proofpoint.

E-BOOK

Ransomware-Leitfaden 2022

Das sollte jedes Unternehmen vor, während und nach einem Angriff beachten

proofpoint.com/de

Inhaltsverzeichnis

Kurzfassung

Ransomware ist eine seit langem bekannte Bedrohung, die bis heute Probleme bereitet. Der Begriff Ransomware bezieht sich darauf, dass nach der Sperrung der Dateien des Opfers ein Lösegeld (engl. „ransom“) verlangt wird. Diese Malware-Form ist für moderne Unternehmen eine große Gefahr, da sie derzeit die größten Schäden anrichtet. In den USA kam es im Jahr 2021 zu schwerwiegenden Zwischenfällen unter anderem in der Kraftstoffindustrie[1], in der Lebensmittelbranche [2] und im Gesundheitswesen[3] – kein Ziel ist dabei tabu. Deshalb ist es nun umso wichtiger, mit einem Plan Risiken zu minimieren und festzulegen, wie im Fall einer Ransomware-Infektion vorgegangen werden soll.

Warum Ransomware immer noch existiert

Ransomware hält sich im Wesentlichen aus vier Gründen:

- Lösegelder können dank Bitcoin und anderen digitalen Währungen einfacher als bei anderen Betrugsarten kassiert werden.
- Die Angreifer haben viele Übertragungskanäle (z. B. bestehende Kompromittierungen einer Umgebung), die die Erfolgschancen erhöhen.
- Viele Unternehmen haben eine schwache oder veraltete Cyberabwehr sowie unzureichende Backup- und Wiederherstellungsroutinen und sind daher besonders attraktive Ziele.
- Angreifer suchen ihre Opfer zunehmend gezielter aus und täuschen sie mit immer raffinierteren Taktiken.

Wie bei den meisten Cyberangriffen muss auch bei Ransomware jemand zu bestimmten Aktionen verleitet werden, zum Beispiel zum Öffnen eines Anhangs oder Klicken auf eine URL.

Abwehr von Ransomware

Ransomware kompromittiert Daten und Systeme, doch zu Beginn eines Angriffs werden die Mitarbeiter ins Visier genommen. Wie bei den meisten Cyberangriffen muss auch bei Ransomware jemand zu bestimmten Aktionen verleitet werden, zum Beispiel zum Öffnen eines Anhangs oder Klicken auf eine URL. Deshalb ist für die Abwehr von Ransomware ein personenzentrierter Ansatz erforderlich.

Der vorliegende Leitfaden soll als Ausgangspunkt dienen.

1 David E. Sanger, Clifford Krauss und Nicole Perlroth *(New York Times)*: „Cyberattack Forces a Shutdown of a Top U.S. Pipeline“ (Cyberangriff legt wichtige US-Pipeline still), Mai 2021.
2 Julie Creswell, Nicole Perlroth und Noam Schreiber *(New York Times)*: „Ransomware Disrupts Meat Plants in Latest Attack on Critical U.S. Business“ (Fleischverarbeiter liegt nach größtem Angriff auf kritisches US-Unternehmen still), Juni 2021.
3 Nicole Perlroth und Adam Satariano *(New York Times)*: „Irish Hospitals Are Latest to Be Hit by Ransomware Attacks“ (Irische Krankenhäuser sind neueste Opfer von Ransomware-Angriffen), Mai 2021.

Vor dem Angriff

Die beste Sicherheitsstrategie besteht darin, Ransomware vollständig zu vermeiden. Dazu ist viel Planung und Arbeit nötig – noch vor einem Krisenfall.

Backup und Wiederherstellung

Ein zentraler Bestandteil jeder Sicherheitsstrategie gegen Ransomware ist das regelmäßige Anlegen von Daten-Backups. Da viele Ransomware-Varianten ans Netzwerk gebundene Backups kompromittieren, sollten Sie die Backups in einem separaten Netzwerk oder in der Cloud aufbewahren. Zudem sollte der Dateisystem-Zugriff auf die Backups gesperrt sein.[4]

Überraschend wenige Unternehmen führen Übungen ihrer Backup- und Wiederherstellungsprozesse durch, dabei ist beides wichtig: Erst durch diese Übungen wissen Sie, ob Ihr Backup-Plan wirklich funktioniert.

