Seminararbeit

Fachrichtung Wirtschaftsingenieurwesen

Ransomware

–

Von der Schadsoftware zum Geschäftsmodel

Erstellt von:	Luca Ernst Bauer Mat-Nr.: 101776 E-Mail: wing101776@fh-wedel.de
Erstellt im:	6. Fachsemester
Abgegeben am:	05.07.2018
Betreuender Dozent:	Prof. Dr. Michael Anders Fachhochschule Wedel Feldstraße 143 22880 Wedel Tel.: (04103) 8048-24 E-Mail: an@fh-wedel.de

Inhalt

1. Abkürzungsverzeichnis

BSI	Bundesamt für Sicherheit in der Informationstechnik
RW	Ransomware

2. Einleitung

Sie kommen abends von der Arbeit nach Hause und wollen noch schnell ein Foto ausdrucken. Der Laptop wird hochgefahren währen sie im Kopf schon planen, welches Foto sie auswählen möchten und wo sie es finden. Doch als Sie die Datei anklicken, um Sie zu öffnen, erscheint auf dem Bildschirm ein rotes Fester mit folgender Überschrift: „Ooops, your files have been encrypted!". Darunter folgt eine Erklärung, was mit dem Computer passiert ist, was man tun soll - eine Zahlung tätigen – und wie genau diese Zahlung erfolgen soll. Um den Druck noch weiter zu erhöhen, läuft neben der Zahlungsaufforderung eine Uhr runter, die angibt, bis wann die Gebühr zu zahlen ist. Sie können nichts an ihrem Laptop unternehmen und auch ein Neustart ermöglicht keine Verbesserung oder Veränderung des Problems.

Dieses Szenario, das frei erfunden ist, handelt von einem Angriff durch die Ransomware WannaCry[1]. WannaCry ist dabei nur eine spezielle Form von Ransomware, die im Jahr 2017 für sehr viel Aufsehen gesorgt hat. Der Begriff Ransomware besteht aus den zwei englischen Begriffen ransom (deutsch: Lösegeld) und malware (deutsch: Schadprogramm). Ransomware wird deshalb auch oft als Erpressersoftware bezeichnet, da der Zugriff des Opfers auf die Daten oder das System entweder eingeschränkt oder verhindert wird. Eine Freigabe wird nur gegen die Zahlung eines Lösegelds in Aussicht gestellt. [2] Viele Opfer sind bereit das geforderte Lösegeld zu zahlen, da der Leidensdruck so hoch ist.[3] Wurde das Geld bezahlt, werden die Daten und Programme nur selten entschlüsselt, daher rät der BSI davon ab, die geforderte Summe zu zahlen.[4] „Es ist wichtig, daran zu erinnern, dass Ransomware nicht eine Familie von Malware ist, sondern ein kriminelles Geschäftsmodell, bei dem bösartige Software verwendet wird"[5] – mit dieser Aussage von Thorsten Henning, Senior Systems Engineering Manager Central & Eastern Europe bei Palo Alto Networks wird verdeutlicht, dass Ransomware nur durch den Einsatz von Malware funktioniert, dass dahinter aber ein Geschäftsmodell steckt, welches sich bereits in der Welt der Cyberkriminalität etabliert hat. Ransomware betrifft dabei sowohl Desktop-Betriebssysteme wie Microsoft Windows, Server-Systeme unter Linux und Apple Mac OS als auch mobile Betriebssysteme wie iOS, Android und Windows.[6] Die Schadprogramme werden immer bedeutender in der IT-Sicherheit und greifen immer mehr Menschen an. Doch was macht Ransomware zu so einem erfolgreichen Konzept und inwiefern lässt sich eine Entwicklung in der Zukunft erkennen?

[1] (Briegleb, 2017)
[2] (Bundesamt für Sicherheit in der Informationstechnik, o. J.)
[3] (Bundesamt für Sicherheit in der Informationstechnik, o. J.)
[4] (Bundesamt für Sicherheit in der Informationstechnik, o. J.)
[5] (Hülsbömer, 2017)
[6] (Bundesamt für Sicherheit in der Informationstechnik, o. J.)

3. Geschichte

Ransomware ist ein Schadprogramm, das durch Erpressung den Betroffenen dazu verleiten möchte ein Lösegeld zu zahlen. Die Art der Erpressung variiert abhängig von der Art des Geräts (Computer, Laptop, Smartphone, etc.), des Betriebssystems (Windows, Mac OS, Android, etc.) und der Art, wie die Ransomware implementiert wird. Meist gelangt Ransomware, wie viele andere Schadprogramme auch, als E-Mail Anhang getarnt oder auf einer Internetseite implementiert auf das Gerät des Betroffenen.[7] Ransomware hat sich mit dem Fortschritt des Internets und der immer mehr vernetzten Welt weiterentwickelt. Heutzutage ist die Entwicklung von Ransomware kaum noch zu überblicken.

3.1 Die ersten Aufzeichnungen von Ransomware

Der erste dokumentierte Fall von Ransomware stammt aus dem Jahr 1989. Dabei handelt es sich um den „AIDS-Trojaner“, der auf einer Diskette an die 20.000 Teilnehmer der Welt-AIDS-Konferenz der Weltgesundheitsorganisation gesendet wurde. Mit dem einschieben der Diskette hat sich ein Programm auf den Computer aufgespielt, wodurch dieser sich infizierte. Beim 90. Systemstart hat das Programm die Verzeichnisse ausgeblendet und die Namen der Dateien verschlüsselt. Die Opfer wurden aufgefordert 189 US-Dollar an eine fiktive Firma zu senden um das System wieder frei zu geben. Der AIDS-Trojaner war noch sehr einfach zu entschlüsseln, da nur eine symmetrische Verschlüsselung zum Einsatz kam.[8]

Mit dem AIDS-Trojaner wurde sich die damalige Gesellschaft erstmals der Gefahr durch Ransomware bewusst und so hat sich auch der Begriff etabliert, für die Cyberkriminellen spielte das „Ransoming“ aber weiterhin kaum eine Rolle. In den neunziger Jahren und den frühen Zweitausendern war Malware eher ein Mittel um Streiche zu spielen oder mutwillig Schaden anzurichten um damit Aufmerksamkeit zu erlangen. Heute dagegen ist Malware ein Mittel der Cyberkriminellen um sich finanziell zu bereichern.

