielperson mobile IT im Sinne eines „always on“, so kann über die vom IT-System übermittelten Standortdaten auch der Aufenthaltsort des Geräteinhabers permanent verfolgt werden.

3. Angriffsvektor Beeinflussung von Standards und Implementierungen: Hierbei werden bereits im Vorfeld der technischen Aufklärung IT-Standards und vor allem kryptografische Standards manipuliert. Die Implementierungen an sich starker Sicherheitsmechanismen und die hiermit verbundene Vertraulichkeit werden so systematisch geschwächt und bieten damit keinen ausreichenden Schutz der Vertraulichkeit mehr.

4. Angriffsvektor Gezielte Manipulation von IT-Equipment: Hierbei erfolgen Eingriffe in Bestell-, Liefer- oder Serviceketten, um Manipulationen durchzuführen. Hierzu zählen beispielsweise das Einbringen von Hintertüren oder die Schwächung technischer Sicherheitseigenschaften, die dann auch wieder im Rahmen der oben dargestellten strategischen Aufklärung oder bei individuellen Angriffen ausgebeutet werden können.

Nachrichtendienstliche Cyber-Angriffe gehören wie APT-Angriffe generell zu den Cyber-Attacken, die am schwersten einem Angreifer zugeordnet werden können. Gerade diese Angriffe nutzen perfekte Tarnungsmethoden, um sowohl die Angriffswege (und damit den Urheber) als auch den Angriff im betroffenen IT-System selbst zu verschleiern. Das BSI sieht es angesichts des rasanten Trends zu immer hochwertigeren Angriffsmethoden als eine der zentralen Aufgaben der kommenden Jahre an, gemeinsam mit anderen Behörden und IT-Forensikfirmen seine technischen Analysemethoden weiterzuentwickeln, um Cyber-Angriffe qualifiziert zu detektieren und zu attribuieren. Alle dargestellten Möglichkeiten, IKT-Systeme zum Zwecke von technischer oder

[21] https://www2.fireeye.com/apt28.html
[22] http://www.symantec.com/connect/blogs/regin-top-tier-espionage-tool-enables-stealthy-surveillance

Cyber-Spionage zu kompromittieren, können auch in gleicher oder ähnlicher Weise genutzt werden, um Cyber-Sabotage zu verüben. Dies trifft in besonderem Maße auf die in Kritischen Infrastrukturen eingesetzte Informations- und Kommunikationstechnik zu, wie insbesondere der ebenfalls dem Typus APT28 zuzuordnende Cyber-Angriff auf den französischen Fernsehsender TV5MONDE belegt.

2.3.2 Cyber-Kriminalität

Ein Nebeneffekt der Veröffentlichungen von Edward Snowden sind die zum Teil sehr detaillierten Informationen über Angriffsziele, -wege, -werkzeuge und -methoden, die zu einer Proliferation, d.h. Weiterverbreitung dieses Know-hows und damit zur Blaupause für neue Angreifer etwa auch in der cyberkriminellen Szene werden können. Die Methoden Cyber-Krimineller orientieren sich sowohl am technischen Fortschritt als auch an den bestehenden Abwehrmaßnahmen. Die Angreifer nutzen dabei die gesamte Bandbreite der technischen Möglichkeiten aus: Bei Privatanwendern sind das Spam- und Phishing-Mails, Schadsoftware zum Identitätsdiebstahl oder Manipulation von Onlinebanking sowie der Einsatz von Ransomware. Unternehmen werden mit unterschiedlichen Formen der Erpressung, dem Hacking von Serverdiensten oder Schadprogrammen für Kassensysteme (Point of Sale, POS) konfrontiert.

Die Teilnehmer der Cyber-Sicherheitsumfrage 2015[23] der Allianz für Cyber-Sicherheit benennen weiterhin Organisierte Kriminalität und Wirtschaftskriminalität als Angreifergruppe mit dem höchsten Bedrohungspotenzial in den kommenden Jahren.

Der bestehende Markt, auf dem die Schwachstellen, Angriffsmethoden oder die Durchführung von Cyber-Angriffen offeriert werden, sorgt dafür, dass die Gefährdungslage unübersichtlicher wird. So bieten Organisationen ihre Fähigkeiten und Leistungen auch anderen interessierten Kreisen im Rahmen von Auftragsarbeiten an („Cybercrime-as-a-Service"). Damit werden hochwertige Angriffe auch für Organisationen und Staaten verfügbar, die diese Expertise bisher nicht eigenständig bzw. aufgrund mangelnder Fähigkeiten grundsätzlich nicht aufbauen können.

Angriff auf die Firma Hacking Team

Im Juli 2015 wurde nach einem Cyber-Angriff eine Vielzahl interner Dokumente der italienischen Firma Hacking Team veröffentlicht. Die Firma verkauft nach eigenen Angaben Angriffswerkzeuge und Überwachungstechnik an Strafverfolgungsbehörden und Regierungseinrichtungen weltweit. Durch die Veröffentlichungen wurden mehrere bisher unbekannte Schwachstellen in weitverbreiteten Anwendungen aufgedeckt, die die Firma eingekauft oder selbst entwickelt hat. Mit der Veröffentlichung der vor den Herstellern zurückgehaltenen Schwachstellen stieg die Gefährdung der betroffenen Anwender, da die Schwachstellen bereits kurz nach der Veröffentlichung sowohl von APT-Gruppen als auch von Cyber-Kriminellen übernommen und in eigenen Angriffskampagnen ausgenutzt wurden.

Die Veröffentlichungen belegen, dass es heute einen aktiven und finanziell lukrativen Markt für Cyber-Angriffsmittel und Schwachstellen gibt. Der Vorfall verdeutlicht zusätzlich, dass die Fähigkeiten zur Entwicklung von Exploits und Schadprogrammen und damit zur Durchführung von Cyber-Spionage nicht auf Nachrichtendienste beschränkt sind. Durch diesen Markt verschärft sich die Bedrohungslage, da die Fähigkeiten von Hacking Team oder vergleichbaren Firmen auch von Marktkonkurrenten oder Nachrichtendiensten, die selbst nicht über hinreichend IT-Know-how verfügen, eingekauft und entsprechend eingesetzt werden können.

[23] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Micro/Umfrage/umfrage2015.html

3 Gefährdungslage der Bundesverwaltung

3 Gefährdungslage der Bundesverwaltung

Das BSI-Lagezentrum ist seit 2010 zentrale Meldestelle für IT-Sicherheitsvorfälle in der Bundesverwaltung. Zusätzlich laufen im BSI-Lagezentrum die Erkenntnisse aus dem Schutz der Regierungsnetze zusammen. Das BSI kann so neben der unmittelbaren Reaktion auf einen Vorfall auch Trends und Entwicklungen im Hinblick auf die Bedrohungslage für die Informationstechnik und Netze der Bundesverwaltung ableiten und entsprechend frühzeitig Maßnahmen ergreifen.

3.1 Abwehr von Angriffen auf die Regierungsnetze

Auch 2015 sind die Netze der Bundesverwaltung kontinuierlich Cyber-Angriffen ausgesetzt. Darunter befinden sich sowohl ungezielte Massenangriffe als auch gezielte Angriffskampagnen. Um eine Kompromittierung von IT-Systemen und -Netzen zu verhindern bzw. schnell zu erkennen, kommt ein mehrstufiges Sicherheitsmodell zum Einsatz. Neben herkömmlichen Virenschutzprogrammen wirken angepasste Schutzmaßnahmen an unterschiedlichen Schnittstellen.

