WAS SIE ÜBER DIE RANSOMWARE-LANDSCHAFT WISSEN SOLLTEN.

Umfang und Komplexität der Bedrohung

EXECUTIVE SUMMARY

Wenn eine Cyber-Bedrohung innerhalb eines Jahres um das 35-fache wächst, sollte sie jedes Unternehmen beachten. Genau das ist mit Ransomware geschehen. Hacktivisten zielten auf Organisationen weltweit ab, auf Unternehmen praktisch jeder Größe und eine Vielzahl von Branchensegmenten. Traditionelle Sicherheitsansätze reichen nicht aus, um Ransomware-Angriffe zu verhindern. Moderne Modelle mit Next-Generation Firewalls, mehrschichtigen Sicherheitsstrukturen und proaktiver Threat Intelligence sind erforderlich.

Ransomware-as-a-Service und ähnliche Modelle haben den Einstieg für Cyber-Kriminelle erleichtert. Und monetäre Technologien wie Bitcoin machen es Strafverfolgungsbehörden praktisch unmöglich, Lösegeldzahlungen zu verfolgen. Mit der exponentiellen Zunahme von Lösegeldzahlungen an Ransomware-Hacktivisten ist die Wahrscheinlicht, dass diese Aktivitäten auch in Zukunft – mit einer höheren Frequenz – Anwendung finden, groß. Banken decken sich, nachdem sie diese Gefahr erkannt haben, mit Bitcoins ein, damit ihre Kunden (und sie selbst) Cyber-Kriminelle gegebenenfalls schnell für das Entsperren gehackter Daten bezahlen können.

Die finanziellen Auswirkungen auf Organisationen gehen weit über das bezahlte Lösegeld hinaus. Die Ausfallzeiten führen zu Umsatz- und Produktivitätsverlusten in einer Größenordnung von Tausenden und häufig Hunderttausenden Dollar. Organisationen aus verschiedensten Branchen können diese Folgen bestätigen.

UMFANG DER BEDROHUNG

Daten sind das Herz der meisten modernen Unternehmen – von kleinen Firmen bis zu Großkonzernen. Die Digitalisierung von immer mehr Assets in Kombination mit der zunehmenden Bedeutung der Cloud rückt Daten in das Fadenkreuz von Cyber-Kriminellen. Dies ist ein wachsendes Problem, da der Datenumfang sich alle zwei Jahre mehr als verdoppelt.[1]

Da auch Cyber-Kriminelle den Wert der Daten kennen, wenden sie sich mehr und mehr Ransomware als Einnahmequelle zu. Sie infiltrieren IT-Systeme und greifen mit verschiedenen Hacking-Methoden an, mit denen sie Dateien verschlüsseln, sperren und herausfiltern. Wenn gehackte Unternehmen nicht mehr auf geschäftskritische Informationen zugreifen können, sind sie gezwungen, den Cyber-Kriminellen Geld für die Freigabe der Daten zu zahlen. Die technische Komplexität vieler dieser Vorgänge ist bereits so weit fortgeschritten, dass Cyber-Kriminelle ihren Opfern Live-Support bereitstellen, der sie durch die entsprechenden Schritte führt, um die Zahlung vorzunehmen und wieder Zugriff auf ihre eigenen Daten und IT-Systeme zu erhalten.

SPRUNGHAFTER ANSTIEG DER RANSOMWARE-ANGRIFFE

Wie ernst ist die Gefahr durch Ransomware wirklich? Im vergangenen Jahr haben sich die Ransomware-Angriffe mehr als verdoppelt.[2] Täglich kommt es zu mehr als 4.000 Ransomware-Angriffen, die durchschnittlich zwischen 30.000 und 50.000 Geräte pro Monat infizieren.[3] Und das Potenzial für weiteres Wachstum ist riesig. Selbst bei dieser Steigerungsrate macht Ransomware jedoch nur zwei Prozent der gesamten Malware-Angriffe aus.[4]

Die finanziellen Folgen von Ransomware sind ebenfalls enorm angestiegen. Im Jahr 2015 wurde eine Gesamtsumme von 24 Millionen USD an Lösegeld bezahlt. 2016 ist diese Zahl auf mehr als 850 Millionen USD angestiegen.[5] Der von Cyber-Kriminellen verlangte Betrag folgt dem gleichen Weg: Der durchschnittlich für jeden Angriff verlangte Betrag ist von 294 USD im Jahr 2015 auf 679 USD im Jahr 2016 in die Höhe geschnellt.[6]

Die umfangreichsten Folgen von Ransomware betreffen jedoch nicht das bezahlte Lösegeld. Dreiundsechzig Prozent der Unternehmen, die im vergangenen Jahr Opfer eines Ransomware-Angriffs wurden, geben an, dass der Angriff zu geschäftsbedrohenden Ausfallzeiten geführt hat. Weitere 48 Prozent berichten, dass er einen Verlust von Daten oder Hardware nach sich gezogen hat. Und jedes vierte Unternehmen, das Lösegeld für die Wiedergewinnung seiner Daten bezahlt hat (42 Prozent geben zu, dass sie Lösegeld bezahlt haben), hat die Daten nicht mehr zurückerhalten.[7] Aus diesem Grund rät das FBI Opfern, kein Lösegeld zu zahlen.