3.2 Der Beginn der asymmetrischen Verschlüsselung

Mit dem Beginn der Zweitausender Jahre entwickelte sich nicht nur das Internet und die Technologien weiter. Cyberkriminelle erkannten, dass diese Entwicklungen es einfacher machen, die Funktion des AIDS-Trojaners aufzugreifen, zu modifizieren und auf viel mehr Menschen anzuwenden.

[7] (Wolf, 2018)
[8] (Francis, 2016)

Im Jahr 2005 wurden erstmals Ransomware-Angriffe verzeichnet, bei denen dem Betroffenen ein Programm zum Entfernen von Schadsoftware verkauft werden sollte. Bei diesen Programmen handelte es sich oft um einen Schwindel, da die Programme keine Schadsoftware erkennen oder entfernen konnten.[9] Durch diesen Angriff ist eine Aufteilung in zwei Ausprägungen erkennbar, zum einen gibt es kryptografische Ransomware und zum anderen Scareware. Scareware ist ein Schadprogramm, welches für automatisiertes Social Engineering benutzt wird. Scareware spielt dem betroffenen als Pop-Up oder als Programm getarnt vor, dass auf dem Rechner eine bösartige Software entdeckt wurde. Es soll die kostenpflichtige Installation eines „Reinigungstools" oder die Hilfe per Telefondienst, was mit kostenpflichtigen Anrufen und eventuell der Preisgabe von vertraulichen Informationen verbunden ist, von den Betroffenen erzwungen werden.[10]

2006 wurden die ersten Ransomware-Attacken erkannt, die auf der Benutzung einer RSA-Verschlüsselung beruhten, dabei handelt es sich um ein asymmetrisches Verschlüsselungsverfahren. Der Archievus Trojaner verschlüsselte alle Daten im Ordner „Dokumente", zudem wurden die Betroffenen dazu aufgefordert, einen Artikel bei einem speziellen Online-Shop zu bestellen, um an das Passwort zur Entschlüsselung zu gelangen. Im selben Jahr wurde der GPCoder weiterentwickelt. 2005 wurde dieser als Jobangebot in einem Mailanhang getarnt und mit einem 660-Bit RSA Schlüssel versehen zu den Opfern geschickt, 2006 hat sich die Schlüssellänge der nun Gpcoder.AK genannten Ransomware auf 1024-Bit verstärkt. Diese Veränderung hat es für Betroffene umso schwerer gemacht die Daten wiederherzustellen. Der Schadcode hat Windows-Systeme infiziert und Dateien mit diversen Endungen ins Visier genommen. Von den Dateien wurde eine verschlüsselte Kopie erzeugt und das Original gelöscht. [11]

3.3 Die größten Angriffe durch Ransomware

In den letzten Jahren ab 2011 hat sich die Bedrohung durch Ransomware enorm erhöht, neue Familien wurden entdeckt von denen mehr und mehr Gefahr ausging, auch wurden bereits bekannte Codes weiterentwickelt. Die Verbreitung von anonymen Zahlungsmethoden wie etwa „Paysafecard" und „Kryptowährungen" machen es zunehmend interessanter für Cyberkriminelle sich dem Konzept der Ransomware zu bedienen. Die nächsten Jahre bis zum heutigen Tag sind geprägt durch fünf große Ransomware Attacken, die nicht nur Privatpersonen, sondern auch öffentliche Dienste und Organisationen betreffen.

[9] (Savage, Coogan, & Lau, 2015)
[10] (Hülsbömer, 2017)
[11] (Laffan, 2016)

Diese Entwicklung lässt sich auf der Abbildung 1 sehr gut nachvollziehen. Wurden im Jahr 2012 und 2013 nur wenige neue Varianten entdeckt, so scheint die Vielfalt an Ransomware in den Jahren 2015 und 2016 zu explodieren. Ransomware hat sich, durch sehr erfolgreiche Angriffe in den Jahren 2013 und 2014, von einem kleinen Nebengeschäft in ein lukratives Geschäftsmodell verwandelt, das immer mehr in den Fokus der Hacker gerät und dadurch so schnell wächst.

