UNIVERSITY OF APPLIED SCIENCES

Fachbereich Informatik

Seminar IT-Sicherheit

Ransomware

Wintersemester 2017/2018

Eingereicht am:

29. November 2017

Eingereicht von:
Simon Nimmerjahn
Student IT-Sicherheit
E-mail: its103282@fh-wedel.de

Betreuer:
Prof. Dr. Gerd Beuster
Fachhochschule Wedel
Feldstraße 143
22880 Wedel
Tel.: 04103 - 80 48 - 38
E-Mail: gb@fh-wedel.de

Inhaltsverzeichnis

Abkürzungsverzeichnis

BSI Bundesamt für Sicherheit in der Informationstechnik

NHS National Health Service

RaaS Ransomware as a Service

BKA Bundeskriminalamt

1 Einführung

1.1 Motivation

In diesem Jahr haben gleich mehrere große Ransomware-Attacken viele Privatpersonen und Unternehmen massiv getroffen. Bei der deutschen Bahn fielen die Anzeigetafeln aus [Bri], die Reederei Maersk konnte ihre Schiffe nicht mehr be- und entladen [GP] und Beiersdorf musste ganze Produktionsstandorte herunterfahren.[NDR] Das sind nur einige Beispiele dafür, wie stark und unvorbereitet Ransomware-Attacken Unternehmen getroffen haben. Bei den genannten Beispielen führten solche Angriffe zu erheblichen finanziellen Verlusten bei den betroffenen Unternehmen. Es gibt allerdings auch mehrere Fälle, in denen Krankenhäuser von solchen Attacken betroffen waren.[Bor] In diesen Fällen treten die finanziellen Aspekte in den Hintergrund. Vielmehr besteht die Gefahr, dass medizinische Geräte ausfallen und notwendige Operationen nicht durchgeführt werden können. In dieser Situation wird ein Angriff auf Computersysteme zu einer Gefahr für Menschenleben. Es ist daher unverzichtbar, dass in allen Bereichen das Thema IT-Sicherheit ernst genommen wird. Auch ist es wichtig die Hintergründe und Vorgehensweisen der Angreifer zu verstehen. Ziel dieser Arbeit ist es daher, einen Überblick über das Thema Ransomware zu bekommen um mögliche Angriffe besser zu verstehen und Gegenmaßnahmen ergreifen zu können.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) befragt zum Ende eines jeden Jahres deutsche Institutionen zum Thema IT-Sicherheit.[fSidI] Im Jahr 2016 haben bei dieser Umfrage 331 Institutionen teilgenommen. Es kam heraus, dass 65,5% der Befragten von einem Cyber-Angriff betroffen waren. Allerdings waren diese nur bei 47% der Befragten erfolgreich. Bei 32% aller Institutionen wurde eine Infektion durch Ransomware festgestellt. Des Weiteren kam in der Umfrage heraus, dass über 60% der Institutionen das größte Bedrohungspotenzial bei Ransomware-Attacken sehen. Diese Umfrage wurde vor den zuvor beschriebenen Attacken auf Unternehmen durchgeführt. Die Befürchtungen haben sich also dahingehend bewahrheitet, dass Ransomware in den nächsten Jahren eine ernstzunehmende Bedrohung darstellt.

1.2 Definition des Begriffes Ransomware

Ransomware gehört der Gruppe von Malware-Programmen an. Malware hat allgemein das Ziel, Computer Systeme zu infizieren um diese Systeme für ihre Zwecke zu nutzen. Der Einsatzzweck von Malware kann vielseitig sein. Zum einen gibt es Trojaner, welche das Ausspähen von Daten als Ziel haben. Daneben kann es auch Malware geben, die ausschließlich Daten auf dem System unwiderruflich zerstören möchte um so einen größtmöglichen Schaden zu verursachen.

Die Ransomware-Programme verfolgen das Ziel, Lösegeld (Englisch: ransom) von dem Betroffenen zu erpressen. Das kann auf unterschiedliche Arten erfolgen. Zum einen existiert die Variante, dass die Ransomware illegales Material auf dem PC hinterlegt und den Anwender damit erpresst, dass die Polizei informiert wird wenn dieser kein Lösegeld bezahlt. Diese Art der Ransomware wird auch Policeware genannt. [HCS17] Die andere Art von Ransomware-Programmen blockiert den Zugriff

auf das System, beziehungsweise auf die sich darauf befindlichen Daten. Daher wird diese Art auch Krypto-Ransomware genannt. In dieser Arbeit soll der Fokus auf der Krypto-Ransomware liegen. Die sogenannte Policeware wird nicht weiter betrachtet.

Nachdem das Programm den Zugriff auf das System gesperrt hat, wird der Anwender von dem Programm informiert, dass der Zugriff auf seine Daten so lange blockiert wird, bis dieser ein entsprechendes Lösegeld bezahlt hat. Nach erfolgter Zahlung wird dem Anwender die Freigabe und damit der Zugriff auf seine Daten versprochen. Der Erpresser hat ein finanzielles Interesse daran, dass dieser Vorgang auch funktioniert. Im anderen Fall hätte der betroffene Anwender keinen Grund das Lösegeld zu bezahlen.

1.3 File-encrypting Ransomware

Bei der „File-encrypting Ransomware“ handelt es sich um die klassische und bekannteste Form von Ransomware. Nachdem die Schadsoftware heruntergeladen wurde, beginnt diese mit der Verschlüsselung der Daten auf dem Computer des Opfers. Im Anschluss wird der Computer neu gestartet um den Sperrvorgang abzuschließen. Nachdem der Computer neu gestartet wurde, begrüßt dieser den Anwender mit einer entsprechenden Meldung und Instruktionen wie dieser wieder Zugriff auf seine Daten bekommt. Die Schadsoftware verschlüsselt entweder alle oder bestimmte Arten von Dateien, welche für den betroffenen mit einer hohen Wahrscheinlichkeit einen großen Wert haben. Hierzu können zum Beispiel Bilddateien oder Office-Dokumente gehören. Daher hat das Opfer in der Regel ein großes Interesse an der Wiederbeschaffung seiner Daten. Auf der anderen Seite hat der Angreifer auch ein Interesse daran, dass das Opfer nach dem Zahlen des Lösegelds die Daten wieder entschlüsseln kann. Sollte das nicht der Fall sein, besteht für das Opfer keine Notwendigkeit das Geld zu bezahlen und der Angreifer verliert sein Geschäftsmodell. Damit dieser Vorgang möglichst reibungslos von statten geht, bekommt das Opfer eine detaillierte Beschreibung für das weitere Vorgehen. Auch Support-Hotlines werden teilweise zur Verfügung gestellt. [Tre]