Im Bereich Abwehr unerwünschter E-Mails wurden in der ersten Jahreshälfte 2015 in den Regierungsnetzen durchschnittlich etwa 11.000 infizierte E-Mails pro Monat in Echtzeit abgefangen, bevor sie die Postfächer der Empfänger erreichten. Dazu werden kommerzielle Virenschutzprogramme eingesetzt und mit eigenen Signaturen ergänzt, die beispielsweise die tagesaktuelle Spamlage berücksichtigen. Die Anzahl der Detektionen schwankt in Abhängigkeit zur Spamlage und der Effektivität der Vorfilterung (Empfänger-Prüfung/Greylisting). Darüber hinaus werden pro Tag im Mittelwert 15 Angriffe auf die Regierungsnetze detektiert, die mit normalen Schutzmaßnahmen nicht zu erkennen gewesen wären. Durchschnittlich ein gezielter Angriff alle zwei Tage hatte einen nachrichtendienstlichen Hintergrund.

Eine weitere Schutzkomponente blockiert ausgehende Netzverbindungen auf infizierte Webseiten, die Schadprogramme verteilen, oder Verbindungsversuche von bereits aktiven Schadprogrammen zu Kontrollservern, die für die Steuerung und den Datenabfluss genutzt werden. Diese Maßnahme greift zum einen präventiv und erkennt zum anderen bereits infizierte Systeme, bei denen die eingesetzten kommerziellen IT-Sicherheitsprodukte nicht gegriffen haben. 2015 wurden mit dieser Methode bisher täglich rund 5.000 Verbindungsversuche zu Schadcodeservern blockiert. Bis September 2015 wurden bereits 152-mal aktive Schadprogramme detektiert, die kommerzielle Schutzsysteme unterlaufen haben.

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

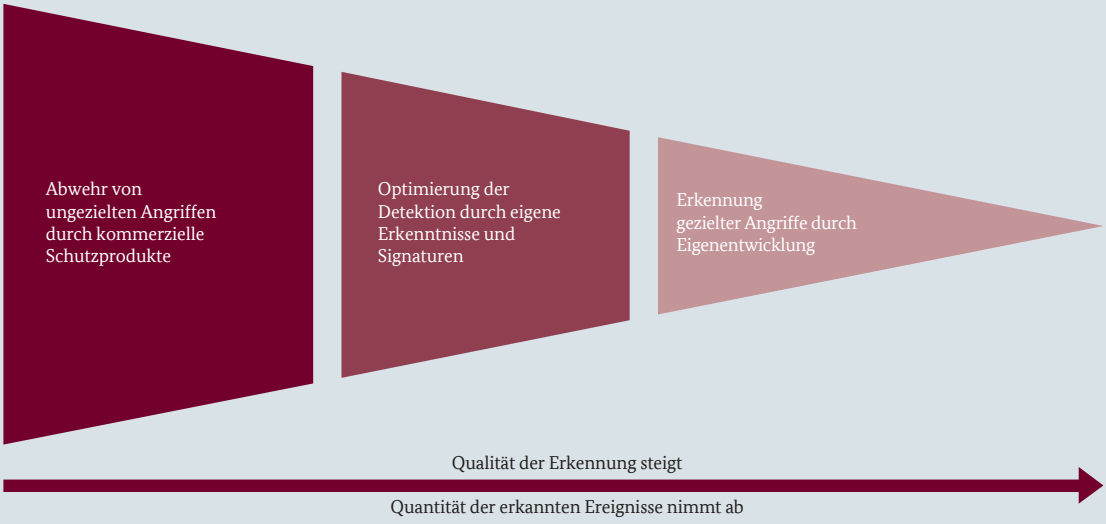

Abbildung 11: Gestufte Schutzmaßnahmen in den Regierungsnetzen gegen E-Mail-basierte Angriffe

Den größten Anteil daran hatten Kampagnen, die den Banking-Trojaner Feodo in gefälschten Rechnungsanhängen versandt haben. Dabei wird keine Schwachstelle ausgenutzt, sondern der Empfänger wird verleitet, die Schadsoftware eigenständig durch Öffnen des Anhangs auszuführen und so zu installieren.

3.2 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 September 2015 wurden von kommerziellen Schutzprodukten über 2.300 Schadsoftware-Infektionen in der Bundesverwaltung erkannt. Die Anzahl der erfolgreich abgewehrten Schadprogramme lag im selben Zeitraum bei knapp 500.000.

Das BSI verzeichnet durchschnittlich drei bis vier Mal im Monat einen Denial-of-Service (DoS)-Angriff auf einzelne Webseiten der Bundesbehörden. Dabei hat sich die Zahl der Angriffe, bei denen die jeweils betroffene Behörde unverzüglich um Unterstützung des BSI bittet, von zwei in 2013 auf 16 im Zeitraum Januar bis September 2015 erhöht.

Informationssicherheit in Behörden

IT-Sicherheitsüberprüfungen wie Revisionen, IT-Penetrationstests oder Web-Checks sind Teil des Beratungsmandats des BSI und erfolgen auf Anfrage einer Behörde. Das BSI beobachtet bei Überprüfungen regelmäßig grundlegende Sicherheitsmängel wie veraltete Patchstände von Betriebssystemen und Anwendungen. Hinzu kommen deaktivierte Sicherheitsmechanismen, fehlende Netzwerküberwachung und Netzwerkzugangskontrollen oder eine unzureichende und nicht verpflichtende Logdatenauswertung. Die fehlende Kontrolle von Schnittstellen sowie der Einsatz unverschlüsselter Mobilgeräte stellen bis heute Herausforderungen für IT-Sicherheitsverantwortliche dar. Auch unzureichende Schulungs- oder Sensibilisierungsmaßnahmen sowie unvollständige und inkonsistente Sicherheitskonzepte sowie unklare Verantwortlichkeiten für die Informationssicherheit bergen große Risiken. Die Informationssicherheit in Behörden kann aus Sicht des BSI signifikant verbessert werden, wenn sich das Personal in IT-Sicherheitsteams kontinuierlich mit den IT-Risiken und der zunehmenden Komplexität der Anwendungen auseinandersetzt. Dazu gehört eine angemessene personelle, technische und organisatorische Ausstattung, um die umfangreichen und dynamischen Aufgaben bewältigen zu können.

4 Schutz Kritischer Infrastrukturen: IT-Sicherheit für das Gemeinwohl

4 Schutz Kritischer Infrastrukturen: IT-Sicherheit für das Gemeinwohl

Strom, Wasser, Finanzen, Ernährung: Ein Ausfall oder eine Beeinträchtigung kritischer Versorgungsdienstleistungen hätte dramatische Folgen für Wirtschaft, Staat und Gesellschaft in Deutschland. Die Betriebsverantwortung für die Kritischen Infrastrukturen liegt bei den jeweiligen Betreibern, meist privatwirtschaftlichen Unternehmen. Aufgrund ihrer Bedeutung für das Gemeinwesen hat jedoch auch der Staat im Rahmen der Daseinsvorsorge eine Fürsorgepflicht gegenüber seinen Bürgern und somit die Gewährleistungsverantwortung für die Kritischen Infrastrukturen. Dem Staat und den Betreibern Kritischer Infrastrukturen kommt somit eine besondere Verantwortung zu, die Anlagen vor Ausfällen und Beeinträchtigungen zu schützen. Staat und KRITIS-Betreiber arbeiten schon seit einigen Jahren gemeinsam erfolgreich zum Schutz der Kritischen Infrastrukturen. Der Rahmen dieser Zusammenarbeit ist die öffentlich-private Kooperation UP KRITIS, die seit 2007 besteht. Der UP KRITIS ist seit Gründung stetig gewachsen und hat viele Maßnahmen zum Schutz Kritischer Infrastrukturen entwickelt und umgesetzt. Es hat sich jedoch gezeigt, dass gerade im Bereich der IT-Sicherheit der rein freiwillige Ansatz des UP KRITIS nicht ausreicht, um ein angemessenes IT-Sicherheitsniveau in allen KRITIS-Sektoren zu erzielen.