DIE SPITZE DES EISBERGS

Diese Zahlen sind jedoch wahrscheinlich kein getreues Abbild des Ausmaßes des Problems. Ransomware-Angriffe werden in großem Umfang nicht gemeldet – nur einer von vier Angriffen wird tatsächlich bekannt. Mehr als die Hälfte der Unternehmen geben zu, dass sie im vergangenen Jahr bereits einen Ransomware-Angriff erfahren haben.[8] Vierunddreißig Prozent von ihnen verloren auf diesem Wege Geld und 20 Prozent waren gezwungen, ihr Geschäft zu schließen! Bei genauer Betrachtung sind die finanziellen Auswirkungen alarmierend. Aber es wird noch schlimmer: 3,5 Prozent der Unternehmen geben an, dass als Folge des Ransomware-Angriffs Leben in Gefahr waren.[9]

Unternehmen, die glauben, zu klein für Ransomware-Angriffe zu sein, sollten sich nicht zu sicher fühlen. Kleine Unternehmen verfügen häufig über keine eigenen IT-Experten und verwalten ihre IT-Systeme ohne die erforderlichen Kontrollfunktionen. Das macht sie Ransomware-Angriffen gegenüber durchaus anfällig. Diese Unternehmen, die ohne geeignete Vorkehrungen zum Schutz ihrer Daten und ohne entsprechende Wiederherstellungsfunktionen agieren, werden schnell zu einem Ransomware-Ziel. Aktuelle Untersuchungen berichten, dass durch Ransomware verursachte Ausfallzeiten kleine Unternehmen ca. 8.500 USD pro Stunde kosten. Dies summiert sich zu einem Gesamtverlust von 75 Milliarden USD pro Jahr.[10]

Ransomware infizierte **30.000** bis **50.000** Geräte pro Monat.

850 Millionen USD

wurden 2016 für **Ransomware-Angriffe** gezahlt.

Es gibt eine große Dunkelziffer von Ransomware-Angriffen. Weniger als **1 von 4** Unternehmen informiert über einen Angriff.

63 % der Unternehmen verzeichneten **geschäftsbedrohende** Ausfallzeiten.

34 % der Unternehmen verloren Geld.

GESCHÄFTLICHE AUSWIRKUNGEN VON RANSOMWARE

Die Kosten für Ausfallzeiten des Systems und die Nichtverfügbarkeit von Informationen aufgrund von Ransomware-Angriffen belaufen sich bereits heute auf Milliarden von Dollar. Diese Zahl kann auf Dutzende Milliarden anwachsen, wenn Ransomware-Hacktivisten auch IoT-Geräte zu ihrem Ziel machen.

DOXING

Cyber-Kriminelle sind erfindungsreich. Einige von ihnen beschränken sich nicht nur darauf, die gesperrten Daten zu löschen, sondern drohen mit ihrer Veröffentlichung (dem so genannten „Doxing"). Für Unternehmen, die mit privaten und sensiblen Kundendaten arbeiten, wie Finanzdienstleister, Krankenhäuser oder Anwaltsfirmen, kann dies katastrophale Konsequenzen haben. Sie verlieren nicht nur den guten Ruf ihres Unternehmens, sondern müssen ihre Kunden entsprechend den geltenden Datenschutzbestimmungen, wie dem Health Information Portability and Accountability Act, über den Vorfall informieren und weitere umfangreiche Maßnahmen ergreifen, die schnell zu Ausgaben von Hunderttausenden – oder sogar Millionen – von Dollar führen können.

BITCOINS FÜR LÖSEGELDZAHLUNGEN

Die Auswirkungen von Ransomware reichen über die gehackten Unternehmen hinaus. Nehmen wir zum Beispiel die Banken. Da die potenziellen Folgen des Verlusts oder der Nichtverfügbarkeit von Daten in Minuten oder sogar Sekunden gemessen wird, können Unternehmen nicht mehrere Tage warten, bis Cyber-Kriminelle ihnen den Zugriff auf die gehackten Daten zurückgeben. Aus diesem Grund halten Banken Bitcoins vor – da es gewöhnlich drei bis fünf Tage dauert, diese zu erhalten –, damit ihre Kunden Cyber-Kriminelle sofort bezahlen können.[11]

WEGE VON RANSOMWARE IN IHR SYSTEM

VERBREITUNG VON RANSOMWARE

Wie gelangt Ransomware in Ihr System? Zur Beantwortung dieser Frage muss zuerst untersucht werden, wie Ransomware verbreitet wird. Hierfür können alle digitalen Wege genutzt werden: E-Mail, Website-Anhänge, Geschäftsanwendungen, soziale Netzwerke und USB-Laufwerke sowie weitere digitale Übertragungswege. E-Mails sind nach wie vor die beliebteste Übertragungsmöglichkeit, wobei Cyber-Kriminelle an erster Stelle Links und an zweiter Stelle Anhänge verwenden.

