Die Wirtschaft im Fokus von Cyber-Angriffen

Stefan Becker · Till Kleinert

Bundesamt für Sicherheit in der Informationstechnik
{stefan.becker | till.kleinert}@bsi.bund.de

Zusammenfassung

Während Cyber-Angriffe in den Anfangszeiten des Internets eher ein seltenes Phänomen waren, hat sich hieraus inzwischen eine hochprofessionelle Branche mit spezialisierten Dienstleistern im Darknet entwickelt. Täglich können neue Angriffe und Schadsoftware-Varianten beobachtet werden. Die zunehmende Vernetzung und Digitalisierung im Alltag eröffnet den Tätern gleichzeitig immer neue Möglichkeiten für Angriffe. Unternehmen sollten daher adäquate Schutzmaßnahmen implementieren und vorgefertigte Notfallpläne bereithalten. Der hier beschriebene Vortrag dient zur Einführung des Workshops „Incident Response - Korrektes Verhalten im Ernstfall“, in dem eine effiziente Bearbeitung von IT-Sicherheitsvorfällen im Unternehmen diskutiert werden soll.

1 Bedrohungslage

Im Jahr 2017 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) pro Monat durchschnittlich fast 52.000 E-Mails abgefangen, die an Empfänger in der Bundesverwaltung gerichtet waren und im Anhang Schadsoftware mit sich bringen sollten. Dies geht aus dem Bericht „zur Lage der IT-Sicherheit in Deutschland 2017“ hervor, den das BSI jährlich veröffentlicht. Bei der Statistik der schadhaften E-Mails, die immer noch als häufigster Angriffsvektor für Attacken auf die Regierungsnetze verwendet werden, ist dabei eine Zunahme von 18% im Vergleich zum Vorjahr zu verzeichnen. Diese Steigerung geht insbesondere auf die zahlreichen Ransomware-Wellen – z.B. mit Locky oder Wannacry – zurück, die in den Vormonaten von sich reden machten und auch in Unternehmen und Privathaushalten für Probleme sorgten.

Auch andere Institutionen beschäftigen sich regelmäßig mit Straftaten im Cyber-Raum und können von ähnlichen Entwicklungen berichten. So stellt das Bundeskriminalamt im Lagebild Cybercrime von 2016 ein Zuwachs auf 253.290 Fälle „mit dem Tatmittel Internet“ fest. Das Bundesamt für Verfassungsschutz und der Digitalverband Bitkom kamen in einer gemeinsamen Studie zu dem Ergebnis, dass der deutschen Wirtschaft durch Cyber-Angriffe jährlich ein Schaden in Höhe von 55 Milliarden Euro entsteht.

Alle Quellen gehen von einer unverändert hohen Bedrohungslage aus. Organisationen aller Branchen und Größen sollten sich daher der ständigen Gefahr bewusst sein.

2 Aktuelle Vorfälle

Im Folgenden finden Sie eine Übersicht verschiedener IT-Sicherheitsvorfälle, mit denen sich das Bundesamt für Sicherheit in der Informationstechnik in den vergangenen Monaten befasst

P. Schartner · N. Pohlmann (Hrsg.) · D•A•CH Security 2018 · syssec (2018) 323-328.

hat. Die Auswahl ist nur exemplarisch. Nahezu täglich können neue Incidents in den gängigen Fachmedien gefunden werden.

2.1 Schwachstellen in Content-Management-Systemen

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

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

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

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

2.2 DDoS-Angriff auf KrebsOnSecurity

Sachverhalt: Am 19. September 2016 meldete Octave Klaba vom französischen Webhoster OVH über Twitter zwei DDoS-Angriffe mit den extrem hohen Bandbreiten von 1.156 und 622

Gigabit pro Sekunde. Das Volumen der Angriffe übertraf die bisher größten verzeichneten Angriffe des DDoS-Mitigation-Dienstleisters Akamai um ein Vielfaches. Am Abend des folgenden Tages wurde das Weblog https://krebsonsecurity.com des Sicherheitsforschers Brian Krebs von einer massiven DDoS-Attacke mit etwa 620 Gigabit pro Sekunde getroffen. Brian Krebs hatte im Vorfeld der Angriffe kritisch über Anbieter von sogenannten Booter-Diensten berichtet, die kostenpflichtige DDoS-Attacken auf beliebige Ziele offerieren.