1.4 Screen Locking Ransomware

Bei einer Screen-Locking-Ransomware-Attacke, werden keine einzelnen Dateien verschlüsselt. Stattdessen wird die Nutzung des PCs verhindert, indem eine Meldung eingeblendet wird, welche die Instruktionen zum entsperren des PCs beinhaltet. Auch das Booten im „sicheren Modus“ wird durch diese Ransomware verhindert. Da aber keine Dateien verschlüsselt werden, ist es trotzdem möglich auf diese Daten zuzugreifen ohne das Lösegeld zu bezahlen. Damit ist diese Art von Ransomware weniger effektiv. Für den normalen Anwender ist aber in der Regel nicht ersichtlich um welche Art von Ransomware es sich bei der Attacke handelt. Wodurch es für ihn keinen Unterschied macht, wenn er sich auf die Forderung des Erpressers einlässt. Für den Erpresser hat diese Art von Ransomware den Vorteil, dass das Entsperren des PCs einfacher ist, da keine Dateien entschlüsselt werden müssen.

1.5 Zahlungsmittel

Zur Bezahlung des Lösegelds, wird in der Regel auf eine Kryptowährung zurückgegriffen. Die bekannteste dürfte hierbei Bitcoin [Nak] sein. Der Vorteil einer Kryptowährung besteht in der dezentralen Struktur. Dadurch existiert keine verantwortliche Stelle, welche den Zahlungsverkehr kontrollieren oder sogar stoppen könnte. Des Weiteren kann diese Art der Bezahlung vollständig

anonym erfolgen, sodass es für Strafverfolgungsbehörden nahezu unmöglich ist, den Empfänger solcher Zahlungen zu identifizieren. Es gilt hierbei allerdings zu beachten, dass zum Beispiel Bitcoin laut Definition keinen anonymen Ansatz verfolgt. Alle Zahlungen sind vollkommen transparent und können jederzeit nachverfolgt werden. Die Anonymisierung erfolgt ausschließlich durch die nicht existierenden Informationen zu dem Eigentümer einer Bitcoin-Adresse. Eine solche Adresse entspricht einem Konto im traditionellen Zahlungsverkehr und lässt sich über eine eindeutige ID identifizieren. Sobald diese ID allerdings einer Person oder einem Unternehmen zugeordnet werden konnte, ist der Zahlungsverkehr vollkommen transparent.

Für einen Ransomware-Erpresser hat diese Art der Bezahlung daher viele Vorteile. Zum einen ist er als Empfänger nicht identifizierbar und zum anderen kann keine Bank oder staatliche Organisation das Konto sperren und Zahlungstransaktionen stoppen. Es gibt allerdings auch einen gravierenden Nachteil. Die meisten Betroffenen einer Ransomware-Attacke haben keine Kenntnis über diese Art von Währung und wissen daher auch nicht wie sie diese verwenden können. Daher ist der Erpresser gezwungen in seiner Software exakt zu erklären, wie eine solche Zahlung erfolgen muss und welche Programme der Betroffene benötigt. Für viele stellt das allerdings einen unmöglichen technischen Aufwand dar. Für den Erpresser führt das zu sinkenden Einnahmen aufgrund der Komplexität der Zahlungsabwicklung.

1.6 Historie

Die Idee mit Computer-Programmen Geld zu erpressen, indem diese den Zugriff auf den PC oder einzelne Dateien verhindern, ist schon alt. Bereits 1989 gab es ein Programm, welches die Namen aller Dateien auf einem PC „verschlüsselt“ hat. [Sim] Der Inhalt dieser Dateien war aber weiterhin lesbar. Nach dem Neustart erschien eine Meldung, dass für die Nutzung des PCs ab sofort eine Lizenz notwendig sei. Außerdem wurde auf einem angeschlossenen Drucker ein Verrechnungsscheck ausgedruckt, welcher an eine Briefkastenfirma in Panama gesendet werden sollte. Da sich diese Ransomware noch nicht über das Internet verbreiten konnte, musste ein klassischer Weg zum versenden genutzt werden. Der Autor dieses Programms verschickte 90.000 Disketten mit seinem Schadcode in 90 Länder. Bei den Empfängern handelte es sich um Forscher, die sich mit dem AIDS Virus beschäftigten. Für den Absender der Disketten dachte sich der Entwickler Joseph Popp die Firma „PC Cyborg Corporation“ aus. Daher wird diese Ransomware auch „PC Cyborg“ oder „AIDS“ genannt.

Die erste Beschreibung eines Krypto-Virus, wie wir ihn heute als Ransomware kennen, erfolgte 1996 von Adam Young und Prof. Moti Yung. [AY] Sie beschrieben die Möglichkeit eine Erpressung anhand von kryptografischen Verfahren durchzuführen. In den ersten Jahren nach der Veröffentlichung wurden aber nur wenige und meist sehr fehleranfällige Programme entwickelt. Die erste ernstzunehmende Ransomware wurde 2013 entdeckt. Es handelte sich hierbei um das Programm *Cryptolocker*, welches bis heute im Umlauf ist. [HCS17]