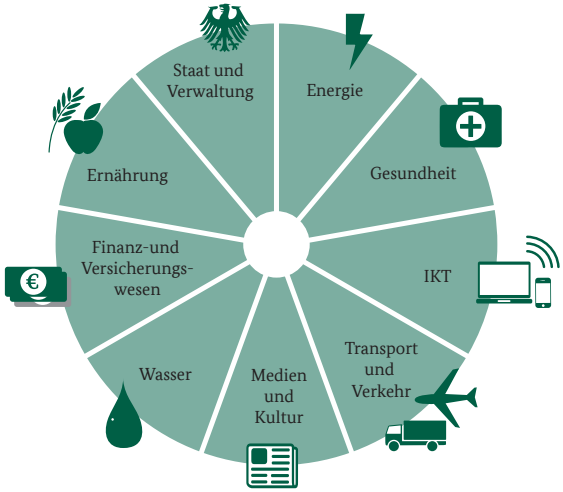

Abbildung 12: Sektoren Kritischer Infrastrukturen in Deutschland

Gezielte Angriffe auf die Infrastruktur von Finanzinstitutionen

Sachverhalt: Unter dem Namen Carbanak/Anunak wurden 2014 gezielte Cyber-Angriffe auf die internen Netzwerke verschiedener osteuropäischer Banken durchgeführt. Durch eine Veröffentlichung der Firma Kaspersky Labs[24] wurde dies im Februar 2015 publik.

Methode: Die Erstinfektionen der Rechner von Bankmitarbeitern erfolgten vermutlich über Spearphishing-E-Mails. Bei der Ausführung von Dateianhängen wurden die Systeme mit der Carbanak-Malware infiziert, einer auf dem Banking-Trojaner Caberp basierenden Schadsoftware. Nach der Infektion wurden die Spearphishing-E-Mails an weitere Empfänger aus dem Adressbuch der Opfer gesendet. Teilweise verleiteten die Angreifer ihre Opfer dazu, kompromittierte Webseiten aufzurufen, und infizierten deren Rechner mittels Drive-by-Exploits.

Schadenswirkung: Über die infizierten Systeme erlangten die Angreifer Zugriff auf das Bezahlsystem SWIFT, auf die Konten von Bankkunden und auf die Steuerungssysteme für Bankautomaten. In der Folge wurden Geldtransaktionen angestoßen und Auszahlungen von Bargeld an Bankautomaten ausgelöst. Vorhandene Betrugserkennungssysteme der Banken erkannten die Manipulation nicht, da sie auf die Aufdeckung von Betrug beim Endanwender ausgerichtet sind. Insgesamt wurden die Netzwerke von hunderten Opfern, darunter über 50 russische Banken, erfolgreich angegriffen. Zwei russischen Banken wurde infolgedessen die Lizenz entzogen. Die Schadenssumme wird auf ca. zwei Millionen US-Dollar pro Vorfall geschätzt. Schätzungen zufolge könnte durch Carbanak/Anunak weltweit ein Schaden von 500 Millionen bis einer Milliarde US-Dollar entstanden sein.

Zielgruppen: Finanzinstitute in Osteuropa, insbesondere in Ländern der ehemaligen Sowjetunion. Trotz anderslautender Berichte und einer groß angelegten Suche nach bekannten Vorfallsindikatoren wurden keine konkreten Fälle in Westeuropa und in den USA bekannt.

Technische Fähigkeiten: Der Aufwand für Planung und Recherche eines derartigen Angriffs in einer von Fachsystemen geprägten Umgebung ist hoch. Auch die gezielten Kompromittierungen von Zielsystemen im Netzwerk weisen auf starke technische Fähigkeiten hin, die bis dahin eher im nachrichtendienstlichen Kontext angesiedelt wurden. Die Anpassungsfähigkeit der Gruppe – verdeutlicht am Angriffsweg von Kundensystemen hin zu internen Transaktionssystemen der Banken und weiteren Bezahlsystemen – weist auf einen hohen Organisationsgrad und eine professionelle Kosten-Nutzen-Rechnung hin.

[24] https://securelist.com/blog/research/68732/the-great-bank-robbery-the-carbanak-apt/

4.1 Kritische Infrastrukturen hängen von funktionierender IT ab

Die fortschreitende Digitalisierung und Vernetzung betrifft auch den Bereich der Kritischen Infrastrukturen. Die Bereitstellung der kritischen Dienstleistungen hängt somit zunehmend vom Funktionieren der eingesetzten Informations- und Kommunikationstechnik (IKT) ab. Ein Ausfall oder eine Beeinträchtigung einer IKT-Komponente in den kritischen Prozessen der Betreiber kann unter Umständen eine Beeinträchtigung der Versorgungsdienstleistung zur Folge haben und im schlimmsten Fall zu einer vollständigen Unterbrechung der Versorgung führen. Durch Abhängigkeiten zwischen einzelnen Sektoren oder Branchen wird das Risiko von Ausfällen noch verstärkt. Ausfälle in einem Sektor können zu Ausfällen in anderen Sektoren führen und auf diese Weise einen Dominoeffekt auslösen.

- Verfügbarkeiten von Transport-, Lager- oder Umschlagskapazitäten wirken sich auf Logistikketten und somit auf die Verfügbarkeit von Waren oder Zulieferteilen in Handel und Industrie aus.
- Beeinträchtigungen der Telekommunikation wirken sich auf die komplexen Kommunikations- und Koordinierungsprozesse vieler Unternehmen und Kritischer Infrastrukturen aus.
- Ein Ausfall der Energieversorgung hätte für alle Wirtschafts- und Gesellschaftsbereiche erhebliche Auswirkungen.

Viele Branchen sind sich dieser Abhängigkeiten von Kritischen Infrastrukturen bewusst und gut aufgestellt. So werden oftmals Redundanzen für Versorgungsengpässe vorgehalten, Mitigationspläne erstellt oder es wird im Fall der Fälle auf Substitute zurückgegriffen. Oft spielen sich die Beeinträchtigungen daher im Bereich des Bewältigbaren ab. Nichtsdestoweniger schmälert jeder IT-Sicherheitsvorfall für einen gewissen Zeitraum die vorhandenen Sicherheitsmargen. Kenntnisse über IT-Sicherheitsvorfälle, die von den Betroffenen gewonnen werden können, sind ein wichtiger Baustein bei der Bewertung der IT-Sicherheitslage in den Kritischen Infrastrukturen. Frühwarnungen und Trendvorhersagen sind wichtige Instrumente, um die vorhandenen Sicherheitsmargen kurzzeitig für einen erwarteten Angriff erhöhen zu können.

4.2 Das IT-Sicherheitsgesetz

Bislang engagieren sich nicht alle KRITIS-Sektoren gleich stark im UP KRITIS. Gleichzeitig ist das IT-Sicherheitsniveau der KRITIS-Betreiber sehr uneinheitlich. Einige Betreiber sind in Bezug auf ihre IT-Sicherheit sehr gut aufgestellt und investieren viel in die Effektivität ihrer Maßnahmen. Andere Betreiber haben hier noch Nachholbedarf. Angesichts der besonderen Verantwortung der KRITIS-Betreiber für das Gemeinwohl und angesichts der weitreichenden gesellschaftlichen Folgen, die ein Ausfall oder eine Beeinträchtigung der Kritischen Infrastrukturen haben kann, ist im Juli 2015 das „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ (IT-Sicherheitsgesetz) in Kraft getreten. Derzeit wird an ei-