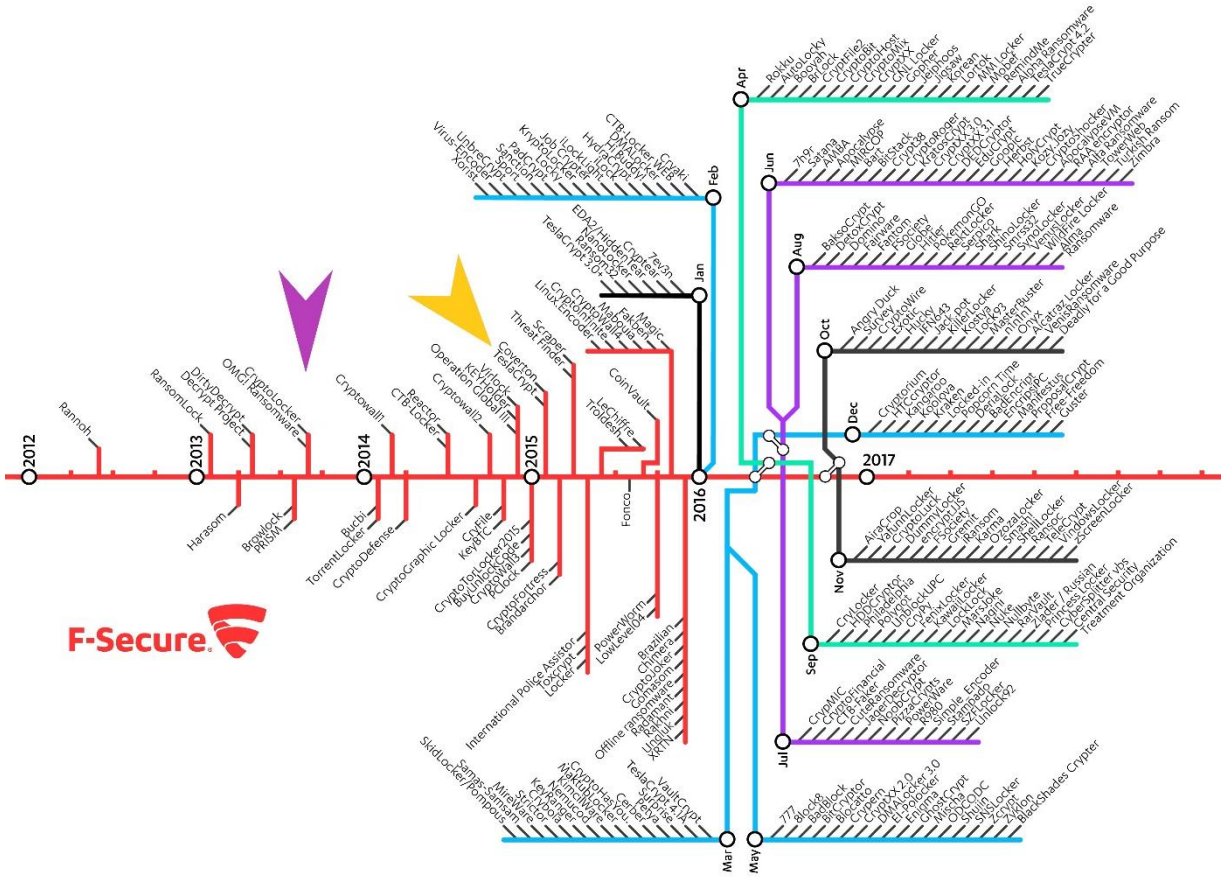

Abbildung 1: Die Entwicklung der Ransomware Varianten von 2012 – 2017
(Quelle: https://de.safeandsavvy.f-secure.com/2017/02/24/warum-ransomware-so-effektiv-ist/) ,09.06.2018

1. CryptoLocker war die erste Ransomware (als lila Pfeil in der Abbildung 1 gekennzeichnet), die auf internationaler Bühne für Aufsehen gesorgt hat. Über das Botnetz Gameover ZeuS, ein Netzwerk aus „Zombie“-Computern, speziell zur Verbreitung von Malware ins Leben gerufen, oder als Anhang von Spam-Mails verbreitete sich der Schädling. Zur Verschlüsselung der Daten nutze CryptoLocker RSA Public Key Encryption. Die Täter versteckten die privaten Schlüssel mithilfe von C2 -Servern im verborgenen Tor-Netzwerk. Gleichzeitig mit der Verschlüsselung kam eine Aufforderung zur Zahlung eines Geldbetrags, um den Schlüssel zur Entschlüsselung zu erhalten. Insgesamt erpressten Hacker rund drei Millionen Dollar mit CryptoLocker und

Abwandlungen, die auf dessen Code beruhten. CryptoLocker ist deshalb so wichtig für die Entwicklung der heutigen Ransomware, da der Code trotz seiner recht primitiven Gestaltung als Basis für viele andere Erpressungstrojaner dient. Im Mai 2014 hat ein internationaler Ermittlungstrupp das Botnetz Gameover ZeuS abgestellt, wodurch die Kommunikation zwischen dem C2-Server und dem CryptoLocker-Client unterbrochen wurde. Zudem konnte man die Datenbank mit den Private-Keys sicherstellen.[12]

2. Die nächste große Ransomware Attacke lies nicht lange auf sich warten, Anfang 2015 (als gelber Pfeil in Abbildung 1 gekennzeichnet) taucht TeslaCrypt auf dem Radar auf. Ursprüngliches Ziel der Erpressungstrojaner waren File-Erweiterungen (gespeicherte Spielstände, heruntergeladene Daten und Erweiterungen) bekannter Videospiele. TeslaCrypt wurde ständig weiterentwickelt und so waren bald alle lokal auf dem PC gespeicherten Dateien verschlüsselt. Zudem wurde 2016 eine Lücke geschlossen, die die Widerherstellung der Dateien ohne Schlüssel unmöglich machte.[13] Zudem soll es den Entwicklern in den ersten zwei Monaten $77,000 eingebracht haben, insgesamt mehr als $500,000.[14] TeslaCrypt ist im Jahr 2016 für 48 Prozent aller Ransomware-Attacken verantwortlich. Ende 2016 verkündeten die Hacker den Austritt aus dem Ransomware-Business und veröffentlichten den Schlüssel zur Entschlüsselung.[15]

3. Mit dem SimpleLocker hat das Zeitalter der mobilen Ransomware eingeläutet. Das Wahlsystem der Hacker lautet in diesem Fall „Android“. Auf dem Gerät werden die Daten verschlüsselt und in Geiselhaft genommen. Auch wenn die Zahl der Betroffenen relativ gering ausgefallen ist, so ist die Bedrohung dennoch real.[16]

4. Am 12. Mai 2017 beginnt die Ausbreitung von WannaCry, einer von zwei globalen Attacken Mitte 2017 durch Ransomware. Vier Tage nach Beginn verzeichnet der Sicherheitsanbieter Avast bereits 250.000 befallene Computer in 116 Ländern. Doch was WannaCry so besonders macht ist nicht die schnelle Verbreitung, sondern dass gestohlene Hacking-Tools der NSA zum Einsatz kommen. Es handelt sich hierbei um „EternalBlue“, einen Programmcode, der eine Schwachstelle im Windows-SMB-Protokoll ausnutzt. Bereits einen Monat zuvor hat Microsoft das Update für diese Schwachstelle bereitgestellt, Unternehmen und Institutionen sind aber, was die Updates

[12] (Maier & Fruhling, 2017); (Schneider, 2015)
[13] (Zaharia, 2015)
[14] (Liska & Gallo, 2016)
[15] (Maier & Fruhling, 2017)
[16] (Maier & Fruhling, 2017)

des Systems angeht, oft sehr langsam. WannaCry besteht dabei aus zwei Bestandteilen, zum einen die Ransomware an sich, zum anderen aus einem Wurm, wodurch sich die Schadsoftware so schnell verbreiten konnte.[17]

5. Direkt nach dem WannaCry-Angriff, am 27. Juni, folgte NotPetya (auch als Petya bekannt) und machte deutlich, wie ernst die Bedrohung durch Ransomware ist. Infiziert wird man nicht, wie bei dem Vorläufer „Goldeneye", durch Dateianhänge in Mails oder Web-Seiten mit Exploits. Der Angriff erfolgte über den Update-Mechanismus einer legitimen Software, wodurch der Schädling ins Netz gelangte. Dort breitet er sich mit Methoden weiter aus, die eher von gezielten Spionage-Angriffen bekannt sind. Auch kam ein modifiziertes „EternalBlue"-Exploit zum Einsatz. Auf dem System überschrieb der Schädling, wie auch der ursprüngliche Petya, Teile des Master Boot Records und verschlüsselte Dateien mit wichtigen Daten. Hauptregion der Angriffe sind die Ukraine und Russland. Petya hat nicht so viele Leute wie WannaCry angegriffen, es sind aber mehr Unternehmen, Krankenhäuser und Regierungsinstitutionen darunter, die zum Teil nicht arbeiten konnten. Die Hacker scheinen es nicht auf Geld abgesehen zu haben, denn auch wenn eine Entschlüsselung gegen Geld angeboten wurde, so wurde von Sicherheitsforschern festgestellt, dass man die angerichteten Schäden gar nicht reparieren könnte. NotPetya überschreibt Teile des MBR irreversibel, außerdem wird für die infizierten PCs keine persönliche ID vergeben, so kann zur Entschlüsselung dem PC kein Schlüssel zugeordnet werden.