2 Ökonomische Betrachtung

2.1 Geschäftsmodell

Die Entwickler von Ransomware verfolgen das Ziel ein möglichst profitables Geschäftsmodell aufzubauen. Dieses Modell basiert auf der Erpressung von, in der Regel zufällig ausgewählten, „Kunden“. Dieses illegale Geschäftsgebaren, unterscheidet sich in der Herangehensweise nicht von der eines klassischen Marktteilnehmers. Allerdings befindet sich der Erpresser in einem monopolistischen Markt, in dem er als einziger die nachgefragte Ware anbietet. Bei der Ware handelt es sich um den Schlüssel, welcher wieder Zugriff auf die Daten gewährt. Da der Erpresser ein Monopol besitzt, kann er auch den Preis bestimmen welchen die Betroffenen zahlen müssen um an ihre Daten zu gelangen. Der Monopolist ist aber trotz seiner marktbeherrschenden Stellung gezwungen, dem Kunden eine gute Leistung anzubieten, damit dieser überhaupt bereit ist die Ware zu erwerben. Im anderen Fall könnte der Kunde die Entscheidung treffen, dass er auf den Kauf der Ware verzichtet. In diesem Fall wären zwar seine Daten unter Umständen verloren, für den Erpresser hätte dieses Verhalten aber finanzielle Konsequenzen, welche er auf anderem Wege ausgleichen müsste.

2.2 Zahlungsbereitschaft

Der Begünstigte von Ransomware verfolgt das Ziel, dass möglichst viele Personen auf seine Forderung eingehen. Das ist notwendig, da der Erpresser zum einen seine bereits entstandenen Kosten decken und zum anderen einen positiven Gewinn erreichen möchte. Der Erpresser ist zum Zeitpunkt der Infektion eines PCs schon in finanzielle Vorkasse getreten. Zum einen musste er die Entwicklung der Software finanzieren und zum anderen musste er einen Vertriebskanal, in den meisten Fällen ein Botnetz, anmieten. Es ist daher für den Erpresser zwingend notwendig, dass er sich bereits im voraus Gedanken über die Zahlungsbereitschaft der Betroffenen macht. Auch sollten die veranschlagten Preise für den Schlüssel im Verhältnis zur erbrachten Leistung stehen.

Ob ein Betroffener bereit ist für die Entschlüsselung seiner Daten zu bezahlen, hängt von mehreren Faktoren ab. [HCS17] Zum einen kommt es auf den Wert der Daten an, welche verschlüsselt wurden. Handelt es sich hierbei um unwichtige Daten, wird der Betroffene in der Regel nicht bereit sein hierfür Geld zu bezahlen. Der zweite Faktor betrifft die Glaubwürdigkeit des Erpressers. Dieser verspricht dem Betroffenen, dass dieser seine Daten entschlüsseln kann sobald er das Lösegeld bezahlt hat. Nur wenn der Geschädigte dem Erpresser vertraut, wird er ihm das Lösegeld überweisen. Der Erpresser hat daher ein Interesse an einer funktionieren Entschlüsselung der Daten. Unabhängig von der Vertrauenswürdigkeit kann der Erpresser aber auch nicht ausschließen, dass die Daten unwiederbringlich verloren gegangen sind.

Ob ein Opfer bereit ist zu zahlen und welche Auswirkungen diese Bereitschaft auf den Gewinn des Erpressers hat, lässt sich auch mathematisch darstellen. [HCS17] Die Bereitschaft einer Person das Lösegeld zu bezahlen wird dabei als v_i dargestellt. Hierbei steht v für die Zahlungsbereitschaft und i für die Person. Angenommen die verschlüsselten Daten sind dem Betroffenen EUR 500,00 Wert

und er vertraut dem Erpresser, dann hat v_i den Wert 500,00. Für den Fall, dass der Betroffene kein Vertrauen gegenüber dem Erpresser aufbringen kann entspricht $v_i = 0$. Um den endgültigen Gewinn des Erpressers zu berücksichtigen müssen allerdings noch mehr Faktoren berücksichtigt werden. Zum einen hängt dieser von der Anzahl der attackierten Personen N ab. Des Weiteren müssen die Kosten für die Entwicklung und den Betrieb F der Ransomware abgezogen werden. Weiterhin müssen gegebenenfalls Transaktionsgebühren c berücksichtigt werden. Die entsprechende Formel lautet wie folgt:

$$G = \sum_{i=1}^{N} (p_i - c)1_i - F \tag{2.1}$$

Ob ein Betroffener bereit ist den geforderten Betrag p_i zu zahlen, wird durch 1_i dargestellt. Dieser Wert ist 1, wenn $v_i >= p_i$. Im anderen Fall ist dieser Wert 0. An dieser Formel ist abzulesen, dass der zu erzielenden Gewinn maßgeblich von der Höhe des geforderten Lösegelds abhängt. Wenn der Erpresser diesen Wert zu groß wählt, werden seine Gewinnabsichten nicht erfolgreich sein. Der Erpresser hat daher zwei Möglichkeiten das geforderte Lösegeld zu bestimmen. Er kann entweder einen Betrag wählen, von dem er erwarten kann das möglichst viele Betroffene bereit sind diesen zu bezahlen, oder er berechnet für jedes Opfer einen individuellen Betrag.

2.2.1 Einheitliche Preisgestaltung

Bei einer einheitlichen Preisgestaltung besteht die Schwierigkeit für den Erpresser darin zu ermitteln bei welchem Betrag die meisten Opfer bereit sind zu zahlen. Die Anzahl der Betroffenen, welche bereit sind den Preis p zu bezahlen werden als $Q(p)$ dargestellt. Die Formel zur Berechnung des Gewinns des Erpresser lautet demnach wie folgt:

$$G = (p - c)Q(p) - F \tag{2.2}$$

Um sich dem optimalen Preis p anzunähern, muss die Preiselastizität der Nachfrage ermittelt werden. "Das Gesetz der Nachfrage besagt, dass ein Preisrückgang für ein Gut die Nachfragemenge ansteigen lässt. Die Preiselastizität misst, wie die Nachfragemenge auf eine Preisänderung reagiert."[MT12, S. 112] Ziel der Preisanpassung muss es daher sein, dass die Preiselastizität möglichst gering ausfällt. Das würde bedeuten, dass der Erpresser einen höheren Preis veranschlagen könnte, ohne das die Nachfrage signifikant sinkt. In diesem Fall hat er einen möglichst optimalen Preis erreicht bei dem $p = v_i$ ist und $Q(p)$ möglichst groß ist.