- E-Mail-Links, 31 %
- E-Mail-Anhänge, 28 %
- Website-Anhänge, 24 %
- Unbekannte Quellen, 9 %
- Social Media, 4 %
- Geschäftsanwendungen, 1 %

Im Fall von E-Mails werden Phishing-E-Mails als Lieferbenachrichtigung oder fingierte Aufforderungen zu Software-Updates gesendet. Sobald der Benutzer auf den Link oder den Anhang klickt, werden häufig (in jüngerer Vergangenheit seltener) ganz offen weitere schadhafte Komponenten heruntergeladen. Diese verschlüsseln dann Dateien mit der 2048-Bit-RSA-Verschlüsselung mittels privater Schlüssel, wodurch es für den Benutzer nahezu unmöglich wird, die Dateien wieder zu entschlüsseln. In anderen Fällen wird Ransomware als Datei auf einer Website eingebettet. Wenn der Benutzer diese Datei herunterlädt und installiert, wird der Angriff aktiviert.

UNTERSCHIEDLICHE RANSOMWARE-TYPEN

Ransomware-Angriffe können auf verschiedene Weise erfolgen. Im vergangenen Jahr haben sich diese Angriffe erheblich verändert. Herkömmliche Ransomware zielt auf Ihre Daten ab und sperrt Dateien, bis das Lösegeld bezahlt wird. Bedingt durch das schnelle Wachstum des Internets der Dinge (IoT) hat sich eine neue Ransomware-Variante entwickelt. Diese sucht nicht nach den Daten eines Unternehmens, sondern zielt auf Steuerungssysteme (z. B. von Fahrzeugen, Fertigungslinien, Antriebssystemen) ab und fährt sie herunter, bis das Lösegeld gezahlt wird.

Folgende Typen von Ransomware werden aktuell am häufigsten verwendet:

- **Standard-Ransomware.** Bestimmte Ransomware existiert als serienmäßige Software, die Cyber-Kriminelle auf Darknet-Marktplätzen kaufen und auf ihren eigenen Servern installieren können. Das Hacken und Verschlüsseln von Daten wird dann direkt von der Software gelenkt. Zu der serienmäßigen Ransomware zählen beispielsweise Stampado und Cerber.
- **Ransomware-as-a-Service.** CryptoLocker ist wahrscheinlich das bekannteste Ransomware-as-a-Service-Modell. Nachdem seine Server aus dem Verkehr genommen wurden, hat sich CTB-Locker zur häufigsten Ransomware-as-a-Service-Angriffsmethode entwickelt. Ein weiterer schnell wachsender Ransomware-as-a-Service ist Tox, ein Kit, das Cyber-Kriminelle herunterladen können. Das Ergebnis erstellt eine spezielle ausführbare Datei, die von den Cyber-Kriminellen installiert oder verteilt werden kann. 20 Prozent der Brutto-Lösegeldeinnahmen gehen in diesem Fall in Form von Bitcoins an Tox.
- **Ransomware-Partner-Programme.** Cyber-Kriminelle, die sich als Partner anmelden, erhalten Zugang zu einem Ransomware-as-a-Service-Modell, das sie auf ihre eigenen Ziele richten können. Sie erhalten dabei häufig bis zu 70 Prozent des Gewinns.[12]

- **Angriffe auf IoT-Geräte.** Ransomware infiltriert IoT-Geräte, die geschäftskritische Systeme steuern. Die Software fährt das System herunter, bis ein Lösegeld für das Entsperren des Systems gezahlt wird. Einige dieser IoT-Geräte steuern unternehmenskritische oder lebenserhaltende Systeme, sodass die Folgen ihrer Unverfügbarkeit erheblich oder sogar katastrophal sein können.[13]

Ransomware-Varianten sind im Jahr 2016 geradezu explodiert. FortiGuard Labs erkannte an jedem Tag des gesamten Jahres neue Varianten. Interessanterweise verwendet Ransomware zusätzlich zu polymorphem Code häufig metamorphen Code, um ihre digitale Identität bei gleicher Vorgehensweise zu ändern. Das schnelle Wachstum und die kontinuierliche Weiterentwicklung machen es für Unternehmen, die sich auf herkömmliche signaturbasierte Antivirus-Lösungen verlassen, noch schwerer, Schritt zu halten. Wenn eine Variante identifiziert und auf die schwarze Liste gesetzt wurde, sind Cyber-Kriminelle bereits zu einer neuen Variation übergegangen. Dies erklärt, warum nahezu drei Viertel der Unternehmen, die 2016 Ransomware-Angriffen ausgesetzt waren, eine oder mehrere Infektionen erlitten.[14]