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

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

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

2.3 CEO-Betrug

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

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

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

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

3 Tätertypologie

Die Motive und Ressourcen der Cyber-Angreifer variieren sehr stark. Die für Unternehmen wie Privatpersonen gleichermaßen häufigste Bedrohung geht von sog. ungezielten Angriffen aus. Hier geht es den Tätern in erster Linie darum, einen Schaden zu verursachen. Wer diesen erleidet, spielt dabei eine untergeordnete Rolle. Ungezielte Angriffe werden insbesondere ausgeübt von:

- **Cyber-Kriminellen**: Die Motivation von Cyber-Kriminellen ist es, mithilfe der Informationstechnik auf illegalen Wegen Geld zu verdienen. Die Bandbreite reicht von organisierter Cyber-Kriminalität bis hin zu einfacher Kriminalität mit geringen Schäden.

- **Skript-Kiddies**: Die Gruppe der Skript-Kiddies führt Cyber-Angriffe durch, um Fähigkeiten und Wissen in der Praxis auszutesten. Es werden keine finanziellen Interessen verfolgt. Die Auswahl der Angriffsziele ist unspezifisch und vielfach allein vom Grad der Absicherung abhängig.

Entsprechend der Kategorisierung existieren neben den ungezielten auch gezielte Angriffe. Bei diesen fokussieren sich die Täter auf ein vorher definiertes Opfer und versuchen über ausgeklügelte Methoden, zum Erfolg zu kommen. Häufig stehen den Angreifern umfangreiche Ressourcen zur Verfügung – bspw. um lange Zeit für die Suche nach Schwachstellen in einem System zu suchen oder um Angriffswerkzeuge für viel Geld einzukaufen. Diese Gegebenheiten machen es den Opfern schwer – wenn nicht sogar unmöglich – die Cyber-Attacken dauerhaft abzuwehren. Hinter gezielten Angriffen stehen häufig diese Tätergruppen:

- **Cyber-Aktivisten**: Angreifer, die durch einen Cyber-Angriff auf einen politischen, gesellschaftlichen, sozialen, wirtschaftlichen oder technischen Missstand aufmerksam machen oder eine diesbezügliche Forderung durchsetzen wollen („Hacktivismus“). Die Motivation hinter dem Angriff ist Einflussnahme. Der durch einen Cyber-Angriff entstandene Schaden wird in Kauf genommen bzw. forciert, um eine höhere Aufmerksamkeit zu erlangen. Sogenannte ethische Hacker fokussieren sich auf gesellschaftliche oder soziale Themen.
- **Wirtschaftsspione im Cyber-Raum**: Durch die Vorteile des Internets ergeben sich für Spione neue Möglichkeiten. Wirtschaftsspionage und Konkurrenzausspähung dienen finanziellen Interessen. Interne Informationen über Mitbewerber und deren Produkte bieten geldwerte Vorteile im globalen Wettbewerb.
- **Staatliche Nachrichtendienste im Cyber-Raum**: Cyber-Angriffe durch staatliche Nachrichtendienste dienen – im Gegensatz zur Wirtschaftsspionage – nicht primär finanziellen Interessen, sondern der Informationsbeschaffung und der Einflussnahme.
- Staatliche Akteure im Cyber-War: Im militärischen Sektor wird der Cyber-Raum inzwischen vielfach als weitere wichtige Domäne neben den klassischen militärischen Domänen Land, See, Luft und Weltraum angesehen.
- **Cyber-Terroristen**: Terroristen können Cyber-Angriffe wie staatliche Akteure und Kriminelle nutzen, um unterschiedliche Ziele anzugreifen und somit ihre Ideologie zu verbreiten und ihren Einfluss auszuweiten.

Vereinzelt werden die Akteure im Cyber-Raum auch lediglich in drei Gruppen unterteilt: Blackhats – die aus krimineller Motivation hacken, Whitehats – die z.B. aus Aspekten der Forschung versuchen, in Systeme einzudringen, dabei jedoch stets gesetzeskonform handeln und die Ergebnisse u.a. zur Optimierung der Produktsicherheit an die Hersteller/Betreiber weitergeben sowie Greyhats – deren Motivation nicht immer eindeutig ist.