Aktualisieren und Patchen von Systemen

Halten Sie Betriebssysteme, Sicherheitssoftware, Anwendungen und Netzwerk-Hardware immer auf dem neuesten Stand.

Investition in zuverlässige personenzentrierte Sicherheitslösungen

Hochentwickelte E-Mail-Sicherheitslösungen schützen vor schädlichen Anhängen, Dokumenten und URLs in E-Mails, die zu Ransomware-Infektionen führen können. Diese Lösungen schützen auch vor anderen Arten von Malware, die in der Regel per E-Mail übertragen werden und in gezielten Folgeangriffen Ransomware installieren können.

Ein weiterer zentraler Punkt ist die Schulung und Sensibilisierung der Mitarbeiter. Diese sollten wissen, was sie tun bzw. lassen müssen und wie sie Ransomware vermeiden sowie melden können. Wenn Mitarbeiter eine Lösegeldforderung erhalten, sollten sie wissen, dass sie sich sofort an das Sicherheitsteam wenden müssen – und niemals versuchen sollten, die Forderung selbst zu bezahlen.

Planen der Reaktion

Keinen Zugang mehr zu geschäftskritischen Systemen zu haben, erzeugt Stress, und Stress beeinflusst die Entscheidungsfähigkeit.[5] Überlegen Sie sich im Voraus, wie Sie reagieren werden, sodass Sie sich im Falle eines Angriffs auf die Eindämmung und Wiederherstellung konzentrieren können.

Es gibt keinen universellen Reaktionsplan für einen Ransomware-Angriff. Krankenhäuser und andere Einrichtungen der Grundversorgung müssen die Kosten durch eine Störung ganz anders als Unternehmen im Privatkundengeschäft abwägen. Wenn Sie den theoretischen Ernstfall durchspielen, können Sie jede Phase Ihrer Reaktion angemessen planen.

4 W. Curtis Preston *(Network World)*: „How to protect backups from ransomware“ (So schützen Sie Backups vor Ransomware), Februar 2021.
5 Kathleen M. Kowalski und Charles Vaught *(International Journal of Emergency Management)*: „Judgement and Decision-Making Under Stress: An Overview for Emergency Managers“ (Einschätzungen und Entscheidungsfindung unter Stress: Ein Überblick für Notfall-Manager), Juni 2003.

Während des Angriffs

Obwohl die beste Strategie gegen Ransomware die Vermeidung von Infektionen ist, haben die immer raffinierteren Angriffe gezeigt, dass es auch sehr gut aufgestellte Unternehmen treffen kann.[6] Es ist gut möglich, dass Ihr System zunächst nicht durch Ransomware infiziert wird. Mittlerweile erwerben viele Ransomware-Gruppen vorzugsweise Zugänge zu Opfersystemen, die bereits mit Trojanern oder Loadern infiziert sind.

Während des Angriffs müssen Sie dringende Probleme bewältigen, zum Beispiel Rechner, Telefone und Netzwerke wieder hochfahren und sich um Lösegeldforderungen kümmern.

Anruf bei den Strafverfolgungsbehörden

Ransomware ist wie jede Form von Diebstahl oder Erpressung eine Straftat. Das Einschalten der zuständigen Behörden ist daher ein erster wichtiger Schritt.

Zudem sollten Sie Ihren Ransomware-Versicherer kontaktieren und in Erfahrung bringen, ob der Schaden von der Versicherung gedeckt wird.

Abtrennung vom Netzwerk

Sobald Ihre Mitarbeiter die Lösegeldforderung sehen oder etwas Ungewöhnliches beobachten, sollten sie sich vom Netzwerk trennen und den infizierten Rechner zur IT-Abteilung bringen. Nur das IT-Sicherheitsteam sollte einen Neustart versuchen. Und auch das funktioniert nur, wenn es sich um Scareware oder gewöhnliche Malware handelt.

Wenn die Ransomware bereits einen Server infiziert hat, sollte das Sicherheitsteam ihn so schnell wie möglich isolieren und Reaktionsmaßnahmen festlegen.

Achtung: Ähnlich wie bei Schädlingen im Haushalt weist ein infiziertes Gerät in der Regel auf ein größeres Problem hin. Suchen Sie Ihre Umgebung proaktiv nach weiteren infizierten Systemen ab.