Heute noch sind Ransomware-Attacken präsent, wie ein Krankenhaus im US-Bundesstaat Indiana erfahren musste. Trotz Backups musste das Krankenhau 60.000 US-Dollar an Erpresser zahlen, um den Betrieb wieder aufnehmen zu können.[18] Grund für die starke Bedrohung ist nicht nur die Vielzahl an Varianten und Familien, die stetig wächst, sondern auch das Angebot um Ransomware zu „bauen". Man muss längst kein Erfahrener Hacker mehr sein um sich ein solches Schadprogramm zusammen zu schreiben. Im Internet lassen sich bereits seit 2015 „built-your-own" Ransomware Baukästen finden, wie Beispielsweise „Tox". Die Software ist kostenlos, es müssen lediglich 20% von erfolgreich durchgeführten Angriffen an die Entwickler abgegeben werden.[19]

[17] (Maier & Fruhling, 2017)
[18] (Gierow, 2018)
[19] (Khandelwal, 2015)

4. Typen von Ransomware

Jeden Tag tauchen neue Ransomware-Arten auf, es ist daher schwer zu sagen, wie viele es insgesamt gibt und was diese genau bewirken. Grob kann man aber vier verschiedene Arten unterscheiden, abhängig davon, wie die Schadsoftware wirkt und welche Systeme diese attackieren soll. Dabei gibt es welche, die Dateien verschlüsseln, solche, die Dateien löschen, mobile Ransomware und welche, die Dateien sperren.

4.1 Verschlüsselungs-Ransomware

Das Schadprogramm verschlüsselt persönliche Dateien und Ordner (Bilder, Videos, Dokumente). Zur Verschlüsselung wurde in den Anfängen ein symmetrischer Schlüssel-Algorithmus verwendet, dieser wurde von der Benutzung eines öffentlichen Schlüssels abgelöst. Heute nutzt Ransomware eine Kombination aus symmetrischen und öffentlichen Schlüsseln zur Verschlüsselung. Da es zu Zeitintensiv wäre, alles mit einem asymmetrischen Schlüssel zu verschlüsseln, wird zur Verschlüsselung der Dateien das symmetrische Verfahren verwendet und zur Verschlüsselung der Schlüssel das Asymmetrische. Der Betroffene bemerkt die Verschlüsselung oft erst, wenn er versucht, die Daten zu öffnen. Entweder geht daraufhin ein Sperrbildschirm auf oder aber es befindet sich eine Textdatei im betroffenen Ordner. In beiden Fällen wird zur Zahlung einer Summe in einer bestimmten Zeit aufgefordert.[20]

4.2 Lösch-Ransomware

Diese Variante läuft analog zur Verschlüsselungs-Variante ab bis zu dem Punkt, an dem der Betroffene zur Zahlung aufgefordert wird. Neben einer Zahlungsaufforderung wird auch damit gedroht, dass die Daten gelöscht werden, sollte das Opfer selbst versuchen diese zu entschlüsseln. Sollten die Daten aber vernichtet werden, so geht man davon aus, dass man diese auf der Festplatte nicht mehr auffinden kann. Forscher haben aber herausgefunden, dass die Daten lediglich als gelöscht in der internen Datenbank (NTFS Master File Table) angezeigt werden, auf der Festplatte aber noch vorhanden sind.[21]

4.3 Sperrbildschirm Ransomware – WinLocker

Diese Art von Ransomware sperrt, wie der Name bereits verrät, den Bildschirm und verlangt eine Zahlung um diesen wieder frei zugeben. Auf dem Computer wird ein Vollbild-Bild

[20] (No More Ransom, Ransomware Q&A, 2018); (Lin, 2016)
[21] (No More Ransom, Ransomware Q&A, 2018); (Lin, 2016)

präsentiert, wodurch auch alle anderen Fenster blockiert sind. Die Sperrung ist von den Erpressern so designt, dass mutmaßlich die Regierung (FBI, örtliche Polizei, o.Ä.) dafür verantwortlich ist. Dahinter steckt aber nur eine Social Engineering Masche, um das Opfer in Bedrängnis zu bringen und zur Zahlung zu animieren. Die persönlichen Dateien bleiben meist aber unverschlüsselt.[22]

4.4 Mobile Ransomware (Andoid)

Durch unabsichtliches Herunterladen von Software, auch bekannt als „Drive-by-Downloads", lassen sich Mobile Geräte, meist mit dem Betriebssystem Android, infizieren. Auf dem Bildschirm erscheint ein Fenster mit der Information, dass das Gerät gesperrt wurde und man in einer bestimmten Zeit einer Zahlungsaufforderung nachkommen solle zum Entsperren.[23]

5. Wie gelangt Ransomware auf mein System?

Ransomware kann auf verschiedene Arten auf den Computer gelangen. Dabei werden die Hacker immer ausgefallener und lassen sich neue Wege einfallen, um in das System des Opfers eindringen zu können. Bei der Art und Weise spielen dazu auch das Betriebssystem und natürlich die Art von Gerät eine wichtige Rolle. So sind für mobile Geräte meist andere Wege zu wählen als für Computer, da einfach andere Anwendungen verwendet werden und das User -Verhalten sich von Gerät zu Gerät unterscheidet.