Praktisch jedes Betriebssystem ist heute Ransomware-Angriffen ausgesetzt. Angriffe richten sich auch auf die Cloud und mobile Geräte. Ransomware-Angriffe auf Android haben sich beispielsweise innerhalb eines Jahres ab April 2015 vervierfacht.[15]

TYPISCHER RANSOMWARE-WORKFLOW

Die meisten Ransomware-Angriffe erfolgen über Spear-Phishing, bei dem eine E-Mail, die vorgeblich von einer bekannten Person oder einem bekannten Unternehmen stammt, auf eine Person abzielt. Bislang wurde Ransomware vorrangig über Spear-Phishing verbreitet. In diesen Fällen enthält die E-Mail einen infizierten Link oder einen Anhang. Diese E-Mail-Links oder -Anhänge können problemlos und schnell geändert werden, sodass Cyber-Kriminelle mit einem einfachen Code eine Vielzahl neuer Websites oder Anhänge erstellen können, über die später weitere Komponenten heruntergeladen werden. Damit gelingt es ihnen, E-Mail-Filter zu umgehen und im Posteingang des Endbenutzers zu landen.

In anderen Fällen besucht ein Benutzer eine infizierte Website oder Geschäftsanwendung, von wo die Ransomware dann gestartet wird. Häufig ist die Ransomware so konfiguriert, dass sie den größeren Teil der Schadensroutinen startet und herunterlädt, ohne dass der Benutzer auf weitere Elemente klicken muss. In einer zunehmenden Anzahl von Fällen wird ein infiziertes IoT-Gerät verwendet, um geschäftskritische oder lebenserhaltende Systeme zu kontrollieren – was gewöhnlich bedeutet, dass sie heruntergefahren werden.

Wenn die Ransomware erfolgreich gestartet wurde, laufen gewöhnlich die folgenden Schritte ab:

1. Wenn der Benutzer auf den infizierten Link oder Anhang klickt, wird die Ransomware über eine PowerShell oder eine andere Erweiterung gestartet.
2. Das infizierte Gerät kommuniziert mit dem Server des Cyber-Kriminellen (häufig über einen indirekten Weg, z. B. Google Apps), von dem es Anweisungen erhält. Diese umfassen häufig das Herunterladen neuer Schadensroutinen, die nachfolgend Dateien auf dem Gerät der Person verschlüsselt.
3. Nach Abschluss dieses Vorgangs (der manchmal weniger als eine Minute dauert) wird eine Lösegeldforderung übermittelt, in der im Gegenzug für einen Entschlüsselungscode Bitcoins gefordert werden.
4. Gleichzeitig versucht die Ransomware, sich im Netzwerk des Unternehmens weiter zu verbreiten, um weitere Systeme zu infiltrieren.

Eine neue Strategie von Ransomware-Hacktivisten ist der Angriff und die Infektion anfälliger Geschäftsserver.[18] Auf diese Weise können sie Hosts identifizieren und angreifen und die Anzahl von potenziell infizierten Servern und Geräten in einem Netzwerk vervielfachen. Der Zeitrahmen des Angriffs wird somit komprimiert, wodurch dieser Angriffstyp viraler ist, als solche, die bei einem Endbenutzer beginnen. Diese Entwicklung könnte dazu führen, dass Opfer mehr für Entschlüsselungscode zahlen und die Zeiten bis zum Wiedererlangen der verschlüsselten Daten länger werden.

SAAS-BASIERTE INFEKTIONEN

Auf die Frage, bei welchen SaaS-basierten Anwendungen sie bereits Infektionen durch Ransomware gesehen haben, antworteten IT-Experten in einer kürzlich durchgeführten Umfrage Folgendes:

- Dropbox, 70 %
- Microsoft Office 365, 29 %
- Google Apps, 12 %
- Box, 6 %
- Salesforce, 3 %

ENTWICKLUNG VON RANSOMWARE[16]

Top-Ransomware-Produktfamilien 2016

1. Locky
2. CryptoWall
3. CryptXXX
4. Bitman
5. Onion (CTB-Locker)

Top-Ransomware-Produktfamilien 2015

1. CryptoWall
2. Blocker
3. Onion (CTB-Locker)
4. Snocry
5. Bitman

97 %
der Phishing-E-Mails übertragen nun Ransomware.[17]

KEINE IMMUNITÄT

Unternehmen, die glauben, dass sie Ransomware-Angriffen gegenüber immun sind, weil sie alle grundlegenden Sicherheitsmaßnahmen implementiert haben, sollten sich nicht zu sicher sein. Laut einer Umfrage von Anbietern gehosteter Lösungen verfügten die meisten angegriffenen Unternehmen über Basis-Sicherheitsfunktionen.[19]

- Anti-Virus- und Anti-Malware-Software, 93 %
- E-Mail- und Spam-Filter, 77 %
- Patches/Updates für Apps, 58 %
- Werbe- und Popup-Blocker, 21 %