2.2.2 Dynamische Preisgestaltung

Bei der dynamischen Preisgestaltung wird für jeden Betroffenen ein individueller Preis berechnet. Ziel ist es, dass v_i möglichst nah an p_i liegt, beziehungsweise das die beiden Werte im optimalen Fall gleich sind. Um dieses Ziel zu erreichen muss der Erpresser möglichst viele Informationen über sein Opfer sammeln. Der Preis für die Herausgabe des Schlüssels, hängt somit von mehreren Parametern ab. Diese können zum Beispiel das Alter des PCs, die Anzahl der verschlüsselten Dateien, die Art der Dateien oder auch der Inhalt der Dateien sein. Es ist auch möglich Techniken des maschinellen Lernens einzusetzen um anhand von Erfahrungswerten den Preis zu optimieren.

3 Beispiele für Ransomware

In einer Studie [KRB+15] von 2015 wurden in den Jahren 2006 bis 2014 1359 Beispiele von Ransomware-Programmen untersucht. Diese ließen sich allerdings auf 15 Ransomware-Familien zusammenfassen. Das bedeutet, dass es tatsächlich nur 15 unterschiedliche Ansätze für die Bau eines Ransomware Programmes gab. In den ersten Jahren war die Bedrohung durch Ransomware allerdings nicht signifikant. Erst durch das Auftauchen von *Cryptolocker* stieg die Anzahl von Ransomware-Attacken um 500% im Jahr 2013.

3.1 Cryptolocker

Wie bereits zuvor erwähnt, war *Cryptolocker* die erste Ransomware, welche tatsächlich funktioniert hat und dadurch auch sehr erfolgreich war. Das erste mal wurde dieses Programm 2013 entdeckt. Die Entwickler hatten es geschafft ein Programm zu schreiben, welches alle Dateien auf der Festplatte verschlüsselt und in der Lage war diese auch wieder zu entschlüsseln. Insgesamt waren von dieser Ransomware über 250.000 Systeme betroffen. [KRB+15] Die Wiederherstellungsrate nach der Bezahlung des Lösegelds lag bei ca. 65%. Die Verbreitung erfolgte via Email. Diese besaßen einen schadhaften Dateianhang, welchen die Empfänger öffnen mussten. Der Versand dieser Emails wurde über das Gameover/Zeus Botnetz gesteuert. [HCS17] Hierbei handelte es sich um einen Verbund von über einer Million infizierter Systeme, welche diese Emails versendeten. Die Bezahlung des Lösegelds erfolgte bei dieser Ransomware erstmalig via Bitcoin. Der Preis Betrug US$ 300,00 was damals ca. 0.5 Bitcoin entsprach. [HC] *Cryptolocker* verwendete für jedes Opfer eine individuelle Bitcoin Adresse, allerdings wurde ein Großteil der Transaktionen auf eine einzige Adresse zusammengeführt. Insgesamt gingen auf diese Adresse (174psvzt77NgEC373xSZWm9gYXqz4sTJjn) 346.102,31357807 Bitcoins ein. Schon damals haben die Erpresser mit ihrer Ransomware fast 2 Millionen US-Dollar verdient. Wenn man den heutigen Wert im November 2017 zugrunde legt, liegt der Gewinn bei über 3 Milliarden US-Dollar. Das resultiert natürlich ausschließlich aus dem enormen Kursanstieg den die Bitcoin-Währung in den letzten Jahren vollzogen hat. Anhand solcher Zahlen ist es daher auch nicht verwunderlich, dass das FBI 2016 von einem Milliarden Dollar Geschäft durch Ransomware gesprochen hat. Durch die Zusammenarbeit von Behörden aus der ganzen Welt ist es später gelungen, dass Gameover/Zeus Botnetz abzuschalten und dadurch auch die Cryptolocker Ransomware weitestgehend zu stoppen. Im Zuge dieser Maßnahmen fanden die Behörden Datensätze mit ca. 500.000 privaten Schlüsseln, wodurch viele Betroffene ihre Daten wieder entschlüsseln konnten ohne das Lösegeld zu bezahlen. [HCS17]

3.2 Locky

Die Ransomware *Locky* tauchte erstmalig Anfang 2016 auf. [Eik] Die Schadsoftware verbreitete sich über Macros in Office-Dokumenten, welche via Email verschickt wurden. Besonders in Deutschland, wo es bis zu 5000 Neuinfektionen pro Stunde gegeben hat, hat diese Ransomware viele Opfer gefordert.

Ein Grund für diese hohen Infektionsraten bestand darin, dass sich *Locky* nach der Infektion des PCs ruhig verhalten hat. Erst zu einem späteren Zeitpunkt hat die Schadsoftware von zentraler Stelle den Befehl zum Verschlüsseln erhalten. Dadurch waren gleichzeitig viele tausende Systeme betroffen. Ein weiteres Problem für Unternehmen bestand darin, dass diese Ransomware nicht nur die lokalen Dateien auf einem PC verschlüsselt hat, sondern auch alle Daten auf angebundenen Netzlaufwerken. Das führte zu der Situation, dass durch einen infizierten PC das gesamte Unternehmen betroffen war. Im Zuge der Infektionen durch *Locky* wurde vom BSI auch erstmalig ein Leitfaden zum Umgang mit Ransomware veröffentlicht. Dieser soll Unternehmen helfen das Risiko durch organisatorische Maßnahmen zu verringern.[fSidI16] In der Folge gab es viele Varianten von *Locky*. Diese hießen zum Beispiel *Zepto* oder ganz aktuell *Diablo6*. [Scha]