5.1 Spam

Der Angriff per Spam erfolgt meist auf Grundlage von professionellem Social Engineering. Das bedeutet, dass das Opfer zwischenmenschlich beeinflusst wird, um eine bestimmte Verhaltensweise hervorzurufen. Im Fall von Ransomware soll das Opfer dazu bewegt werden, den E-Mail-Anhang zu öffnen. So werden angebliche Rechnungen, Bestellbestätigungen, eingescannte Dokumente, usw. versendet, teilweise unter der Verwendung von echten Firmennamen und -adresse, die soweit perfektioniert sind, dass zum Original kaum ein Unterschied zu erkennen ist. Im Anhang befindet sich meistens ein sogenannter Downloader, dabei handelt es sich um ein Programm, das mit Aktivierung die eigentliche Schadsoftware nachlädt. Die Schadsoftware wird auf einem Server gehostet, auf den der Downloader zugreift. So kann die Schadsoftware immer auf dem aktuellen Stand gehalten werden, ohne dass man dazu immer den Mail-Anhang ändern muss.[24]

[22] (No More Ransom, Ransomware Q&A, 2018); (Lin, 2016)
[23] (No More Ransom, Ransomware Q&A, 2018); (Lin, 2016)
[24] (Bundesamt für Sicherheit in der Informationstechnik, 2016)

5.2 Drive-By Infektionen durch Exploit-Kits

Einen weiteren Infektionsvektor für Ransomware stellen Exploit-Kits dar.

Bei einem Exploit handelt es sich um kleine Programme, die auf dem Computer nach Sicherheitslücken suchen und ausnutzen.

Abbildung 2: Ablauf eines Exploit-Angriffs (Quelle: https://www.gdata.de/ratgeber/was-ist-eigentlich-ein-exploit) ,23.06.2018

Ein Angriff läuft in fünf Schritten ab, wie in Abbildung 2 zu sehen ist:

1. Exploits werden beispielsweise in einem Word-Dokument versteckt oder als „Drive-By-Download“ beim Besuchen einer Webseite ohne das Wissen des Opfers heruntergeladen. In dem Programm, in dem die Exploits geöffnet wurden (in diesen Fällen Word und der Browser), suchen Sie nach angreifbaren Punkten.
2. Ist eine Schwachstelle infiziert, wird im Arbeitsspeicher des Computers ein schädlicher Code platziert.
3. Über den Programmcode wird der genaue Ablauf der Prozessschritte im Programm angegeben. Exploits ändern die ursprüngliche Arbeitsfolge so, dass der Programmfluss auf den manipulierten Code gelenkt wird. Dadurch wird der vorher eingeschleuste Schadcode ausgeführt und nicht der eigentliche Programmcode.
4. Der aktive Schadcode kann die Funktionen des Programms und die damit verbundenen allgemein zugänglichen Betriebssystem-Funktionen aufrufen. Es können so Informationen über das System gesammelt werden und Schadsoftware kann aus dem Internet nachladen.
5. Auf diesem Weg landet Ransomware auf dem Computer.[25]

Seit mehreren Jahren werden dabei Zero-Day-Exploits (Exploits, die erscheinen, bevor ein Patch für die Sicherheitslücke) oder Exploits für neue Schwachstellen in weit verbreiteten Programmen in sehr kurzer Zeit in Exploit-Kits integriert. Diese Methode wird nicht nur zur

[25] (G DATA Ratgeber, 2018)

Infektion, sondern auch zur Verteilung von Ransomware verwendet. Über Drive-By -Infektionen werden die Exploit-Kits auf kompromittierten Webseiten oder Werbebannern verbreitet. Die Ransomware oder andere Schadsoftware wird danach nachgeladen.[26]

5.3 Schwachstellen in Servern

Weist ein Webserver eine Schwachstelle auf, so wird diese gnadenlos ausgenutzt. Über diese wird der Webserver infiziert und daraufhin die Inhalte des Web-Auftritts verschlüsselt.[27]

5.4 Infizierung durch ungeschützte Fernwartungszugänge

Es gibt Systeme mit Programmen, wie etwa Microsoft Remote-Desktop oder Teamviewer, die Fernwartungszugänge ins Internet anbieten. Die Täter Suchen im Internet gezielt nach solchen Systemen, führen Brute-Force-Angriffe auf das benötigte Passwort durch und installieren bei einem erfolgreichen Login eine Ransomware-Malware. Dieser Infektionsvektor wurde aber nur in einigen Fällen mit der Ransomware GPCode durchgeführt.[28]

5.5 Mobile Ransomware

Für mobile Ransomware gibt es spezielle Formen, um sich zu infizieren. So können beim Download von Apps, die nicht aus dem offiziellen Stores kommen, Ransomware Downloader als Drive-By-Download mit heruntergeladen werden. Das ist bei offiziellen Geräten nur bei Android der Fall, Apple-Gerät sind so lange sicher, bis man sich zu einem Jailbreak entschließt, dadurch können auch auf einem iPhone/iPad Inhalte aus anderen Quellen als dem App-Store bezogen werden. Für mobile Ransomware stellen aber auch die meisten oben genannten Infizierungsvektoren eine Gefahr dar.

6. Ablauf einer Infizierung

Eine Ransomware-Attacke kann in fünf Schritte aufgeteilt werden. Die Schritte beginnen mit der Installation und enden mit der Geldforderung.

[26] (Bundesamt für Sicherheit in der Informationstechnik, 2016)
[27] (Bundesamt für Sicherheit in der Informationstechnik, 2016)
[28] (Bundesamt für Sicherheit in der Informationstechnik, 2016)

6.1 Schritt 1: Installation

Hat ein Opfer das System über eine der in 5. genannten Möglichkeiten mit einer Schadsoftware, in diesem Fall Ransomware, infiziert, beginnt die Krypto-Ransomware sich selbst zu installieren. Im Windows Register werden Schlüssel eingegeben, damit die Ransomware sich mit jedem Systemstart automatisch mitstartet.[29]

6.2 Schritt 2: Server kontaktieren

Bevor die Ransomware das System attackiert, stellt sie einen Kontakt zum Server her, der von den Tätern betrieben wird.[30]

6.3 Schritt 3: Handschlag und Schlüsselerstellung

Mit Hilfe eines Prozesses mit dem Namen „Handshake“ wird zwischen dem Ransomware Client und dem Server eine Authentifizierung durchgeführt. Daraufhin erstellt der Server zwei kryptografische Schlüssel, der eine wird auf dem System des Opfers deponiert, der andere auf dem Server des Täters.[31]

6.4 Schritt 4: Verschlüsselung

Sind die Schlüssel generiert, beginnt die Ransomware mit der Suche nach Dateien und der Verschlüsselung. Welche Dateien verschlüsselt werden und nach welchem Verfahren ist von Fall zu Fall unterschiedlich.[32]