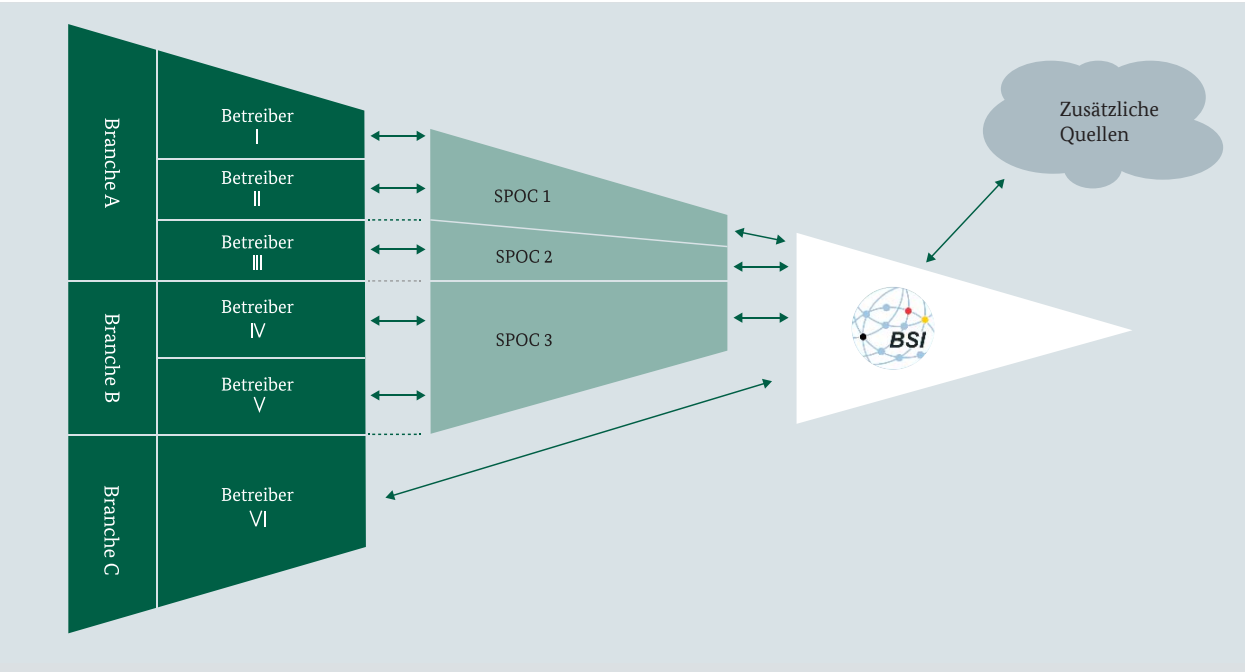

Abbildung 13: Kommunikationsstruktur im UP KRITIS

ner Verordnung gearbeitet, mit der unter anderem die unter das Gesetz fallenden KRITIS-Betreiber konkret identifiziert werden.

Ziel des Gesetzes ist es unter anderem, die IT-Sicherheit von Unternehmen, insbesondere von Betreibern Kritischer Infrastrukturen, zu erhöhen. KRITIS-Betreiber werden verpflichtet, ein Mindestniveau an IT-Sicherheit einzuhalten sowie dem BSI IT-Sicherheitsvorfälle zu melden. Das BSI wertet die gemeldeten Informationen aus und erstellt daraus kontinuierlich ein Lagebild, das auch den KRITIS-Betreibern sowie den zuständigen Behörden zur Verfügung gestellt wird. Die Betreiber erhalten somit Informationen und Know-how zurück und können von der Auswertung der Meldungen aller Betreiber sowie vieler anderer Quellen durch das BSI profitieren.

Die Umsetzung des Gesetzes soll gemeinsam mit den zuständigen Fachbehörden und den Betreibern der Kritischen Infrastrukturen erfolgen. Dazu werden der kooperative Ansatz und die Strukturen des UP KRITIS als etablierter Kooperationsplattform zwischen Betreibern und Staat genutzt und weiterentwickelt und existierende Kommunikationsstrukturen weiter ausgebaut. Die KRITIS-Betreiber müssen nach dem IT-Sicherheitsgesetz eine Kontaktstelle benennen, über die sie jederzeit erreichbar sind. Hierfür können auch „Single Points of Contact“ (SPOC) genutzt werden, die als gemeinsame übergeordnete Ansprechstelle für Betreiber eines Sektors fungieren (siehe Abb. 13) und eine anonyme Meldung ermöglichen. Kooperativ erfolgt auch die Erarbeitung branchenspezifischer IT-Sicherheitsstandards zur Gewährleistung eines der Bedrohungslage angemessenen Mindestniveaus an IT-Sicherheit. Die Standards werden von den Betreibern und deren Verbänden erarbeitet und vom BSI anerkannt. Umsetzung und Wirksamkeit der erarbeiteten Maßnahmen werden in Audits geprüft.

! Cyber-Angriff auf französischen Fernsehsender TV5MONDE

Sachverhalt: Der französische Fernsehsender TV5MONDE wurde im April 2015 Opfer eines massiven Cyber-Angriffs. Die Täter sabotierten essenzielle Produktions- und Übertragungsserver, sodass die Ausstrahlung des Fernsehprogramms für mehrere Stunden nicht möglich war. Parallel wurden die Twitter-, Facebook- und YouTube-Auftritte des Senders übernommen und zur Verbreitung von Propagandabotschaften für den „Islamischen Staat“ missbraucht. Zudem führte ein langanhaltender DDoS-Angriff dazu, dass die Webseite des Fernsehsenders über Stunden nicht erreichbar war.

Methode: Es ist bisher unklar, wie die Täter Zugang zum internen Netzwerk von TV5MONDE erlangten. Die sichtbaren Auswirkungen im April dürften jedoch das Ergebnis einer bereits länger zurückreichenden Netzwerk-Kompromittierung sein. Um die Fernsehausstrahlung und interne Server zu sabotieren, müssen die Täter über profunde Kenntnisse des internen Netzwerks und der Prozessabläufe des Senders verfügen. Es ist davon auszugehen, dass die Täter sich dieses Wissen über einen längeren Zeitraum angeeignet haben, indem sie das Netzwerk erst kompromittiert und dann aufgeklärt haben. Während dieser Aufklärungsphase können auch die Zugangsdaten für die Social-Media-Kanäle gesammelt worden sein. Diese Vorgehensweise entspricht der eines klassischen APT-Angriffs, bei dem zunächst ein einzelnes System mit einem Schadprogramm infiziert wird, um sich von diesem Einstiegspunkt aus weiter im internen Netz auszubreiten. Veröffentlichungen im Nachgang des Vorfalls zeigen, dass die gefundenen Schadprogramme im Mittleren Osten weit verbreitet sind[25].

Schadenswirkung: Erstmalig führte ein Cyber-Angriff zum Ausfall zentraler Funktionen eines TV-Senders. Durch ausgefallene Werbeeinnahmen und Aufwände für die Wiederherstellung der Infrastruktur hat der Sender finanzielle Verluste zu tragen. Hinzu kommt ein enormer Reputationsschaden.

Zielgruppen: Der Vorfall ist ein gutes Beispiel dafür, dass auch der KRITIS-Sektor Medien durch Cyber-Angriffe verwundbar ist. Medien- und Kultureinrichtungen – speziell Fernsehsender, deren Programm wie in diesem Fall weltweit ausgestrahlt wird – sind lohnenswerte Ziele, um eigene politische Botschaften zu verbreiten oder über diese Kanäle verbreitete Informationen zu manipulieren oder zu sabotieren. Die Methode, die bei dem Angriff auf TV5MONDE angewandt wurde, ist allerdings auch typisch für Spionageangriffe auf Unternehmen und Behörden.