3.3 WannaCry

Eine der bekanntesten Ransomware-Attacken der letzten Jahre dürfte *WannaCry* gewesen sein. Dieser Ransomware gelang mediale Berühmtheit, da zum Beispiel auf den Anzeigetafeln der Deutschen Bahn die Erpressermeldung angezeigt wurde. [MH] *WannaCry* unterschied sich von früheren Ransomware Attacken, da sich die Schadsoftware selbständig und ohne Interaktion des Benutzers weiterverbreiten konnte. Grund hierfür war eine Sicherheitslücke im SMB-Protokoll, welche auf vielen Windows Systemen zu dem Zeitpunkt noch nicht geschlossen war. Öffentlich wurde diese Sicherheitslücke durch den Vault 7 Leak von CIA Spionage Programmen. [Gua] Zwar hatte Microsoft bereits kurz vor bekanntwerden der Sicherheitslücke einen entsprechenden Patch herausgebracht, viele Unternehmen hatten diesen allerdings noch nicht installiert. Des Weiteren betraf die Sicherheitslücke auch hauptsächlich ältere Windows-Versionen, die noch das SMB-Protokoll Version 1 verwendeten. Es wurde in diesem Zusammenhang erneut deutlich, dass es für ein Unternehmen von existentieller Bedeutung ist ein funktionierendes Patchmanagement implementiert zu haben. Nach kurzer Zeit war festzustellen, dass sich die Ausbreitung dieser Schadsoftware verlangsamte. Grund hierfür war die Entdeckung eines Sicherheitsforschers, dass die Software versucht eine bestimmte URL zu erreichen. Nur wenn diese nicht erreichbar war, verbreitete sich die Schadsoftware weiter. Diese Domain war allerdings nicht registriert, wodurch dieser Check keine Bedeutung hatte. Erst nachdem der Sicherheitsforscher die Domain registrierte, stellte die Schadsoftware ihre Arbeit ein. [New] Großen Schaden hatte *WannaCry* unterdessen schon bei dem britischen Gesundheitsdienst National Health Service (NHS) angerichtet. In Folge dessen konnten in den Krankenhäusern viele Patienten nicht mehr richtig behandelt werden. [Off17] Für die Angreifer hat sich dieser Angriff allerdings nicht gelohnt. Insgesamt haben sie nach Schätzungen nur ca. 30.000 EUR erbeutet. Das ist im Vergleich zum *Cryptolocker* nur eine sehr geringe Summe.

Die Schadsoftware *WannaCry* war die Erste, welche sich selbständig verbreitet hat. Bis zu diesem Zeitpunkt war immer eine Interaktionen des Anwenders erforderlich, damit die Software Daten verschlüsseln konnte. Aufgrund dieses Verhaltens galt *WannaCry* zu dem Zeitpunkt auch als Ransomware mit den größten Auswirkungen. Ein Grund für die vielen Ausfälle und prominenten Opfer, zu denen auch Automobilkonzerne wie Renault und Honda [Lyo] gehörten, lag in der Anfälligkeit von Windows XP. Viele Industrie PCs zur Steuerung von Produktionsanlagen oder auch Systeme in der Gesundheitsversorgung laufen noch mit diesem alten Betriebssystem, welches Microsoft schon vor langer Zeit abgekündigt hat. Die Schadsoftware besaß des weiteren eine besondere Eigenschaft. Die Entwickler verschlüsselten die Daten mit zwei unterschiedlichen Public Keys. Der eine Schlüssel wurde verwendet um den Großteil der Daten zu verschlüsseln und mit dem anderen wurde nur ein kleiner Teil der Dateien auf der Festplatte verschlüsselt. Ziel der Erpresser war es damit zu beweisen, dass sie die Daten auch wieder entschlüsseln konnten. Hierfür mussten sie dem Betroffenen nur den Privaten Schlüssel zukommen lassen. Durch dieses Vorgehen wächst das Vertrauen in den Erpresser, wodurch bei dem Opfer die Zahlungsbereitschaft v_i steigt. Zum

Verschlüsseln der Daten wurde jeweils ein 2048bit RSA Schlüsselpaar für jedes Opfer erzeugt. Mit dem zugehörigen privaten Schlüssel konnten die Betroffenen daher nur ihre eigenen Dateien wieder entschlüsseln.

3.4 Petya / NotPetya

Wenige Wochen nach dem Auftauchen der *WannaCry-Ransomware*, gelangte eine Schadsoftware namens *Petya* beziehungsweise *NotPetya* in den Umlauf. Diese nutzte die selbe Sicherheitslücke im SMB-Protokoll wie schon *WannaCry*. Allerdings gelang diese über einen Update-Mechanismus einer ukrainischen Steuersoftware MeDoc in die Unternehmen. Diese Schadsoftware hatte nicht das Ziel Privatnutzer zu schädigen, sondern galt in erster Linie ukrainischen Unternehmen beziehungsweise allen Unternehmen die in der Ukraine Steuern zahlen und damit diese Software im Betrieb haben. Im Gegensatz zu *WannaCry* wurde aber relativ schnell klar, dass diese Art von Schadsoftware sich nur als Ransomware getarnt hatte. [AI] Ziel dieser Software war es vielmehr die Daten unwiederbringlich zu zerstören, in dem diese verschlüsselt wurden. Für viele bekannte Unternehmen entstand so ein großer Schaden. Bei der dänischen Reederei Maersk führte die Schadsoftware zu Systemausfällen über mehrere Wochen. Schiffe konnten nicht be- und entladen werden, wodurch ein Schaden von 200 – 300 Millionen Euro entstand. [juh] Auch bei dem Logistik Unternehmen Fedex führte diese Attacke zu einem Verlust von ca. 300 Millionen US-Dollar. [Hol] In Deutschland sorgte diese Schadsoftware bei Unternehmen wie zum Beispiel Beiersdorf für einen Millionen Schaden. [NDR]

Zwar gehört diese Schadsoftware nicht zu der Kategorie von Ransomware, da gegen die Bezahlung von Lösegeld kein Schlüssel ausgehändigt wurde, allerdings ist das Verhalten der Software identisch. Durch die Verschlüsselung der Daten ist für die Unternehmen ein hoher Schaden entstanden. Interessant in dem Zusammenhang ist allerdings, dass Maersk angegeben hat keinen Datenverlust erlitten zu haben. Daraus lässt sich schließen, dass trotz eines funktionierenden Backups die Systeme durch solche Attacken langfristig gestört werden können.