6.5 Schritt 5: Erpressung

Auf dem System des Opfers erscheint auf dem Bildschirm ein Fenster oder eine Textdatei, auf der die Zeit runter läuft und die Täter damit drohen, den zur Entschlüsselung benötigten Schlüssel zu zerstören, wenn in der angegebenen Zeit ein Lösegeld nicht gezahlt wird. Das Lösegeld soll meistens in Bitcoins oder einer anderen elektronischen Währung gezahlt werden, die nicht nachverfolgbar ist. Die Beträge, die zu zahlen sind, liegen in einer Höhe von $300 bis $500.[33]

[29] (Salvi & V.Kerkar, 2017)
[30] (Salvi & V.Kerkar, 2017)
[31] (Salvi & V.Kerkar, 2017)
[32] (Salvi & V.Kerkar, 2017)
[33] (Salvi & V.Kerkar, 2017)

7. Schutz vor einer Infizierung

Es ist wichtig, sich im Klaren darüber zu sein, wie Ransomware und auch andere Schadprogramme sich Zugang auf ein System verschaffen können. Nur so kann man die Wege (??) blockieren oder beobachten und sich so vor einer Infizierung schützen. Es muss dazu gesagt werden, dass es keinen vollkommenen Schutz gibt. So wie sich die Technik weiterentwickelt, wird es immer neue Wege für die Täter geben um sich einen Zugang auf das System des Opfers zu verschaffen.

7.1 Datensicherung

Es ist von höchster Priorität, eine regelmäßige Datensicherung zu machen. Es empfiehlt sich dafür zwei Backup-Kopien zu erstellen. Eine wird in einer Cloud gespeichert, die andere Kopie sollte auf einem externen Datenträger (tragbare Festplatte, USB-Stick, etc.) gespeichert werden. Der externe Datenträger sollte in jedem Fall nach der Sicherung vom Computer getrennt werden um eine Infizierung des externen Datenträgers zu verhindern. [34]

7.2 Antivirensoftware

Es sollte in jedem Fall eine aktuelle, vertrauenswürdige Antivirensoftware auf dem System installiert sein. Die „heuristischen Funktionen“ müssen eingeschaltet werden, da diese helfen, Ransomware-Varianten zu erfassen, die noch nicht formell aufgenommen wurden.[35]

7.3 Aktualisierungen beachten

Wie man am Beispiel WannaCry und Petya sehen kann, ist es wichtig, sein System stets auf dem aktuellen Stand zu halten. Die größte Gefahr geht von Anwendungen aus, die Inhalte aus dem Internet herunterladen oder öffnen. Bietet ein Betriebssystem oder eine Anwendung eine neue Version zur Freigabe an, installieren Sie die Updates. Auch bieten mehrere Softwares die Möglichkeit einer automatischen Aktualisierung. Auch diese sollte man nutzen.[36]

7.4 Angriffsfläche minimieren

Je mehr Programme zum Öffnen von unbekannten Inhalten auf dem System zur Verfügung stehen, desto höher ist die Gefahr einer Infektion. Nicht benötigte Software sollte daher deinstalliert werden. In Web-Browsern sollte nicht zwingend benötigte Browser-Plugins (z.B.

[34] (No More Ransom, Tipps zur Vorbeugung, 2018)
[35] (No More Ransom, Tipps zur Vorbeugung, 2018)
[36] (No More Ransom, Tipps zur Vorbeugung, 2018); (Bundesamt für Sicherheit in der Informationstechnik, 2016)

Java, Flash) entfernt sowie die Ausführung aktiver Inhalte, wenn möglich, eingeschränkt werden (z.B. Click-to-Play).[37]

7.5 E-Mails richtig behandeln

Heutzutage werden E-Mails häufig als HTML-E-Mails versendet. Um diese im E-Mail-Programm korrekt darzustellen, nutzen E-Mail-Clients die gleichen Mechanismen zur Darstellung wie der Web-Browser. Die Darstellung verlangt eine große Zahl an Komponenten und Funktionen ab, die im Web-Browser durch zusätzliche Sicherheitsmaßnahmen eingedämmt werden, im E-Mail-Programm in der Regel aber nicht. Um die Zahl der Komponenten und Funktionen zu minimieren, sollten daher die E-Mails nur als Text dargestellt werden (oft als „Nur-Text“ bzw. „reiner Text“ bezeichnet anstatt als „HTML-Mail“). Diese Darstellungsweise verhindert zudem die Verschleierung von Webadressen (in der HTML-Darstellung könnte ein Link mit der Bezeichnung „www.fh-wedel.de“ z.B. in Wahrheit auf die Adresse „www.schadsoftware.de“ verweisen). Möchte man die HTML-Darstellung nicht ausstellen, so sollte mindestens die Ausführung aktiver Inhalte bei Verwendung von HTML -Mails unterdrückt sein. Schadhafte Skripte können somit nicht mehr ausgeführt werden.
Ein weiterer Aspekt ist die Filterung von Spam-Emails. Bietet ein E-Mail-Programm die Möglichkeit, den Filtern zu justieren, so sollten alle Mails mit ausführbaren Anhängen, verschlüsselte Archive / Zip-Dateien und MS-Office-Dokumente-Makros blockiert oder zumindest in Quarantäne verschoben werden.[38]

7.6 „Dateierweiterungen anzeigen“ aktivieren

In den Windows-Einstellungen auf kann man die Option „Dateierweiterungen anzeigen“ finden, diese sollte man aktivieren. Mit Aktivierung dieser Option lassen sich die Dateierweiterungen jeder Datei ansehen, dadurch ist es viel einfacher, potenziell schädliche Dateien zu erkennen. Es ist davon abzuraten, auf Dateierweiterungen wie „.exe“, „.vbs“, „.scr“ zu klicken. Auch sind doppelte Erweiterungen wie „.avi.exe“ oder „.doc.scr“ auch Hinweise darauf, dass es sich bei dieser Datei um eine potenzielle Schadsoftware handelt.