Technische Fähigkeiten: Der oder die Angreifer besaßen die Fähigkeit, sich über längere Zeit unbemerkt in einem internen Netz auszubreiten. Dies spricht für erfahrene Täter. Über die Fähigkeit zur Ausbreitung hinaus verfügten die Täter auch über die Kompetenz, interne Arbeitsabläufe durch Beobachtung zu verstehen und die kritischen Punkte im Sendebetrieb zu identifizieren. Die koordinierte Vorgehensweise von Sabotage der Ausstrahlung, Defacement der Social-Media-Kanäle und langanhaltender DDoS-Angriffe spricht zudem für eine koordiniert funktionierende und disziplinierte Arbeitsorganisation.

[25] http://blog.trendmicro.com/trendlabs-security-intelligence/vbs-malware-tied-to-media-attacks

Erpressung: DDoS-Angriffe auf KRITIS-Unternehmen

Sachverhalt: Eine international agierende Gruppe namens DD4BC („DDoS for Bitcoins“) erpresst Unternehmen mit der Androhung und Durchführung von DDoS-Angriffen.

Ursache: Die Ursache ist im Bereich der Cyber-Kriminalität zu sehen. Es geht den Angreifern darum, Geld zu erpressen. Darüber hinausgehende Ziele wie Reputationsschädigung der angegriffenen Unternehmen oder Marktverdrängung der Opfer sind zum jetzigen Zeitpunkt nicht erkennbar.

Methode: Die Erpresser zielen mit DDoS-Angriffen (Reflection/Amplification-Angriffe) mit einer Bandbreite von bis zu 25 Gbit/s über einen Zeitraum von bis zu 60 Minuten auf die Unternehmen ab. Im Anschluss erhalten die Unternehmen ein Schreiben der Erpresser, in dem eine Zahlung von einigen Hundert Bitcoins verlangt wird. Bei Nichtzahlung wird ein weiterer Angriff von bis zu 500 Gbit/s angedroht.

Schadenswirkung: Die Auswirkungen der initialen Angriffe von bis zu 25 Gbit/s fallen sehr unterschiedlich aus. Bei einigen Unternehmen wurde der Angriff sofort mitigiert und es gab keine Schadwirkung, bei anderen kam es zu Ausfällen der Internetverbindung und der damit verbundenen Serviceleistungen. Es wurden auch Kollateralschäden beobachtet, etwa Ausfälle von Diensten, die sich auf derselben Server-Infrastruktur wie die des eigentlichen Opfers befinden, mit der Erpressung aber nichts zu tun haben. Ein Angriff mit der Bandbreite von bis zu 500 GBit/s, wie im Erpresserschreiben angedroht, hat bislang offenbar nicht stattgefunden, ist in technischer Hinsicht aber möglich. Bislang sind Bandbreiten von 40 bis 60 Gbit/s für den Hauptangriff öffentlich bekannt geworden.

Zielgruppen: In Deutschland und international sind dem BSI Betroffenheiten aus dem Finanz- und Versicherungswesen bekannt. Das BSI wirkte im Rahmen verschiedener behörden- und organisationsübergreifender Arbeitskreise an der Fallbearbeitung mit, beispielsweise im Rahmen des UP KRITIS oder in nationalen und internationalen CERT-Arbeitskreisen. Im Nationalen Cyber-Abwehrzentrum wurde eine Arbeitsgruppe zu dem Thema eingerichtet.

Technische Fähigkeiten: Über die technischen Fähigkeiten der Angreifer sind auf Basis der vorliegenden Erkenntnisse keine belastbaren Aussagen möglich. Mitunter könnten Kapazitäten zur Durchführung von DDoS-Angriffen im beschriebenen Kontext auch über Dritte zugekauft worden sein. Das bedeutet, dass die Erpresser auch ohne eigene technische Fähigkeiten die Erpressungskampagne betreiben könnten.

4.3 Bedrohungslage Kritischer Infrastrukturen

- Für Kritische Infrastrukturen besteht grundsätzlich die gleiche Gefährdungslage wie für andere Wirtschaftsunternehmen auch. Gefährdungen durch Cyber-Sabotage bzw. -Terrorismus sind jedoch für Kritische Infrastrukturen speziell, da hier die Störung der Verfügbarkeit bzw. ein möglichst großer gesellschaftlicher Schaden das Ziel der Angreifer ist.

- Die Bedrohung durch Cyber-Crime ist insbesondere für den Sektor Finanz- und Versicherungswesen relevant. Die verübten Verbrechen reichen von Identitätsdiebstahl über Cyber-Angriffe auf die Infrastrukturen von Bankinstitutionen bis hin zur Erpressung.

- Angriffe politisch motivierter Hacktivisten sind bei Unternehmen der KRITIS-Sektoren Medien (Defacements oder Platzierung von Falschinformationen auf gekaperten Medienwebseiten), Energie und Kreditwirtschaft zu beobachten.

- Besorgniserregend ist die Bedrohung durch Cyber-Sabotage. Seit Stuxnet weiß man, dass die Sabotage von Maschinen und Einrichtungen durch Cyber-Angriffe nicht nur denkbar ist, sondern tatsächlich durchgeführt wird. Der Angriff auf die französische Sendergruppe TV5MONDE ist ein aktuelles Beispiel für eine erfolgreiche Cyber-Sabotage.

- Das Potenzial für Cyber-Angriffe durch andere Staaten stellt für die deutsche Wirtschaft eine Bedrohung dar. Darüber hinaus sind Unternehmen in Deutschland in vielen Fällen nicht ausreichend gegen Cyber-Angriffe gerüstet. Dies gilt auch für Kritische Infrastrukturen.

- Nicht nur gezielte Angriffe stellen eine Bedrohung für Kritische Infrastrukturen dar. Auch ungerichtete Angriffe zum Beispiel mit Schadsoftware können Kritische Infrastrukturen treffen und den normalen Betriebsablauf stören (siehe Vorfall „Ransomware im Krankenhaus“). Die Herausforderung für viele Kritische Infrastrukturen ist, dass technische Geräte und Softwareprodukte genutzt werden bzw. genutzt werden müssen, die entweder gar nicht oder nur mit hohem Aufwand gepatched werden können. Dies bietet den zigtausend Schadprogrammen, die im Internet kursieren, viele Angriffsmöglichkeiten. In diesem Zusammenhang ist das sogenannte „Bring Your Own Device“ eine der größten Gefahrenquellen, da Schadsoftware aus den privaten Netzen der Mitarbeiter direkten Zugang zu den Unternehmensnetzen erhalten kann.

- Durch die zunehmende Vernetzung bei Kritischen Infrastrukturen ergeben sich immer mehr mögliche Fehlerquellen. Grund dafür sind die zunehmende Komplexität der Netze an sich sowie die Nutzung von Standardsoftware und Standardprotokollen für die Vernetzung. So hat die falsche Konfiguration von Geräten und Software bei einem Test eines Steuerungssystems eines Gasnetzbetreibers zu erheblichen Problemen in den Steuerungssystemen von Stromnetzen geführt.

- Eine Aussage darüber, welcher Sektor von welcher Gefährdung besonders betroffen ist, ist nur sehr schwierig zu treffen. Ein gezielter Angriff auf den Sektor X kann versehentlich auch den Sektor Y betreffen, da hier dieselben Protokolle und dieselbe Software genutzt werden. Gleichwohl kann die Art und Größe der Auswirkung in den Sektoren sehr unterschiedlich sein. Wenn Sektor X öfter mit Angriffen einer bestimmten Art zu tun und sich dementsprechend abgesichert hat, ist der Angriff unter Umständen für Sektor Y völlig neu und könnte erhebliche Störungen verursachen.