3.5 Aktuelle Situation

Nach den beiden großen Ransomware Attacken durch *WannaCry* und *NotPetya* ließt man zwar immer wieder von neuen Bedrohungen, aber vergleichbare Attacken blieben bislang aus. Allerdings tauchen immer wieder neue Varianten der bereits vorstellten Schadsoftware Programme auf. Diese sind häufig aber nicht mehr so erfolgreich, da die Unternehmen und Privatpersonen die Sicherheitslücken geschlossen haben. Allerdings tauchen in letzter Zeit vermehrt Meldungen von Ransomware für Android-Geräte auf. [Kha] Das ist ein logischer nächster Schritt für die Erpresser, da immer mehr Menschen nur noch ein mobiles Gerät anstatt eines PCs verwenden. Für Unternehmen dürfte die Gefahr allerdings überschaubar sein. Da auf einem mobilen Gerät keine Unternehmenskritischen Daten liegen sollten, welche nicht auch noch an anderer Stelle vorgehalten werden.

4

Ransomware as a Service

Das Geschäft mit Ransomware steigt stetig. Daher hat sich ein neuer Geschäftszweig entwickelt, in dem fertige Ransomware-Programme zum Kauf angeboten werden. Im Zeitraum von 2016 bis 2017 ist der Verkauf von Ransomware um 2500% gestiegen. In einer Studie von Carbon Black [Bla17] kam heraus, dass auf über 6300 Marktplätzen im Darknet ca. 45.000 Ransomware-Programme zum Kauf angeboten werden. Die Preise für ein solches Programm variieren zwischen $0,50 und $3.000. Im Mittel liegt der Preis bei 10.50 US-Dollar. In 2017 wurden damit ca. 6 Millionen US-Dollar umgesetzt. Im Vorjahr betrug die Summe lediglich 250.000 US-Dollar. Die Bezahlung solcher Programme erfolgt via Bitcoin und die Shops in denen die Programme angeboten werden, sind nur im Tor-Netzwerk erreichbar. Daher ist es für Justizbehörden auch sehr schwer, die Verantwortlichen ausfindig zu machen.

Ein Grund für den starken Anstieg im Ransomware-Geschäft sind die guten Verdienstmöglichkeiten für die Entwickler. Ein Vergleich mit den durchschnittlichen Gehältern in der Softwarebranche zeigt, dass ein Ransomware Entwickler um die 30.000 US-Dollar im Jahr mehr verdienen kann als ein Entwickler, der einer legalen Tätigkeit nachgeht. Das ist im ersten Moment nicht verwunderlich und ist auch mit anderen kriminellen Bereichen vergleichbar. Allerdings haben die Ransomware-Entwickler den Vorteil, dass sie völlig anonym agieren können. Sie haben nie direkten Kontakt zu den Käufern. Auch müssen sie im Vergleich zum Rauschgift- oder Waffenhandel nie ihre Ware über einen öffentlichen Weg, verschicken. [Cox] Ein weiterer Grund für den Anstieg in den letzten Jahren ist die Entwicklung von Bitcoin. Weder der Anbieter noch der Käufer muss sich Gedanken über eine anonyme und verdeckte Zahlungsabwicklung machen. Die Infrastruktur hierfür steht bereits zur Verfügung und kann mit geringem Aufwand genutzt werden.

Die Anbieter von Ransomware-Programmen unterscheiden sich kaum noch von legalen Software-Anbietern. Von einzelnen Programmen bis zu Ransomware Komplettlösungen, wird alles angeboten. Das gesamte Ökosystem lässt sich in drei Schichten unterteilen. Die erste Schickt beschreibt die Entwickler. Diese entwickeln die Software, leisten Support und verteilen Updates mit neuen Funktionen oder Bugfixes. Diese Gruppe verwendet in der Regel aber nie die Software. In der nächsten Ebene befinden sich die Betreiber von Ransomware as a Service (RaaS) Systemen. Diese Systeme stellen die Komplettlösung dar. Ein Käufer kann hierüber seine Ransomware individuell konfigurieren und verteilen. Des Weiteren bieten solche Angebote die Möglichkeit, Statistiken über den Erfolg von Ransomware-Attacken zu erstellen um zukünftige Angriffe zu optimieren. Es gibt auch die Variante, dass sich der Interessent ein RaaS-System mietet. Der Betreiber bekommt dann eine Provision [Schb] von den erpressten Lösegeldern. In der dritten und letzten Ebene befinden sich die Verteiler von Ransomware. Diese verschicken die Ransomware oder nutzen RaaS-Umgebungen, welche sie zuvor erworben haben. Diese Gruppe von Personen haben das größte Risiko in der Kette, da sie diejenigen sind, welche am Ende die „Waffe“ abfeuern.

5 Gegenmaßnahmen

5.1 Backup

Eine der besten und einfachsten Schutzmaßnahmen gegenüber Ransomware besteht in einer regelmäßigen Sicherung der eigenen Daten. Aufgrund eines Backups ist der PC oder Server zwar weiterhin gegenüber Ransomware-Attacken verwundbar, allerdings besteht für für den Betroffenen keine Notwendigkeit auf die Lösegeldforderung einzugehen. Vielmehr muss er das System lediglich neu installieren und das vorhandene Backup zurückspielen. Im Unternehmensumfeld ist eine solche Maßnahme weiterhin mit hohem Aufwand und dadurch mit hohen Kosten verbunden, es führt allerdings zu einem entgangenen Gewinn für den Erpresser.

Die Zahlungsbereitschaft v_i hat bei den Betroffenen einen Wert von 0. Sie haben keinen Grund auf die Forderung einzugehen. Im Umkehrschluss bedeutet dass, je mehr Personen und Unternehmen eine regelmäßige Datensicherung durchführen, desto kleiner wird $Q(p)$. Daraus resultiert, dass der Gewinn für den Erpresser schrumpft. Das bedeutet wiederum, dass ein Backup der eigenen Daten nicht nur dem eigenen Schutz dient, sondern dem Schutz der Allgemeinheit, sprich einem Kollektivschutz.