7.7 Vertrauen Sie niemandem

E-Mail Anhänge von unbekannten Personen sollten nicht geöffnet werden, da Cyberkriminelle oft E-Mails versenden, die wie E-Mail-Benachrichtigungen von einer Bank, der Polizei, dem Gericht oder der Steuerbehörde aussehen. Durch dieses Social Engineering soll der Empfänger dazu verleitet werden auf einen böswilligen Link zu klicken, wodurch eine Malware installiert

[37] (Bundesamt für Sicherheit in der Informationstechnik, 2016)
[38] (Bundesamt für Sicherheit in der Informationstechnik, 2016)

werden kann. Vorsicht ist aber nicht nur bei fremden E-Mail-Benachrichtigungen geboten. Es kann jedes Konto kompromittiert werden, was dazu führen kann, dass von den Konten von Freunden in sozialen Netzwerken oder Gaming-Partnern bösartige Links gesendet werden. Klicken Sie diese nur an, wenn Sie sich absolut sicher sein können, dass der Inhalt beabsichtigt geschickt wurde und für Sie bestimmt ist. Der Nachteil an den Anwendungen, die die Breite Masse der Bevölkerung im Internet nutzt, ist die Unwissenheit über die Personen, mit der man kommuniziert. Sobald etwas auffällig erscheint und nicht in das normale Bild passt, sollte Vorsicht geboten sein. Ganz nach dem Motto: „Vertrauen ist gut, Kontrolle ist besser!“[39]

8. Was ist zu tun, wenn man infiziert wurde?

Sollte man sich doch mit einer Ransomware infizieren, so ist es wichtig, die nächsten Schritte in Ruhe zu planen und vorsichtig anzugehen. Im Fall von Ransomware handelt es sich, wie der Name bereits sagt, um eine Lösegelderpressung. Ob man das Lösegeld zahlt, ist jedem selbst überlassen, das BSI, Antivirenanbieter und IT-Experten raten von der Zahlung des Lösegeldes aber ab. Zum einen bestärkt man die Erpresser durch eine Zahlung in ihren bösen Absichten und gibt ihnen die Bestätigung für den Erfolg des Angriffs, wodurch die Angreifer weiter motiviert werden und die finanziellen Mittel zur Weiterentwicklung der Schadsoftware besitzen. Zum anderen gibt es keine Garantie, dass durch die Zahlung des Lösegeldes auch ein Entschlüsselungsschlüssel von den Erpressern geschickt wird oder dass dieser, wenn er geschickt wird, funktioniert. So geht aus dem „Kaspersky Security Bulletin: Story of the year 2017” hervor, dass eine von sechs Personen, die der Lösegeldforderung nachgekommen ist, Ihre Daten niemals entschlüsseln konnte.[40]

Am wichtigsten ist es aber zunächst, das betroffene System vom Netzwerk zu trennen. Das bedeutet, das Netzwerkkabel zu ziehen und alle vom Gerät benutzten WLAN-Adapter abzuschalten.

Die erste Anlaufstelle sollte die Website „The No More Ransom Project“ sein. Hierbei handelt es sich um eine Initiative der National High-Tech Crime Unit der niederländischen Polizei, Europols europäischem Cybercrime Center und zwei Cyber Security Unternehmen, Kaspersky Lab und McAfee. Ziel der Initiative ist es, von Ransomware Betroffenen bei der Entschlüsselung zu helfen ohne Lösegeld zu zahlen.[41] Findet man auf der Seite keine Hilfe, so kann man folgende Schritte einleiten:

[39] (No More Ransom, Tipps zur Vorbeugung, 2018)
[40] (Kaspersky Lab GmbH, 2017);
[41] (No More Ransom, Über das Projekt, 2018)

- Hat man durch den Angriff keine wichtigen Daten verloren, so lässt sich einfach eine Neuinstallation des Systems von einem vertrauenswürdigen Datenträger durchführen.
- Sind wichtige Daten verloren gegangen, die aber zuvor auf einer Datensicherung gesichert wurden, lassen sich diese einfach auf das neue System spielen.
- Ist keine Datensicherung vorhanden und wichtige Dateien sind verschwunden, hilft nur noch die Konsultierung eines Experten.

Der Ransomware-Angriff sollte zudem als Strafanzeige bei der Polizei aufgegeben werden. Die Polizei hat viele Möglichkeiten, die Unternehmen nicht haben, so kann z.B. der Fluss gezahlter Lösegelder nachverfolgt oder aus dem Ausland agierende Täter verfolgt werden. Nur auf diesem Wege kann man dem Geschäftsmodell Ransomware erfolgreich entgegentreten. [42]

Ergebnis

Ransomware hat einen Entwicklungsprozess von fast 30 Jahren hinter sich. Zu Beginn war die Art und Weise, wie man mit Ransomware seine Opfer erpressen konnte, nicht sehr rentabel. Das lag vor allem an mehreren Faktoren, die zu dieser Zeit noch ein Hindernis darstellten. Die Technologie und das Internet waren noch nicht weit ausgebaut, kaum eine Privatperson hatte einen eigenen Computer und noch weniger einen Laptop. Damit war die Möglichkeit, Privatpersonen zu erpressen sehr eingeschränkt. Außerdem war es sehr aufwendig die Schadsoftware zu verbreiten. 1989 verbreitete sich der AIDS-Trojaner zwar auf bis zu 20.000 Computer, trotzdem mussten dazu 20.000 Floppy-Discs mit der Malware infiziert und verteilt werden. Das war in diesem Maße nur schwer zu bewerkstelligen und kein Mittel für die breite Masse der Cyberkriminellen.

Mit der Ausbreitung des Internets und der Entwicklung in der Technologie ist es viel einfacher geworden Malware, in diesem Fall Ransomware, zu versenden. Als Mailanhang getarnt oder durch das Ausnutzen von Schwachstellen im Code eines Betriebssystems ist die Verbreitung von Malware viel einfacher und in einem größeren Ausmaß zu bewerkstelligen. Dazu kommen noch mehr verschiedene Geräte, die sich durch Ransomware infizieren lassen. Außer Computern lassen sich heutzutage Smartphones, Tablets, Laptops und auch die verschiedenen Cloudspeicher angreifen. Möchte man einen Code für die Erstellung einer Ransomware schreiben, so ist man nicht mehr auf ausgeprägte Programmierkenntnisse angewiesen. Im sogenannten Dark Web finden sich mehrere Baukästen dazu und die Anleitung, wie man diesen einsetzt. Die Verfügbarkeit von anonymen und einfach zu

[42] (Bundesamt für Sicherheit in der Informationstechnik, 2016)

benutzenden Zahlungsmitteln erklärt auch, warum Ransomware zu so einer populären Methode geworden ist. Vor allem Kryptowährungen, wie aktuell Bitcoin, machen es den Betrügern sehr einfach, die Zahlungsmittelbewegungen zu verschleiern und so nicht auffindbar zu sein.