4 Angebote von BSI und Ermittlungsbehörden

Ein wesentlicher Schlüssel, um gut vor Cyber-Angriffen gerüstet zu sein, besteht im kontinuierlichen Austausch zur aktuellen Bedrohungslage. Die deutschen Behörden bieten hierzu verschiedene Anlaufstellen an, über die aktuelle Warnmeldungen und andere Erkenntnisse zur Cyber-Sicherheitslage verteilt werden. Gleichzeitig leben diese Angebote jedoch auch davon, dass Unternehmen eigene Erkenntnisse (anonym) an die Anlaufstellen weitergeben. Nur so können ein realistischer Eindruck der aktuellen Lage ermittelt und Hinweise zu den derzeitigen Methoden der Täter an andere Unternehmen weitergereicht werden.

Als Anlaufstellen bieten sich insbesondere:

- Die Allianz für Cyber-Sicherheit, eine Initiative des Bundeamtes für Sicherheit in der Informationstechnik, die als Public Private Partnership eine Plattform zum Austausch bietet. Das Bundesamt und zahlreiche Experten aus der Wirtschaft stellen hier kostenlos Inhalte zur Prävention – z.B. Whitepaper und Seminare – als auch zur Reaktion – z.B. in Form von Warnmeldungen – zur Verfügung. Im Gegenzug können Teilnehmer eigene Beobachtungen zu Cyber-Angriffen über ein Online-Formular an die Community weitergeben (siehe auch www.allianz-fuer-cybersicherheit.de).
- Die Zentralen Ansprechstellen Cybercrime (ZAC) der Länder und des Bundes unterstützen Unternehmen sowohl mit Informationen zur Vermeidung von Angriffen als auch im Falle von Cybercrime-Straftaten. Hierfür haben die Landeskriminalämter und das Bundeskriminalamt Anlaufstellen eingerichtet, an die sich betroffene wenden können (siehe auch https://www.bka.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html).
- Ein Angebot zum Schutz von Unternehmen im Allgemeinen stellen die deutschen Sicherheitsbehörden mit der Initiative Wirtschaftsschutz zur Verfügung. Hier erhalten Interessierte nicht nur präventive Informationen zum Schutz vor Cyber-Angriffen, sondern ebenfalls zu weiteren Bedrohungsszenarien. (siehe auch https://www.wirtschaftsschutz.info).

5 Skizzierung Incident Response

Um auf die beschriebenen Störungen – unabhängig davon, ob mutwillig durch Cyber-Angriffe oder z.B. durch Defekte verursacht – adäquat reagieren zu können, sollten Unternehmen vorgefertigte Notfallpläne bereithalten. Diese beinhalten einerseits eine Liste der miteinzubeziehenden Stellen in der Organisation, andererseits auch konkrete Maßnahmen, wie auf welche Bedrohung zu reagieren ist. Idealerweise werden dieses Verhalten in den Institutionen regelmäßig durch Übungen trainiert und die Maßnahmen validiert. Das konkrete Vorgehen wird im Rahmen des Workshops der Allianz für Cyber-Sicherheit während der DACH Security erarbeitet.

Literatur

[BSI17] Bundesamt für Sicherheit in der Informationstechnik: "Die Lage der IT-Sicherheit in Deutschland 2017" https://www.bsi.bund.de/Lagebericht (abgerufen am 18. Juli 2018)

[BKA16] Bundeskriminalamt: „Bundeslagebild Cybercrime 2016“ https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html (abgerufen am 18. Juli 2018)

[Bitkom17] Bitkom: „Spionage, Sabotage, Datendiebstahl: Deutscher Wirtschaft entsteht jährlich ein Schaden von 55 Milliarden Euro“ https://www.bitkom.org/Presse/Presseinformation/Spionage-Sabotage-Datendiebstahl-Deutscher-Wirtschaft-entsteht-jaehrlich-ein-Schaden-von-55-Milliarden-Euro.html (abgerufen am 18. Juli 2018)

[BSI12] Bundesamt für Sicherheit in der Informationstechnik: „Cyber-Bedrohungen – ein Einstieg“ https://www.allianz-fuer-cybersicherheit.de/dok/6649744 (abgerufen am 19. Juli 2018)