Umsetzung der geplanten Reaktionsmaßnahmen

Die geplanten Reaktionsmaßnahmen sollten flexibel genug sein, um eine Vielzahl von Faktoren berücksichtigen zu können:

- Den Angriffstyp, insbesondere die eingesetzte Ransomware-Variante und den dahinterstehenden Angreifer
- Die Anwesenheit bereits bestehender Malware-Schaddaten, die womöglich zur Aufklärung oder zum Herunterladen der Ransomware genutzt wurden
- Die Anwender, die in Ihrem Netzwerk kompromittiert sind
- Die Netzwerkberechtigungen der kompromittierten Konten

Ransomware-Infektionen sind häufig sekundäre Infektionen in bereits kompromittierten Netzwerken. Das heißt, dass jeder dieser Faktoren bei der Einschätzung des Ausmaßes des Problems sowie bei der Verhinderung weiterer Infektionen und Datenverluste eine wichtige Rolle spielt.

Kein Verlass auf kostenlose Ransomware-Entschlüsselungstools

Die meisten kostenlosen Tools funktionieren nur für eine einzelne Ransomware-Variante oder sogar nur eine einzige Angriffskampagne. Da die Angreifer ihre Ransomware weiterentwickeln, sind die kostenlosen Tools oft nicht mehr aktuell und für Ihren Fall wahrscheinlich nutzlos.

Wiederherstellung aus Backups

Eine vollständige Erholung von einer Ransomware-Infektion ist nur durch die Wiederherstellung aus Backups möglich. Doch selbst mit aktuellen Backups kann es aus finanzieller und betrieblicher Hinsicht günstiger sein, das Lösegeld zu zahlen.

6 Kellen Browning *(New York Times)*: „Hundreds of Businesses, from Sweden to U.S., Affected by Cyberattack“ (Hunderte Unternehmen – von Schweden bis zu den USA – von Cyberangriff betroffen), Juli 2021.

Nach dem Angriff

Die unmittelbare Krise ist zwar vorbei, doch es gibt noch viel zu tun.

Überprüfung und Verstärkung

Wir empfehlen eine gründliche Sicherheitsbewertung durchzuführen, damit Sie Bedrohungen finden, die eventuell noch in Ihrer Umgebung lauern. Werfen Sie ebenfalls einen kritischen Blick auf Ihre Sicherheitstools sowie -abläufe, und ermitteln Sie, was genau dort schiefging.

Bereinigung

Einige Ransomware-Varianten werden über andere Bedrohungen oder Backdoor-Trojaner übertragen, die weitere Angriffe ermöglichen. Häufig war die betroffene Umgebung bereits kompromittiert und bot der Ransomware leichtes Spiel.

Suchen Sie sorgfältig nach verborgenen Bedrohungen, die Sie im Chaos möglicherweise übersehen haben – besonders wenn die Gefahr besteht, dass Ihre Backups ebenfalls kompromittiert wurden.

Rückschau-Sicherheitsanalysen

Prüfen Sie, wie gut Sie auf die Bedrohung vorbereitet waren, welche Ereigniskette zur Infektion geführt hat und wie Sie darauf reagiert haben. Wenn Sie nicht wissen, wie die Ransomware Ihre Schutzmaßnahmen überwunden hat, lässt sich auch der nächste Angriff nicht stoppen.

Bewertung des Sicherheitsbewusstseins der Anwender

Gut geschulte Mitarbeiter sind Ihre letzte Verteidigungslinie. Sorgen Sie dafür, dass Ihre Mitarbeiter der Aufgabe gewachsen sind. Regelmäßige Bewertungen und Phishing-Simulationen können aufdecken, wer am stärksten gefährdet ist und auf E-Mail-Köder sowie andere Taktiken hereinfällt.

Schulungen

Erstellen Sie einen Schulungsplan, um die Schwachstellen Ihrer Mitarbeiter bei Cyberangriffen zu beseitigen. Der Plan sollte auf realen Angriffskampagnen und Taktiken beruhen. Entwerfen Sie einen Krisenkommunikationsplan für den Fall eines künftigen Angriffs und führen Sie anschließend Übungen sowie Penetrationstests durch.

Verstärkung der technischen Schutzmaßnahmen

Die sich rasch wandelnde Bedrohungslandschaft erfordert Sicherheitslösungen, die in Echtzeit schädliche URLs und Anhänge analysieren, identifizieren und blockieren können, die für Ransomware als primäre Eintrittspunkte dienen.