Insbesondere für Unternehmen besteht die Möglichkeit ihre vorhandenen Speicherlösungen gegen revisionssichere Produkte auszutauschen. Diese haben den Vorteil, dass eine Datei auf einen bestimmten Stand zurückgesetzt werden kann. In dem Fall auf den Stand bevor die Ransomware zugeschlagen hat. Dieses Vorgehen ist sehr schnell und für das Unternehmen mit geringem Aufwand und daher mit geringen Kosten verbunden.

5.2 Spamfilter / AntiVirus

Natürlich spielen auch Spamfilter und AntiVirus Systeme eine Rolle bei der Bekämpfung von Ransomware Angriffen. Viele Ransomware Programme werden via Email verschickt. Es ist daher sinnvoll, eingehende Emails zu scannen um zumindest bekannte Schadprogramme zu entdecken. Des Weiteren müssen die Mitarbeiter geschult werden, um unseriöse Emails erkennen zu können. Eine weitere Möglichkeit besteht in modernen AntiVirus-Programmen. Diese können gestartete Programme, beziehungsweise geöffnete Dateien, in einem abgeschlossenen System ausführen und im Anschluss überprüfen, ob die Ausführung zu einer Schädigung des Systems geführt hat. Wenn das der Fall ist, sperrt ein solches Programm die Ausführung für den Benutzer. Die Entwickler von Schadsoftware versuchen aber auf der anderen Seite solche abgeschlossenen Systeme zu erkennen um die wahre Eigenschaft ihres Programms zu verbergen.

5.3 Weitere Maßnahmen

Viele Schadprogramme wie zum Beispiel *WannaCry* oder *NotPetya* waren nur so erfolgreich, weil die Unternehmen und Privatpersonen Software eingesetzt haben, welche bekannte Sicherheitslücken aufwiesen. Anhand dieser beider Fälle wurde deutlich, dass es wichtig ist seine Systeme regelmäßig zu patchen, um gegen solche Angriffe immun zu sein. Weitere Entwicklungen gehen dahin, dass die Hersteller von Sicherheitslösungen versuchen Ransomware aufgrund des verursachten Traffics zu erkennen. Das kann im einfachen Fall durch die Auswertung von Logdateien geschehen oder auch durch das Mitschneiden und Analysieren von Datenpaketen im Netzwerk. Falls eine Ransomware die sich selbst weiter verbreitet, wie zum Beispiel *WannaCry*, entdeckt wird sollte schnellstmöglich die Netzwerkkommunikation unterbrochen werden. Eine effektive Maßnahme könnte darin bestehen, zentrale Netzwerkknoten abzuschalten. Das führt unter umständen zu einer Störung im Betriebsablauf, diese lässt sich aber schneller beheben, als wenn große Teile der Infrastruktur von einer Ransomware befreit werden müssen.

5.4 No More Ransom Projekt

Falls es doch zu einer Infektion mit einer Ransomware gekommen ist, sollte man wenn möglich darauf verzichten das Lösegeld zu bezahlen, da man damit die Erpresser in ihrem Verhalten bestätigt. Um Privatpersonen in solche Fällen zu unterstützen, wird das Projekt „No More Ransom“ von Unternehmen für Sicherheitslösungen aber auch von Strafverfolgungsbehörden wie zum Beispiel Interpol oder dem Bundeskriminalamt (BKA) unterstützt. Auf der Webseite `https://www.nomoreransom.org` erhalten die Betroffenen Informationen über das weitere Vorgehen nach einer Infektion oder Tipps welche präventiven Maßnahmen es gibt. Des Weiteren gibt es die Möglichkeit herauszufinden welche Ransomware den eigenen PC befallen hat und ob es dafür bereits Programme zur Entschlüsselung gibt. Diese Programme lassen sich inklusive einer detaillierten Anleitung herunterladen. Auch entsprechende Links zum Anzeigen der Straftat gibt es auf der Seite.

Quellenverzeichnis

[AI] Orkhan Mamedov Anton Ivanov. ExPetr/Petya/NotPetya is a Wiper, Not Ransomware. Website. Online erhältlich unter https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902; abgerufen am 15. September 2017.

[AY] Moti Yung Adam Young. Cryptovirology: Extortion Based Security Threats and Countermeasures. Website. Online erhältlich unter https://pdfs.semanticscholar.org/8767/f574688f40e9fb1df9d15219b18748c003a5.pdf; abgerufen am 21. November 2017.

[Bit] Bitdefender. How to remove FBI Ransomware infection. Website. Online erhältlich unter https://www.bitdefender.com/support/how-to-remove-fbi-ransomware-infection-1081.html?zanpid=2327168447349857280; abgerufen am 31. July 2017.

[Bla17] Carbon Black. The ransomware economy, 2017. Online erhältlich unter https://www.carbonblack.com/wp-content/uploads/2017/10/Carbon-Black-Ransomware-Economy-Report-101117.pdf; abgerufen am 10. Oktober 2017.

[Bor] Detlef Borchers. Ransomware-Virus legt Krankenhaus lahm. Website. Online erhältlich unter https://www.heise.de/newsticker/meldung/Ransomware-Virus-legt-Krankenhaus-lahm-3100418.html; abgerufen am 25. November 2017.

[Bri] Volker Briegleb. Ransomware WannaCry befällt Rechner der Deutschen Bahn. Website. Online erhältlich unter https://www.heise.de/newsticker/meldung/Ransomware-WannaCry-befaellt-Rechner-der-Deutschen-Bahn-3713426.html; abgerufen am 09. November 2017.

[Cox] Joseph Cox. 7 ways the cops will bust you on the dark web. Website. Online erhältlich unter https://motherboard.vice.com/en_us/article/vv73pj/7-ways-the-cops-will-bust-you-on-the-dark-web; abgerufen am 13. November 2017.

[Eik] Ronald Eikenberg. Erpressungs-Trojaner Locky schlägt offenbar koordiniert zu. Website. Online erhältlich unter https://www.heise.de/security/meldung/Erpressungs-Trojaner-Locky-schlaegt-offenbar-koordiniert-zu-3104069.html; abgerufen am 09. September 2017.