Bewertung

Aufgrund der voranschreitenden Digitalisierung und Vernetzung sind Unternehmen mehr denn je abhängig von funktionierender Informationstechnologie. In besonderem Maße gilt dies für Kritische Infrastrukturen, deren Ausfall erhebliche Konsequenzen nicht nur für das betroffene Unternehmen, sondern für Wirtschaft, Staat und Gesellschaft haben kann. Daher tragen die Betreiber, aber auch der Staat eine besondere Verantwortung, der beide Seiten gerecht werden müssen. Dass Cyber-Angriffe auch vor den Kritischen Infrastrukturen nicht Halt machen, haben die Vorfälle des Jahres 2015 gezeigt. Die Verbesserung der IT- und Cyber-Sicherheit Kritischer Infrastrukturen ist Aufgabe und Ziel des UP KRITIS, der jedoch nicht in allen Bereichen zum gewünschten Erfolg geführt hat. Durch das im Juli 2015 in Kraft getretene IT-Sicherheitsgesetz werden Betreiber Kritischer Infrastrukturen verpflichtet, ein Mindestniveau an IT-Sicherheit einzuhalten und dies auch überprüfen zu lassen.

Spear-Phishing gegen KRITIS-Unternehmen im Energie-Sektor

Sachverhalt: Ein Mitarbeiter der Finanzbuchhaltung eines KRITIS-Unternehmens aus dem Energiesektor erhielt eine sehr gut gemachte Phishing-Mail, in der er aufgefordert wurde, sich an eine E-Mail-Adresse einer Anwaltskanzlei zu wenden, um dort Daten für eine Finanztransaktion zu erhalten. Dem Mitarbeiter kam die E-Mail seltsam vor und er informierte sein Unternehmen darüber.

Methode: In der Phishing-Mail wird ein existierender Mitarbeiter der Geschäftsführung als angeblicher Absender angegeben, um den Auftrag zur Zahlung zu legitimieren. Tatsächlich wurde die Identität des Mitarbeiters jedoch nur vorgetäuscht und dessen E-Mail-Adresse missbräuchlich verwendet.

Schadenswirkung: Es ist kein Schaden entstanden.

Technische Fähigkeiten: Die Phishing-Mail ist sehr gut gemacht. Die E-Mail-Adresse des Absenders ist authentisch und auch die genannte Anwaltskanzlei existiert wirklich. Der Text ist in einwandfreiem Deutsch geschrieben:

Von: <Mitarbeiter-GF>
An: <Mitarbeiter-Finanzbuchhaltung>
Betreff: <Projektname/Code>

Sehr geehrter Herr <Mitarbeiter-Finanzbuchhaltung>,

Ich teile Ihnen mit, dass ich derzeit eine vertrauliche Finanztransaktion behandle, die heute mithilfe von Herr <Mitarbeiter-Anwaltskanzlei> der Anwaltskanzlei, deren Angaben Sie unten finden, zum Abschluss gebracht werden muss.

Bitte wenden Sie sich umgehend per E-Mail an <E-Mail-Adresse Mitarbeiter-Anwaltskanzlei> oder melden Sie sich telefonisch unter der Nummer +XXX XX XXX XXX. Ihre Kontaktperson wird Ihnen die Bankverbindung zusenden, um eine erste Anzahlung auf diese Operation zu leisten. Bitte befolgen Sie strikt seine Anweisungen. Geben Sie in Ihrer Nachricht oder beim Aufruf die Referenz <Projektname/Code> an.

Ich bitte Sie um die notwendige Diskretion und Vertraulichkeit bezüglich dieses Dossiers, da Sie bis zur offiziellen Bekanntmachung, die sehr bald stattfinden wird, der einzige Kontakt zwischen unserer Gruppe und der Anwaltskanzlei sind. Alle unsere zukünftige Kommunikation zu diesem Dossier wird über die E-Mail-Adresse von Herr <Mitarbeiter-Anwaltskanzlei> erfolgen. Ich zähle auf Ihre Reaktionsbereitschaft, da die Anwaltskanzlei mich über die Entwicklung dieses Dossiers, das mir besonders wichtig ist, informieren muss.

Mit freundlichen Grüßen,
<Mitarbeiter-GF>
„Von meinem Mobile gesendet“

5 Gesamtbewertung und Fazit

5 Gesamtbewertung und Fazit

Die hohe Komplexität der Informationstechnik lässt sich auch in der IT-Sicherheitslage in Deutschland feststellen. Die Frage der Bedrohung zum Beispiel durch ein einzelnes Schadprogramm ist nachrangig im Hinblick auf die Vielfältigkeit der Ursachen, Methoden und Rahmenbedingungen, die die Gefährdungslage im Berichtszeitraum prägen. Es sind deswegen vielmehr die Abhängigkeiten untereinander, das Zusammenwirken und die gegenseitige Beeinflussung der einzelnen Faktoren, die das Gesamtbild der Gefährdungslage zeichnen. Folgerichtig dürfen auch Lösungsansätze nicht singulär greifen, sondern müssen nach Möglichkeit einen positiven Einfluss auf die IT-Sicherheitslage in der Breite haben.

5.1 Kausalität der Gefährdungen

Die Gefährdungslage der IT-Sicherheit in Deutschland 2015 wird in vielen Bereichen als hoch bewertet:

Gefährdung	2014	2015
Cloud Computing		→
Software-Schwachstellen	→	↑
Hardware-Schwachstellen		→
Nutzerverhalten und Herstellerverantwortung		↑
Kryptografie		→
Internet-Protokolle		↑
Mobilkommunikation		↑
Sicherheit von Apps		↑
Sicherheit von Industriellen Steuerungsanlagen		↑
Schadsoftware	↑	↑
Social Engineering	↑	→
Gezielte Angriffe - APT	→	↑
Spam	↑	↑
Botnetze	→	↑
Distributed Denial-of-Service (DDoS)-Angriffe	→	→
Drive-by-Exploits und Exploit-Kits	→	↑
Identitätsdiebstahl	↑	↑

Legende
Gefährdung 2015 (niedrig, durchschnittlich, hoch) ↓ → ↑

Eine isolierte Betrachtung der einzelnen Aspekte wird der Gesamtbewertung jedoch nicht gerecht. Die aktuelle Gefährdungslage ist vielmehr das Produkt der Kausalität und Komplexität ihrer einzelnen Aspekte. Abbildung14 zeigt beispielhaft, wie die im Bericht skizzierten Ursachen, Methoden und Rahmenbedingungen teilweise zusammenhängen und sich gegenseitig beeinflussen:

- Ein unzureichendes Patch-Management und somit die Nutzung veralteter Software auf Rechnern, Mobilgeräten oder zentralen Server-Systemen bleibt eine große technische Herausforderung für die Anwender und ist Ursache vieler erfolgreicher Angriffe. Gerade die vielen im Jahr 2015 bekannt gewordenen Zero-Day-Schwachstellen sowie die schnelle Nutzung neuer Schwachstellen zum Beispiel in Exploit-Kits verdeutlichen die Notwendigkeit, ein durchgängiges und schnelles Patch-Management aufzusetzen, das Grundlage einer nachhaltigen Informationssicherheit ist.

- Es fehlt vielfach an Bewusstsein der Anwender für Social Engineering und Manipulationsversuche, die viele Cyber-Angriffe begleiten. Im privaten wie auch im geschäftlichen Kontext ist ein gesundes Misstrauen gegenüber unerwarteten Kontaktaufnahmen notwendig, sei es in Bezug auf angebliche Telefonrechnungen, ungefragte Support-Angebote am Telefon oder angebliche Geheimprojekte in Unternehmen, die zur Weitergabe vertraulicher Informationen oder sogar zu Finanztransaktionen führen.

- Hersteller und Diensteanbieter tragen Verantwortung für ihre Produkte und Dienstleistungen. Nach Meldung oder Bekanntwerden einer Schwachstelle sind sie in der Pflicht, diese schnellstmöglich zu schließen und die Anwender mit Sicherheitsupdates zu versorgen. Zum Schutz von Unternehmens- und Kundendaten sollten Diensteanbieter aus eigenem Selbstverständnis ein hohes Interesse an einem verlässlichen Sicherheitsniveau haben.