Suchen Sie nach Lösungen, die sich an neue und zukünftige Bedrohungen anpassen lassen und eine schnellere Reaktion ermöglichen.

Einführung

Ransomware gibt es nun bereits seit drei Jahrzehnten. In dieser Zeit hat sie einige Entwicklungen durchgemacht. Als wir den Bericht das letzte Mal aktualisiert haben, gingen die Ransomware-Zahlen nach unten, da Unternehmen und Sicherheitsanbieter die Ransomware Locky blockierten, die 2016 für ein Wiederaufleben der Bedrohung gesorgt hatte.

300 % ANSTIEG
von Ransomware-Angriffen im Jahresvergleich seit Anfang 2021 (laut Zahlen der US-Regierung).

Das ändert sich gerade. Seit Anfang 2021 weisen Zahlen der US-Regierung auf einen erneuten Anstieg hin: Ransomware-Angriffe nehmen im Jahresvergleich um 300 % zu.[7]

Die treibende Kraft hinter dieser Entwicklung ist eine Veränderung im Ökosystem der Cyberkriminellen. Die Ransomware-Gruppen setzen nicht mehr auf eine großflächige Verteilung und geringe Lösegeldsummen. Stattdessen arbeiten sie nun häufig mit anderen Malware-Verteilern zusammen, die ihnen Zugriff auf Systeme liefern, die bereits mit Trojanern und Loadern infiziert sind und somit leichter ausgekundschaftet, aufgeklärt und angegriffen werden können. Dieser Ansatz ermöglicht den Kriminellen, wertvolle Ziele zu identifizieren, die durch Störungen mehr zu verlieren und tiefere Taschen haben.

Zusammen mit dem steigenden Wert von Bitcoins und anderen Kryptowährungen hat diese Entwicklung die Voraussetzungen für eine Ransomware-Epidemie geschaffen.

In den Schlagzeilen

In den ersten sechs Monaten des Jahres 2021 hat sich Ransomware von einem Ärgernis zu einer Krise entwickelt, über die in den höchsten Regierungsebenen diskutiert wird. Mit Angriffen auf Schulbezirke, Polizeireviere und Verkehrsbehörden zeigen Ransomware-Gruppen, dass sie nicht davor zurückschrecken, auch öffentliche Infrastrukturen ins Visier zu nehmen.

Mit Angriffen auf Schulbezirke, Polizeireviere und Verkehrsbehörden zeigen Ransomware-Gruppen, dass sie nicht davor zurückschrecken, auch öffentliche Infrastrukturen ins Visier zu nehmen.

Im Mai 2021 schließlich griffen mit der Ransomware-Gruppe DarkSide verbundene Kriminelle die Firma Colonial Pipeline an, deren Anlagen große Teile der US-amerikanischen Ostküste mit Kraftstoff versorgen. Durch die Störung kam es zu Engpässen in mehreren Bundesstaaten, da viele Verbraucher aus Panik auf Vorrat kauften. Letztendlich entschied sich Colonial Pipeline dazu, das Lösegeld von über 4 Millionen US-Dollar in Bitcoin zu zahlen und damit den Zugang zu ihren Systemen wiederzuerlangen.[8]

Noch im selben Monat infizierten Angreifer aus der Ransomware-Gruppe REvil den Fleischverarbeiter JBS Foods, der unter anderem in den USA, Brasilien und Australien tätig ist. Lieferungen von Rindfleisch und anderen Fleischprodukten kamen zum Erliegen, bis JBS ein Lösegeld von 11 Millionen US-Dollar zahlte.[9]

7 James Rundle und David Uberti *(The Wall Street Journal)*: „How Can Companies Cope with Ransomware?“ (Wie bewältigen Unternehmen Ransomware?), Mai 2021.
8 Collin Eaton und Dustin Volz *(The Wall Street Journal)*: „Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom“ (CEO von Colonial Pipeline erklärt, warum er Hackern 4,4 Mio. USD Lösegeld gezahlt hat), Mai 2021.
9 Jacob Bunge *(The Wall Street Journal)*: „JBS Paid $11 Million to Resolve Ransomware Attack“ (JBS zahlte 11 Mio. USD zur Behebung von Ransomware-Angriff), Juni 2021.