[fSidI] Bundesamt für Sicherheit in der Informationstechnik. Cyber-Sicherheits-Umfrage 2016. Website. Online erhältlich unter https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/cybersicherheitslage/umfrage2016_ergebnisse.pdf; abgerufen am 09. November 2017.

[fSidI16] Bundesamt für Sicherheit in der Informationstechnik, editor. *Ransomware - Bedrohungslage, Prävention und Reaktion*, 2016. Online erhältlich unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf; abgerufen am 15. November 2017.

[GP] Jacob Gronholt-Pedersen. Maersk says global IT breakdown caused by cyber attack. Website. Online erhältlich unter https://www.reuters.com/article/us-cyber-attack-maersk/

maersk-says-global-it-breakdown-caused-by-cyber-attack-idUSKBN19I1NO; abgerufen am 09. November 2017.

[Gua] The Guardian. WikiLeaks publishes „biggest ever leak of secret CIA documents“. Website. Online erhältlich unter https://www.theguardian.com/media/2017/mar/07/wikileaks-publishes-biggest-ever-leak-of-secret-cia-documents-hacking-surveillance abgerufen am 09. September 2017.

[HC] Julio Hernandez-Castro. Cryptolocker has you between a back up and a hard place. Website. Online erhältlich unter https://phys.org/news/2014-03-cryptolocker-hard.html; abgerufen am 28. November 2017.

[HCS17] Julio Hernandez-Castro, Edward Cartwright, and Anna Stepanova. Economic analysis of ransomware, 2017. Online erhältlich unter http://arxiv.org/abs/1703.06660.

[Hol] Martin Holland. NotPetya: Auch Fedex kostet die Cyber-Attacke 300 Millionen US-Dollar. Website. Online erhältlich unter https://www.heise.de/newsticker/meldung/NotPetya-Auch-Fedex-kostet-die-Cyber-Attacke-300-Millionen-US-Dollar-3838159.html; abgerufen am 29. September 2017.

[juh] juh/AP/Reuters. Hackerangriff kostet Reederei Hunderte Millionen. Website. Online erhältlich unter http://www.spiegel.de/netzwelt/netzpolitik/moller-m-rsk-cyberangriff-kostet-reederei-hunderte-millionen-a-1163111.html; abgerufen am 15. September 2017.

[Kha] Swati Khandelwal. New ransomware not just encrypts your android but also changes pin lock. Website. Online erhältlich unter https://thehackernews.com/2017/10/android-ransomware-pin.html; abgerufen am 13. November 2017.

[KRB+15] Amin Kharraz, William Robertson, Davide Balzarotti, Leyla Bilge, and Engin Kirda. Cutting the gordian knot: A look under the hood of ransomware attacks. In *DIMVA 2015, 12th Conference on Detection of Intrusions and Malware & Vulnerability Assessment, July 9-10, 2015, Milan, Italy*, Milan, ITALY, 07 / 2015.

[Lyo] Peter Lyon. Cyber Attack At Honda Stops Production After WannaCry Worm Strikes. Website. Online erhältlich unter https://www.forbes.com/sites/peterlyon/2017/06/22/cyber-attack-at-honda-stops-production-after-wannacry-worm-strikes; abgerufen am 15. September 2017.

[MH] Axel Kannenberg Martin Holland. WannaCry: Angriff mit Ransomware legt weltweit Zehntausende Rechner lahm. Website. Online erhältlich unter https://www.heise.de/newsticker/meldung/WannaCry-Angriff-mit-Ransomware-legt-weltweit-Zehntausende-Rechner-lahm-3713235.html; abgerufen am 09. November 2017.

[MHUS15] Mr. Ravindra V. Kerkar Miss. Harshada U. Salvi, editor. *Ransomware: A Cyber Extortion.* Asian Journal of Convergence in Technology, 2015.

[MT12] N. Gregory Mankiw and Mark P. Taylor. *Grundzüge der Volkswirtschaftslehre.* Schäfer-Poeschel Verlag, Stuttgart, 2012.

[Nak] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Online erhältlich unter https://bitcoin.org/bitcoin.pdf.

[NDR] NDR. Bei Beiersdorf sind die Telefone noch tot. Website. Online erhältlich unter http://www.ndr.de/nachrichten/hamburg/Bei-Beiersdorf-sind-die-Telefone-noch-tot,beiersdorf226.html; abgerufen am 09. November 2017.

[New] Lilly Hay Newman. How an accidental „kill switch“ slowed friday's massive ransomware attack. Website. Online erhältlich unter https://www.wired.com/2017/05/accidental-kill-switch-slowed-fridays-massive-ransomware-attack/; abgerufen am 09. September 2017.

[Off17] National Audit Office. Investigation: WannaCry cyber attack and the NHS, 2017. Online erhältlich unter https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf; abgerufen am 28. November 2017.

[Scha] Fabian A. Scherschel. Locky ist wieder da: Erpressungstrojaner grassiert jetzt als Diablo6. Website. Online erhältlich unter https://www.heise.de/security/meldung/Locky-ist-wieder-da-Erpressungstrojaner-grassiert-jetzt-als-Diablo6-3806833.html; abgerufen am 09. September 2017.

[Schb] Fabian A. Scherschel. Ransomware-as-a-Service: Mit Satan den eigenen Erpressungstrojaner bauen. Website. Online erhältlich unter https://www.heise.de/security/meldung/Ransomware-as-a-Service-Mit-Satan-den-eigenen-Erpressungstrojaner-bauen-3605326.html; abgerufen am 13. November 2017.

[Sim] Alina Simone. The Strange History of Ransomware. Website. Online erhältlich unter https://medium.com/un-hackable/the-bizarre-pre-internet-history-of-ransomware-bb480a652b4b; abgerufen am 18. November 2017.

[Tre] TrendMicor. JIGSAW Crypto-Ransomware Turns Customer-Centric, Uses Chat for Ransom Attempts. Website. Online erhältlich unter http://blog.trendmicro.com/trendlabs-security-intelligence/jigsaw-crypto-ransomware-turns-customer-centric-uses-chat-ransom-attempts/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Anti-MalwareBlog+%28Trendlabs+Security+Intelligence+Blog%29; abgerufen am 25. November 2017.