VIRALE VERBREITUNG

Ransomware ist viral und verbreitet sich in 63 Prozent aller Fälle über Netzwerke. In den restlichen Fällen bleibt sie in einem einzelnen System isoliert.[20]

ANGRIFFE IN DER PRAXIS

Nahezu jede Branche und Unternehmen jeder Größe sind von Ransomware-Angriffen betroffen. Dabei steht der Fertigungsbereich ganz oben auf der Liste der angegriffenen Branchen (16 Prozent). Der Versorgungs- und Energiesektor folgt knapp dahinter (15,4 Prozent) und auch die Bereiche Technologie, Dienstleistungen, Einzelhandel, Gesundheitswesen, Finanzdienstleistungen und der Rechtsbereich weisen einen erheblichen Anteil auf. Einige Berichte nennen den Dienstleistungssektor als den Bereich mit der schnellsten Zunahme von Ransomware-Angriffen.

Im Folgenden werden die Folgen von Ransomware auf diese führenden Sektoren untersucht. Dabei werden spezifische Beispiele für gehackte Unternehmen angeführt, die nicht nur das Lösegeld gezahlt haben, sondern auch erhebliche finanzielle und geschäftliche Auswirkungen hinnehmen mussten.

GESUNDHEITSWESEN

Das Gesundheitswesen ist ein Sektor, in dem große Sorge hinsichtlich Ransomware besteht. Das ist sehr gut nachvollziehbar, da viele IT-Systeme und Daten in Gesundheitswesen mit der Patientenbetreuung in Zusammenhang stehen. Jeder Systemausfall und jede Situation, in der kein Datenzugriff möglich ist, kann Patientenleben gefährden. Selbst wenn der Ransomware-Angriff nicht das System und die Daten für die Patientenbetreuung betrifft, kann der Verlust von Patientendaten erhebliche Geldbußen und einen großen Zeitaufwand für die Behebung des Schadens nach sich ziehen.

Durch das Doxing, den taktischen Ransomware-Angriffen, bei denen Cyber-Kriminelle drohen, private Daten nicht zu löschen, sondern zu veröffentlichen, sind die Konsequenzen noch drastischer. Nehmen Sie die Ransomware-Angriffe auf die für die Patientenbetreuung verwendeten IoT-Geräte hinzu, so sind die Auswirkungen lebensbedrohend.

Die Angriffe werden in den kommenden Jahren nicht nachlassen. Es wird davon ausgegangen, dass sich die Zahl der Ransomware-Angriffe auf Gesundheitsdienstleister im nächsten Jahr verdoppeln wird. Verglichen mit anderen Branchen sind Gesundheitsdaten im Darknet 50 Mal teurer als etwa Finanzdaten. Gestohlene Gesundheitsdaten können bis zu 60 USD pro Datensatz erzielen.[21] Es gibt zahllose Beispiele für Gesundheitsdienstleister, die von Ransomware-Angriffen betroffen waren. Im Folgenden werden drei Beispiele genannt:

Hacktivisten erhielten Zugriff auf eine MongoDB-Datenbank mit geschützten Gesundheitsdaten von 200.000 Patienten des *Emery Brain Health Center*. Der Inhalt der Datenbank wurde vollständig gelöscht und für die Rückgabe der Daten wurden ein Lösegeld in Höhe von 180.000 USD in Bitcoins verlangt.

Das *Hollywood Presbyterian Medical Center in Hollywood, Kalifornien* erklärte den internen Ausnahmezustand, nachdem seine Systeme mit Locky-Ransomware infiziert worden waren. Ärzte und anderes medizinisches Personal konnten nicht mehr auf die elektronischen Patientendaten zugreifen. Die Mitarbeiter waren gezwungen, Patientendaten mit Papier und Bleistift zu protokollieren und miteinander per Fax – anstelle von E-Mail – zu kommunizieren. Für das Entschlüsseln der gesperrten Dateien verlangte der Hacktivist 40 Bitcoins (also ca. 17.000 USD), die vom Krankenhaus gezahlt wurden.

Aber Cyber-Kriminelle geben ihren Opfern nicht immer den Zugang zu ihren Daten zurück. Im Fall des *Kansas Heart Hospital in Wichita im US-Staat Kansas* zahlte das Krankenhaus das zunächst verlangte Lösegeld. Die Hacktivisten entsperrten die Dateien jedoch nicht vollständig und verlangten stattdessen noch mehr Geld. An diesem Punkt lehnte das Krankenhaus ab, das zusätzliche Lösegeld zu zahlen.

VERSORGUNGS- UND ENERGIEBRANCHE

Die Versorgungs- und Energiebranche ist ebenso vielen Cyber-Angriffen ausgesetzt wie alle anderen Bereiche. Die industriellen Steuerungssysteme (ICS), die für die Verwaltung und Steuerung der kritischen Infrastruktur für Versorgungs- und Energieunternehmen verwendet werden, bieten Cyber-Kriminellen neue Möglichkeiten – auch den Ransomware-Hacktivisten.