- APT-Angriffe sind aktuell und zukünftig eine große Bedrohung für Unternehmen und Verwaltungseinrichtungen. APT-Angriffe zum Zweck der Wirtschaftsspionage oder Konkurrenzausspähung werden auch in Zukunft von verschiedenen Gruppen durchgeführt werden. Insbesondere Unternehmen, die international aktiv und sichtbar sind, sollten APT-Angriffe in ihr unternehmerisches Risikomanagement einbeziehen und IT-Sicherheitsmaßnahmen im Bereich Detektion und Monitoring sowie im Bereich der Vorfallsbearbeitung umsetzen.

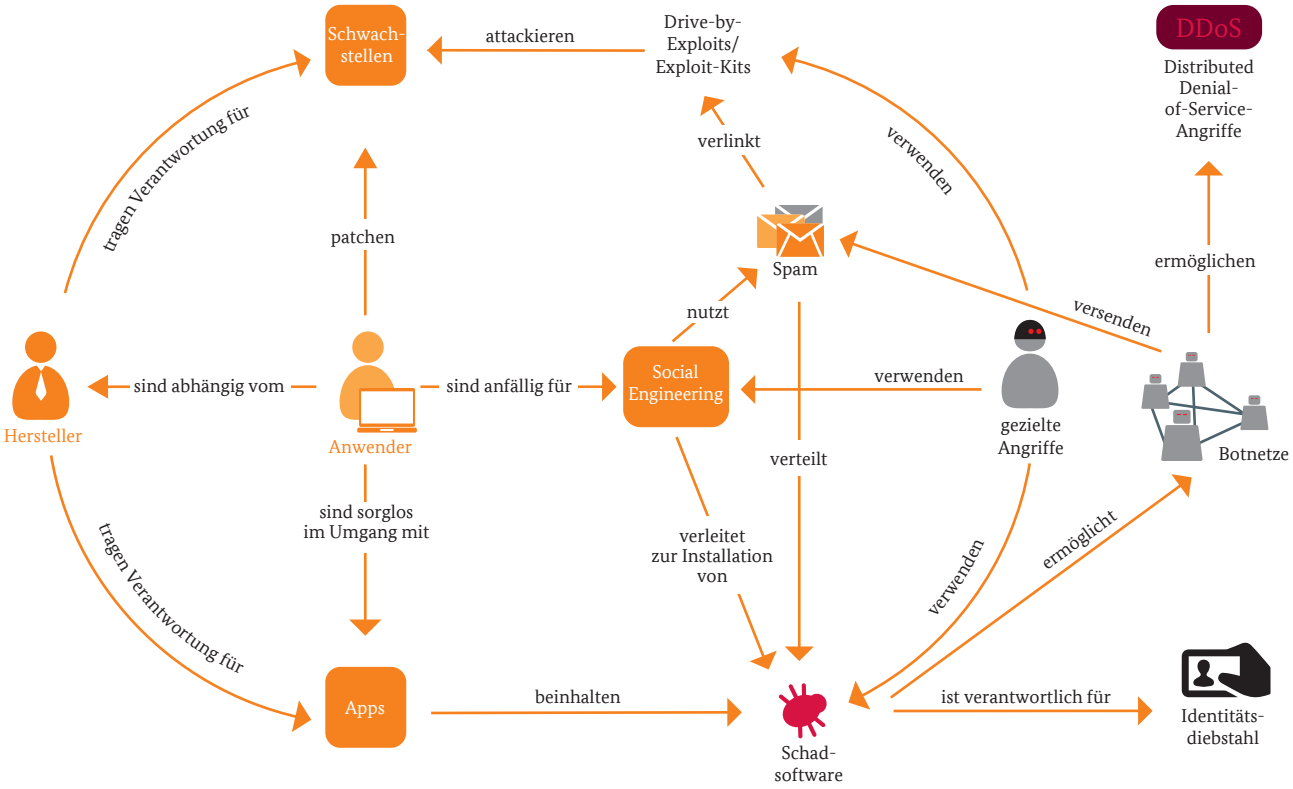

Abbildung 14: Kausalität der aktuellen Gefährdungslage

- IT im industriellen Umfeld sowie die Vernetzung industrieller Steuerungssysteme bleiben über das Jahr 2015 hinaus eine große Herausforderung, gerade auch im Bereich der Kritischen Infrastrukturen. Eine hinreichende Segmentierung der Netze ist derzeit nicht gegeben, sodass auch Angriffe auf Büronetze Auswirkungen auf Steuerung und Fertigung haben können.

- Die Anzahl der detektierten Schadprogramme steigt sowohl für stationäre als auch insbesondere für mobile Plattformen weiter an. In Verbindung mit den kürzer werdenden Verteilzyklen der Angreifer setzt dies den signaturbasierten Ansatz von Schutzkomponenten weiter unter Druck. Spamnachrichten bleiben dabei eine Hauptquelle von Schadprogramminfektionen.

- Für das Management einer Organisation stellt sich zunehmend die Frage, welche wirtschaftlichen Folgen ein erfolgreicher Cyber-Angriff für die betroffene Organisation selbst (interne Kosten) oder aber für Kunden, Dienstleister und Lieferanten (externe Kosten) nach sich ziehen kann. Produktions- bzw. Betriebsausfälle sowie der oft erhebliche finanzielle und personelle Aufwand zur Wiederherstellung betroffener Systeme und zur Aufklärung der Vorfälle zählen nach der Cyber-Sicherheitsumfrage 2015[26] in der Allianz für Cyber-Sicherheit zu den häufigsten Schäden nach erfolgreichen Angriffen.

- Die technische Fortentwicklung der Gefährdungslage spricht auch für eine weiter fortschreitende Professionalisierung der Angreifer, egal ob bei Angriffen gegen den Staat, die Wirtschaft, die Wissenschaft oder Bürger und Gesellschaft. Die Verfügbarkeit von Werkzeugen sowie das Angebot von Dienstleistungen und kompletten Infrastrukturen zur Durchführung von Cyber-Angriffen sorgen dafür, dass das Einstiegsniveau zu deren Durchführung weiter sinkt und gleichzeitig neuen Akteuren zur Verfügung steht.

- Angesichts der Schwierigkeiten bei der Verfolgung von Straftaten (Attribuierung und Anonymisierung) ergibt sich daraus ein lukratives Geschäftsmodell und eine damit einhergehende zusätzliche Gefährdung für die IT-Sicherheit.

- Die praktischen Auswirkungen zeigen sich in den im vorliegenden Lagebericht dargestellten Vorfällen, von denen alle Anwendergruppen in Deutschland betroffen sind. Auch hier sind es nicht isolierte Einzelaspekte, sondern ein Zusammenwirken verschiedener Merkmale, die einen Angriff erfolgreich machen.

[26] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Micro/Umfrage/umfrage2015.html

5.2 Gemeinsame Verantwortung für die IT-Sicherheit in Deutschland

In einer Welt, in der die Digitalisierung nahezu alle Lebensbereiche und Anwendergruppen betrifft, wird auch die Verantwortung für IT-Sicherheit zu einer gesamtgesellschaftlichen Aufgabe, die gemeinsam von Bürgern, Wirtschaft, Forschung und Politik getragen werden muss. Prävention, Reaktion und Nachhaltigkeit bleiben dabei die Handlungsfelder des BSI.