Ransomware ist daher lange keine einfache Malware mehr. Cyberkriminelle haben mit diesem Mittel einen neuen Geschäftszweig für sich entdeckt. Wie sich anhand der aktuelleren Fälle erkennen lässt, entwickelt sich das Beuteschema der Kriminellen weg von den Privatpersonen hin zu großen Firmen und vor allem öffentlichen Organisationen und Unternehmen wie z.B. Krankenhäusern. Bei Privatpersonen bringt der Verlust von persönlichen Daten oft nur Ärger und Umstände mit sich, großen Unternehmen droht dadurch aber im schlimmsten Fall ein großer Umsatz- oder Kapitalverlust. Daher sind diese auch manchmal bereit, das geforderte Lösegeld zu zahlen, damit der tägliche Betrieb schnell wieder aufgenommen werden kann, wie es beispielsweise in einem Krankenhaus in den USA der Fall war. [43]

[43] (Gierow, 2018)

Literaturverzeichnis

Briegleb, V. (13. Mai 2017). *WannaCry: Was wir bisher über die Ransomware Attacke wissen*. Abgerufen am 13. April 2018 von heise.de: https://www.heise.de/newsticker/meldung/WannaCry-Was-wir-bisher-ueber-die-Ransomware-Attacke-wissen-3713502.html

Bundesamt für Sicherheit in der Informationstechnik. (2016). *Ransomware - Bedrohungslage, Prävention & Reaktion.* (N. IT-Lagezentrum, Hrsg.) Abgerufen am 04. April 2018 von bsi.bund.de: https://www.bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik. (o. J.). *Ransomware*. Abgerufen am 12. April 2018 von bsi-fuer-buerger.de: https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/Schadprogramme/Ransomware/ransomware_node.html

Francis, R. (20. Juli 2016). *The history of ransomware*. Abgerufen am 15. April 2018 von csoonline: https://www.csoonline.com/article/3095956/data-breach/the-history-of-ransomware.html

G DATA Ratgeber. (23. 06 2018). *Was ist eigentlich ein Exploit?* Abgerufen am 23. 06 2018 von G DATA Software AG: https://www.gdata.de/ratgeber/was-ist-eigentlich-ein-exploit

Gierow, H. (17. Januar 2018). *Ransomware - Krankenhaus zahlt 60.000 US-Dollar trotz Backups*. Abgerufen am 10. April 2018 von golem.de: https://www.golem.de/news/ransomware-krankenhaus-zahlte-60-000-us-dollar-trotz-backups-1801-132206.html

Hülsbömer, S. (31. Oktober 2017). *FAQ Ransomware - Fragen und Antworten*. Abgerufen am 29. März 2018 von computerwoche: https://www.computerwoche.de/a/faq-ransomware-fragen-und-antworten,3228721

Kaspersky Lab GmbH. (2017). *Kaspersky Security Bulletin: Story of the year 2017.* Ingolstadt: Kaspersky Lab GmbH. Abgerufen am 20. 06 2018 von https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07164824/KSB_Story_of_the_Year_Ransomware_FINAL_eng.pdf

Khandelwal, S. (29. 05 2015). *"Tox" Offers Free build-your-own Ransomware Malware Toolkit*. Abgerufen am 17. 06 2018 von thehackernews.com: https://thehackernews.com/2015/05/ransomware-creator.html

Laffan, K. (18. Mai 2016). *A Brief History of Ransomware*. Abgerufen am 15. April 2018 von Varonis: https://blog.varonis.com/a-brief-history-of-ransomware/

Lin, D. (29. 03 2016). *Ransomware - Teil2, Die wichtigesten Typen von Ransomware und welche Art von Verschlüsselung sie benutzt*. Abgerufen am 16. 06 2018 von varonis.de: https://blog.varonis.de/ransomware-teil-2-die-wichtigsten-typen-von-ransomware-und-welche-art-von-verschlusselung-sie-benutzen/

Liska, A., & Gallo, T. (2016). *Ransomware - Defending Against Ditorsion.* Sebastopol, CA, United States of America: O'Reilly Media.

Maier, J., & Fruhling, F. (04. 08 2017). *Von Hackern erpresst - Die 5 größten Ransomware-Attacken*. Abgerufen am 09. 06 2018 von www.computerwoche.de: https://www.computerwoche.de/a/die-5-groessten-ransomware-attacken,3331319

No More Ransom. (04. 06 2018). *Ransomware Q&A*. Abgerufen am 14. 06 2018 von No More Ransom: https://www.nomoreransom.rog/de/ransomware-qa.html

No More Ransom. (15. 06 2018). *Tipps zur Vorbeugung*. Abgerufen am 17. 06 2018 von No More Ransom: https://www.nomoreransom.org/de/prevention-advice.html

No More Ransom. (15. 06 2018). *Über das Projekt*. Abgerufen am 20. 06 2018 von No More Ransom: https://www.nomoreransom.org/de/about-the-project.html

Salvi, H. U., & V.Kerkar, R. (17. 12 2017). Ransomware: A Cyber Extortion. *Asian Journal of Convergence in Technology (AJCT) - UGC Listed, 2(2)*. Abgerufen am 17. 06 2018 von https://doi.org/https://doi.org/10.1212/ajct.v2i2.55

Savage, K., Coogan, P., & Lau, H. (06. August 2015). *The evolution of ransomware.* (Symantec, Hrsg.) Abgerufen am 12. April 2018 von symantec: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf

Schneider, M. (10. 12 2015). *Ransomware Grundlagen.* Abgerufen am 21. 06 2018 von scip: https://www.scip.ch/?labs.20151210

Wolf, J. (2018). *Ransomware Detection.* Friedrich-Alexander-Universität, Erlangen-Nuremberg. Abgerufen am 12. April 2018 von https://julian-wolf.eu/doc/en/ransomware_detection.pdf

Zaharia, A. (11. 11 2015). *Security Alert_: TeslaCrypt Infections Rise, Git Eurpean Companies.* Abgerufen am 14. 06 2018 von heimdalsecurity.de: https://heimdalsecurity.com/blog/security-alert-teslacrypt-infections-rise-spam-campaign-hits-companies-europe/