Glücklicherweise war im Fall des Unternehmens *Lansing Board of Water & Light*, das die Stadt Lansing in Michigan versorgt, das ICS-System nicht von dem Spear-Phishing-Angriff betroffen, der das Versorgungsunternehmen zwang, seinen Server und seine Telefonleitungen eine Woche lang herunterzufahren. Ursache dafür war wahrscheinlich das Öffnen einer E-Mail mit einer infizierten Datei durch einen Mitarbeiter. Die Ransomware sperrte sehr schnell das E-Mail- und Buchführungssystem, Drucker und andere technologische Einrichtungen. Erst nach einer Woche von Wiederherstellungsmaßnahmen gelang es dem Unternehmen, seine Systeme wieder online zu bringen.

PRODUZIERENDES GEWERBE

Die Fertigungsbranche entwickelt sich zunehmend zu einem interessanten Ziel für Ransomware-Hacktivisten. Hersteller unterliegen einem höheren Risiko als andere Branchen, da sie nicht denselben aufsichtsbehördlichen und Compliance-Vorschriften wie andere Branchen, beispielsweise Finanzdienstleister, unterliegen.

Sie nutzen IT-Systeme, auf denen geistiges Eigentum und firmeneigene Informationen gespeichert sind, und legen besonders großen Wert auf effiziente Prozesse und Abläufe. Eine Unterbrechung kann zu Ausfall- und Stillstandzeiten führen, die eine Abnahme der finanziellen Rentabilität nach sich zieht. Für Fertigungsunternehmen ist Zeit Geld. Sie ziehen es daher vor, Lösegeld zu zahlen, um ihre Systeme so schnell wie möglich wieder zum Laufen zu bringen.

Allein im letzten Jahr richteten sich mehr als drei Viertel der verzeichneten 8,63 Millionen Ransomware-Angriffe auf Unternehmen mit mehr als 1.000 Mitarbeitern. Das Botnet Necurs war das bevorzugte Ransomware-Übertragungswerkzeug im Bereich der Fertigung und wurde in 41 Prozent der Fälle eingesetzt. Deutlich dahinter folgt Conficker mit 17,7 Prozent.[23]

Ein Betonhersteller verzeichnete einen Produktionsausfall von über einer Woche, nachdem ein Mitarbeiter auf einen E-Mail-Anhang klickte, der mit der Ransomware CryptoWall infiziert war. Ransomware verbreitete sich im gesamten Unternehmensnetzwerk und verschlüsselte Buchhaltungsdaten und zentrale Dateien mehrerer Produktionssysteme. Der Vorgang wurde zu Beginn des Geschäftstags erkannt, als ein Arbeiter nicht in der Lage war, auf Produktionsdateien zuzugreifen und die Produktion zu starten. Selbst nachdem das Unternehmen das Lösegeld nach zwei Tagen zahlte, waren einige der Buchhaltungsdateien weiterhin gesperrt. Da das Unternehmen über keine Backups der Daten verfügte, musste es ein langwieriges Wiederherstellungsprojekt starten.

BILDUNG

Die Schlagzeilen über Ransomware-Angriffe konzentrieren sich gewöhnlich auf Datendiebstähle im Gesundheitswesen, bei Finanzdienstleistern und in anderen Branchen. Bildungseinrichtungen stehen jedoch weit oben auf der Liste der Organisationen, die von Ransomware-Angriffen betroffen sind. Warum? Bildungseinrichtungen verfügen über Sozialversicherungsnummern, medizinische Daten, Finanzdaten und geistiges Eigentum von Fakultät, Mitarbeitern und Studenten und stellen somit ein lukratives Ziel dar. Die Cyber-Sicherheit von Schulen aller Stufen ist besonders gering, was den Angriff für Cyber-Kriminelle sehr interessant macht.

Die *University of Calgary* verzeichnete einen Ransomware-Angriff, durch den ihr E-Mail-Server blockiert wurde. Die Universität bezahlte ein Lösegeld von 16.000 Dollar für einen Schlüssel, mit dem sie die verschlüsselten Server-Dateien entschlüsseln konnten. Glücklicherweise isolierten die IT-Mitarbeiter die Infiltration, bevor andere Systeme angegriffen wurden.

Das *Los Angeles Valley College* zahlte nach einem Ransomware-Angriff, bei dem Hunderttausende Dateien in seinem Netzwerk, dem E-Mail- und Voicemail-System gesperrt wurden, fast 28.000 USD in Bitcoins. Die Infektion wurde am 30. Dezember 2016 erkannt und das College entschied am 4. Januar 2017, einen Tag nach dem Start des Wintersemesters, das Lösegeld zu zahlen.

Ransomware in Bildungseinrichtungen ist ein globales Problem. Auch die *Queen's University in Belfast in Irland* weiß das. Im letzten Jahr gelang es Ransomware bei drei Angriffen, in ihr Netzwerk zu gelangen. In einem Fall zahlte die Queen's University ein Lösegeld von ca. 600 USD, nachdem Hacktivisten einen Windows XP-Server mit Dokumenten und Bildern infizierten.