Assume the Breach: Verantwortung für Prävention, Detektion und Reaktion in der Wirtschaft

In der Wirtschaft muss sich durchsetzen, dass IT-Sicherheit Teil des Risikomanagements und damit eine Managementaufgabe ist, die in der Unternehmensleitung verankert ist. Eine mangelnde Entschlossenheit der Unternehmensführung führt somit zu mangelhafter IT-Sicherheit. Dabei kann IT-Sicherheit nach dem Pareto-Prinzip wirtschaftlich umgesetzt werden: Die Investition in bewährte Basismaßnahmen in den Bereichen Technik, Personal und Organisation lässt sich wirtschaftlich vertreten und schützt bereits gegen eine Vielzahl heutiger Angriffe. Punktuell können weitere Schutzmaßnahmen ergänzt werden. Nach diesem Vorbild wird aktuell der IT-Grundschutz des BSI weiterentwickelt. Daneben bietet die Allianz für Cyber-Sicherheit eine Plattform zum Informations- und Erfahrungsaustausch. Im Hinblick auf die aktuelle Gefährdungslage ist eine Investition in die Prävention bereits aktive Spionageabwehr.

Neben der Prävention muss auch die Säule der Detektion gestärkt werden. Je eher ein Angriff detektiert und darauf reagiert werden kann, desto geringer sind die Schäden, zum Beispiel für die Bereinigung der betroffenen Systeme oder durch tatsächlich abgeflossene Daten. Dabei ist der Datenschutz kein Hinderungsgrund für effektive Detektionsmaßnahmen: Datenschutzkonforme Maßnahmen sind heute in Absprache mit der Personalvertretung und/oder den Datenschutzbeauftragten möglich. Bestehende Detektionsmaßnahmen können durch den Einkauf sogenannter Early Warnings oder Angriffsmerkmale („Indicators Of Compromise“) ergänzt werden, um die Chance zu erhöhen, auch gezielte und neuartige Angriffe zu erkennen. In gleicher Weise wird das BSI seine zukünftigen Erkenntnisse, die aus der Meldepflicht von Betreibern der Kritischen Infrastrukturen nach dem IT-Sicherheitsgesetz gewonnen werden, gebündelt an die Unternehmen weitergeben.

Trotzdem reichen Prävention und Detektion bei der heutigen Bedrohungslage nicht mehr aus. Statt einer reinen Abwehr gegen Angriffe gehört es zum Risikomanagement einer Organisation, sich darauf einzustellen und darauf vorzubereiten, dass ein IT-Sicherheitsvorfall eintritt oder ein Cyber-Angriff erfolgreich ist (Paradigma: Assume the Breach). Dazu müssen Strukturen geschaffen, Verantwortlichkeiten benannt und Prozesse geübt werden, wie mit einem anzunehmendem Vorfall umzugehen ist. Durch eine professionelle Reaktion auf einen Vorfall können Folgeschäden wirksam vermindert werden. Dazu existieren bereits Dienstleister, die auf die Reaktion auf Cyber-Angriffe spezialisiert sind und Unternehmen bei der Vorfallsbewältigung unterstützen.

Förderung der Kryptografie und der IT-Sicherheitswirtschaft

Die Entwicklung und Anwendung starker und verlässlicher Kryptografie ist Voraussetzung für Verschlüsselung, Authentisierung und Integritätssicherung elektronischer Kommunikation. Ohne sie gibt es kein Vertrauen in die heutige Kommunikationstechnik. Dennoch ist das Potenzial von Kryptografie, auch aufgrund mangelnder Nachfrage, heute noch nicht ausgeschöpft, weshalb sich das BSI weiterhin für eine Förderung der Forschung und Anwendung von Kryptografie in Deutschland einsetzt und diese unterstützt. Gleiches gilt für die IT-Sicherheitswirtschaft und die Entwicklung von Cyber-Abwehrmaßnahmen in Deutschland, die sich bisher noch nicht zu einem eigenständigen Marktsegment weiterentwickeln konnten. Beide Bereiche müssen sich immer wieder neu an den Bedarf und die aktuelle Bedrohungslage anpassen. Zum Schutz der technischen Souveränität ist es notwendig, Firmen und Investitionen in Kryptografie und IT-Sicherheit in Deutschland zu halten und bei sich abzeichnendem Unternehmenserfolg vor Übernahmen aus dem Ausland zu schützen.

Die außergewöhnlich hohe Innovationsgeschwindigkeit der Informationstechnik wird auch in den kommenden Jahren die IT-Sicherheit vor neue Herausforderungen stellen. Eine weitere Zunahme bei erfolgreichen Angriffen auf Systeme und Dienste aller Anwendergruppen ist abzusehen. Rahmenbedingungen sowie Maßnahmen der Prävention, Detektion und Reaktion müssen sich in gleicher Geschwindigkeit weiterentwickeln. Bereits heute trägt jeder Anwender mit seinem Verhalten Verantwortung für die IT-Sicherheit in Deutschland.

6 Glossar

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

Adware
Als Adware werden Programme bezeichnet, die sich über Werbung finanzieren. Auch Schadprogramme, die Werbeeinnahmen für den Autor des Schadprogramms generieren, werden als Adware bezeichnet.

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.

BIOS
Das BIOS (Basic Input Output System) auf PC-Systemen ist der Programmcode, der nach dem Start eines Systems als Erstes ausgeführt wird. Das BIOS stellt standardisierte Zugriffsmöglichkeiten des Betriebssystems auf die Hardware bereit.

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

Bring Your Own Device
Mit Bring Your Own Device (BYOD) wird die Nutzung privater Endgeräte für berufliche Zwecke sowie deren Einbindung in Unternehmensnetze bezeichnet.

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 und die Prävention von sowie Reaktion auf IT-Sicherheitsvorfälle kümmern.

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

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

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

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

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

Logdaten / Logdatei
Eine Logdatei enthält ein Protokoll von Aktionen und Prozessen auf einem Computer.

NTP
Das Network Time Protokoll dient der Zeitsynchronisation von IT-Systemen in Netzwerken.

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, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internetnutzers zu gelangen und damit Identitätsdiebstahl zu begehen.

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

Ransomware
Ransomware sind Schadprogramme, mit deren Hilfe ein Eindringling eine Zugriffs- oder Nutzungsverhinderung der Daten sowie des gesamten Computersystems erwirkt. Meist dient dies dazu, Lösegeld („ransom") zu erpressen.

Reflection-Angriff
Hierbei handelt es sich um eine spezielle Form eines DDoS-Angriffs. Bei einem Reflection-Angriff wird das Opfersystem nicht direkt angegriffen. Stattdessen spielt der Angreifer „über Bande" (reflection). Dazu sendet er eine Anfrage mit gefälschter Absenderadresse (Opfersystem) an ein Zielsystem (Bande). Die Antwort auf die Anfrage des Angreifers erhält dann aufgrund der gefälschten Adresse nicht der Angreifer, sondern das Opfersystem. Die Antwortpakete sind häufig deutlich größer als die Anfragen. Dadurch ist es dem Angreifer möglich, mit Einsatz einer geringen eigenen Bandbreite viel Angriffsbandbreite zu erzeugen. Man spricht in diesem Fall von einer Verstärkung der eingesetzten Bandbreite.

Social Engineering
Bei Cyber-Angriffen mittels 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 Spamnachrichten 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).

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

Watering-Hole-Angriffe
Die Analogie des Begriffs Watering Hole bezieht sich auf ein Wasserloch, das Beutetiere anlockt und somit ein bevorzugtes Revier für deren Jäger ist. Bei dieser Angriffsform werden im Vorfeld Internetseiten gehackt und mit Schadcodes versehen, die von einer Zielperson mit hoher Wahrscheinlichkeit aufgerufen werden. Wird eine dieser infizierten Seiten besucht, installiert sich automatisch ein Schadprogramm (etwa durch Drive-by-Download).

Webbrowser
Webbrowser sind spezielle Computerprogramme zur Darstellung von Webseiten im World Wide Web oder allgemein von Dokumenten und Daten.

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
November 2015

Druck
Druck- und Verlagshaus Zarbock Frankfurt am Main

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

Bildnachweis Titelbild
Fotolia

Grafiken
BSI

Artikelnummer
BSI-LB15/504

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

www.bsi.bund.de