FINANZDIENSTLEISTER UND BANKEN

Die Breite der von Finanzdienstleistern und Banken gespeicherten Informationen über ihre Kunden macht sie zu einem vorrangigen Ziel von Ransomware-Angriffen. Finanzdienstleistunger und Banken sind sich einig: 55 Prozent nennen Ransomware als größte Cyber-Bedrohung. Nahezu ein Drittel von ihnen erklärt außerdem, bedingt durch Cyber-Angriffe zwischen 100.000 USD und 500.000 USD verloren zu haben.[24]

Volksbanken und kleinere Banken beobachten einen signifikanten Anstieg des Ransomware-Hacktivismus. Sie verzeichneten im Jahr 2015 54 Prozent der gesamten Angriffe auf Finanzdienstleister und Banken, verglichen mit 81 Prozent im Jahr 2016.[25] Dies ist weitgehend darauf zurückzuführen, dass sie traditionell kleinere Security-Budgets als größere Mitbewerber haben.

BEHÖRDEN

Fast 10 Prozent der von Ransomware-Angriffen betroffenen Organisationen sind öffentliche Einrichtungen. Da sie kritische Informationen auf ihren Systemen speichern, stellen Behörden ein verlockendes Ziel dar.

Der Staat von Ohio gab letztes Jahr eine Warnung an lokale Gemeinden aus, in der darauf hingewiesen wurde, dass Ransomware-Angriffe stark zunehmen und lokale Gemeinden sich auf diese Gefahren mit angemessenen Technologien und Prozessen vorbereiten sollten.

Mehrere lokale Gemeinden in Ohio waren im vergangenen Jahr Ransomware-Opfer. Mehr als 170.000 Stimmabgaben in *Henry County* waren kompromittiert. Der Hacktivist drohte, sie zu veröffentlichen, wenn kein Lösegeld bezahlt würde. Das Lösegeld wurde nicht bezahlt und die Daten wurden bis heute nicht veröffentlicht.

Die Computersysteme für den *Morrow County Ohio Court* waren mit Ransomware infiziert. Der Landkreis entschied sich, das Bitcoin-Lösegeld nicht zu zahlen, und die Dateien wurden von den Cyber-Kriminellen gelöscht. Leider waren die Backup-Systeme des Gerichtssystems nicht auf dem neuesten Stand und Morrow County besaß die Dateien nur in Papierform. Die Wiederherstellung der Dateien anhand der Papierdokumente kostete den Landkreis über 30.000 USD an Personalaufwand.

Cyber-Kriminelle zielen sogar auf Strafverfolgungsbehörden ab. Die Computersysteme des *Sheriffs von Lincoln County in Maine* waren mit Ransomware infiziert. Nach mehreren Versuchen, die Informationen wiederherzustellen, entschloss sich die Behörde für die Informationen etwa 300 USD in Bitcoins an den Hacktivisten zu zahlen.

SCHLUSSFOLGERUNGEN

Nachdem Cyber-Kriminelle im Jahr 2016 ihre Einnahmen aus Ransomware-Angriffen um das Fünfunddreißigfache steigern konnten, werden Häufigkeit und Komplexität, Geschwindigkeit und Umfang der Angriffe zweifellos zunehmen. Da Ransomware weiterentwickelt wird und zu einer ständig wachsenden Bedrohung für Organisationen praktisch jeder Art und Größe wird, sollten Organisationen folgende Vorsichtsmaßnahmen unbedingt beachten:

1. **Stoppen bekannter Bedrohungen.** Wählen Sie eine Sicherheitslösung, die bekannte Ransomware-Bedrohungen auf allen Angriffswegen stoppt. Hierzu ist ein mehrstufiges Sicherheitsmodell erforderlich, das Netzwerk-, Endgeräte-, Anwendungs- und Rechenzentrums-Controls umfasst und über weltweite Bedrohungsdaten verfügt.
2. **Erkennen neuer Bedrohungen.** Da sich die bestehende Ransomware kontinuierlich ändert und neue Ransomware Verbreitung findet, ist es unerlässlich, die richtige Sandbox und andere moderne Erkennungsverfahren einzurichten, um die verschiedenen Varianten auf den jeweiligen Übertragungswegen zu erkennen.
3. **Das Unbekannte abwehren.** Verwertbare Echtzeit-Bedrohungsdaten müssen zwischen den verschiedenen Sicherheitsebenen (und generell Anbieterprodukten) ausgetauscht und selbst an die breitere Cyber-Sicherheitsgemeinde außerhalb Ihrer Organisation, wie etwa die Computer Emergency Response Teams (CERTs), Information Sharing and Analysis Centers (ISACs) und Branchenbündnisse wie die Cyber Threat Alliance, weitergegeben werden. Diese schnelle Weitergabe ist der beste Weg, umgehend auf Angriffe zu reagieren und die Bedrohungskette zu durchbrechen, bevor sie mutiert oder auf andere Systeme oder Organisationen übergreift.
4. **Vorbereitet sein auf das Unerwartet.** Die Segmentierung der Netzwerksicherheit hilft beim Schutz vor wurmähnlichem Verhalten, das zum Beispiel von SamSam und ZCryptor an den Tag gelegt wird. Ebenso wichtig sind Datensicherung und -wiederherstellung. Unternehmen, die über aktuelle Datenbackups verfügen, sind in der Lage, Lösegeldzahlungen abzulehnen und ihre Systeme schnell und problemlos wiederherzustellen.
5. **Erstellen von Backups kritischer Systeme und Daten.** Wenngleich die Wiederherstellung eines verschlüsselten Systems ein zeitaufwendiger Prozess sein kann, der die Geschäftsabläufe unterbricht und die Produktivität belastet, ist das Wiederherstellen mithilfe eines Backups die weitaus bessere Option gegenüber einer Geiselhaft ohne jede Garantie, dass die Lösegeldzahlung zu einer Entsperrung und Wiederherstellung Ihrer Daten und Systeme führen wird. In diesem Fall brauchen Sie die richtige Technologie, geeignete Prozesse und auch Geschäftspartner, um sicherzustellen, dass Ihre Backups die Geschäftsanforderungen erfüllen und ihre Wiederherstellung ohne großen Zeitaufwand erfolgen kann.

[1] „The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things“, IDC, April 2014.

[2] „Non-Malware Attacks and Ransomware Take Center Stage in 2016“, Carbon Black Threat Report, 2016.

[3] Minal Khatri, „Ransomware Statistics – Growth of Ransomware in 2016“, Systweak, 25. August 2016.

[4] „Non-Malware Attacks.“

[5] Ibid.

[6] Khatri, „Ransomware Statistics.“

[7] „State der Channel Ransomware BERICHT 2016“, Datto, 2016.

[8] Angela Moscaritolo, „Ransomware Hit 40 Percent of Businesses in the Last Year“, PC Magazine, 3. August 2016.

[9] Ibid.

[10] „Non-Malware Attacks.“

[11] Adam Chandler, „How Ransomware Became a Billion-Dollar Nightmare for Businesses“, The Atlantic, 3. September 2016.

[12] Vincent Weafer, „Franchising Ransomware“, DARKReading.com, 1. Juli 2015.

[13] Ben Dickson, „What Makes IoT Ransomware a Different and More Dangerous Threat?“, TechCrunch, 2. Oktober 2016.

[14] „The Complete Guide to Ransomware“, Barkly, letzter Zugriff 30. Januar 2017.

[15] Khatri, „Ransomware Statistics.“

[16] „Non-Malware Attacks.“

[17] „2016 Q3 Malware Review“, PhishMe, Oktober 2016.

[18] „Ransomware Getting More Targeted, Expensive“, KrebonSecurity.com, 20. September 2016.

[19] „State of the Channel Ransomware Report.“

[20] Ibid.

[21] Jennifer Schlesinger, „Dark Web Is Fertile Ground for Stolen Medical Records“, CNBC, 11. März 2016.

[22] Erin Dietsche, „12 Healthcare Ransomware Attacks of 2016“, Health IT & CIO Review, 29. Dezember 2016.

[23] Bill McGee, „Move Over Healthcare, Ransomware Has Manufacturing in Its Sights“, Fortinet Blog, 6. Juni 2016.

[24] G. Mark Hardy, „From the Trenches: 2016 Survey on Security and Risk in the Financial Sector“, SANS Institute, Oktober 2016.

[25] „Cyber Attacks on Financial Firms Up; Ransomware Attacks Way Up“, Insurance Journal, 22. Juli 2016.

DEUTSCHLAND
Feldbergstrasse 35
60323 Frankfurt
Deutschland
Verkaufsabteilung:
+49 69 310 192 0

SCHWEIZ
Riedmühlestrasse 8
8305 Zürich-Dietlikon
Schweiz
Verkaufsabteilung:
+41 44 833 68 48

ÖSTERREICH
Wienerbergstrasse 11
Turm A / 9.OG
1100 Wien
Österreich
Verkaufsabteilung:
+43 1 22787 120

KONZERNSITZ
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
USA
Tel.: +1 (408) 235 7700
www.fortinet.com/sales

VERTRIEBSBÜRO EMEA
905 rue Albert Einstein
06560 Valbonne
Frankreich
Tel.: +33 (0)4 8987 0500

VERTRIEBSBÜRO APAC
300 Beach Road 20-01
The Concourse
Singapur 199555
Tel.: +65 6513 3730

LATEINAMERIKA
ZENTRALE
Sawgrass Lakes Center
13450 W. Sunrise Blvd.,
Suite 430
Sunrise, FL 33323
Tel: +1 954 368 9990

09. Februar 2017