Zudem stellte sich Anfang Juli heraus, dass die Gruppe REvil hinter einem Lieferkettenangriff auf das Software-Unternehmen Kaseya steckte.[10] DarkSide und REvil sind seit diesem Zeitpunkt nicht mehr aktiv. Es tauchen jedoch stets neue Ransomware-Betreiber auf – und viele Gruppen versuchen mit einer Umbenennung der ungewollten Aufmerksamkeit zu entkommen.

Da die Lösegeldforderungen immer weiter steigen und ernsthafte Schäden an landeseigener Infrastruktur durch Cyberangreifer – mit oder ohne deren Absicht – immer wahrscheinlicher werden, wird den Regierungen weltweit der Ernst der Lage langsam bewusst. Nach dem Zwischenfall bei Colonial Pipeline erließ US-Präsident Joe Biden eine Verfügung, die Cyberschutzmaßnahmen des Landes verstärken sollte. Zudem kritisierte er den russischen Präsident Wladimir Putin dafür, dass dessen Regierung die aus seinem Land heraus agierenden Ransomware-Gruppen nicht strafrechtlich verfolgt.

Funktionsweise von Ransomware

Ransomware blockiert den Zugriff auf ein Rechnersystem oder dessen Daten, wobei in der Regel Dateien mit bestimmten Dateiendungen (z. B. JPG, DOC, PPT) verschlüsselt werden. Die Dateien bleiben so lange unzugänglich, bis das Opfer dem Angreifer Geld für einen Verschlüsselungsschlüssel bezahlt, mit dem die Dateien entsperrt werden können. In vielen Fällen läuft bei der Lösegeldforderung ein Countdown. Wird dieser überschritten, kann es sein, dass das Lösegeld verdoppelt wird oder die Daten für immer verloren sind bzw. veröffentlicht oder sogar zerstört werden.

Immer häufiger werden die Opfer mehrfach erpresst: Zunächst für einen Verschlüsselungsschlüssel zur Entschlüsselung der Daten und danach als Gegenleistung dafür, dass die Angreifer nicht Kopien davon veröffentlichen oder im Dark Web veräußern.

Die realen Kosten

Beinahe 80 % der US-Unternehmen verzeichneten im Jahr 2020 einen Ransomware-Angriff – und 68 % von ihnen zahlten das Lösegeld.[11] Die finanziellen Folgen eines Angriffs können beträchtlich sein, wobei die Lösegeldsummen von Jahr zu Jahr steigen.

80 %
der US-Unternehmen haben 2020 einen Ransomware-Angriff erlebt.

68 %
haben Lösegeld gezahlt.

Im ersten Halbjahr 2021 gab es folgende bestätigte Zahlungen: 4,4 Millionen US-Dollar durch Colonial Pipeline[12], 11 Millionen US-Dollar durch JBS Foods[13] und eine Rekordsumme von 40 Millionen US-Dollar durch CNA Financial[14]. Hierbei handelt es sich jedoch lediglich um Fälle, die öffentlich bekannt wurden. Die wahren finanziellen Kosten durch Ransomware sind wahrscheinlich höher, als diese Zahlen vermuten lassen, da einige Unternehmen einen Zwischenfall natürlich eher im Stillen bewältigen.

Die betrieblichen Kosten beschränken sich jedoch nicht nur auf den finanziellen Aspekt.

10 Jonathan Vanian *(Fortune)*: „Everything to know about REvil, the group behind a big ransomware spree“ (Was Sie über REvil, eine der aktivsten Ransomware-Gruppen, wissen sollten), Juli 2021.
11 Proofpoint: „State of the Phish 2021“, Februar 2021.
12 Collin Eaton und Dustin Volz *(The Wall Street Journal)*: „Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom“ (CEO von Colonial Pipeline erklärt, warum er Hackern 4,4 Mio. USD Lösegeld gezahlt hat), Mai 2021.
13 Jacob Bunge (*The Wall Street Journal)*: „JBS Paid $11 Million to Resolve Ransomware Attack“ (JBS zahlte 11 Mio. USD zur Behebung von Ransomware-Angriff), Juni 2021).
14 Kartikay Mehrotra und William Turton *(Bloomberg)*: „CNA Financial Paid $40 Million in Ransom After March Cyberattack“ (CNA Financial zahlte 40 Mio. USD Lösegeld nach Cyberangriff im März), Mai 2021.
15 Coveware: „Q2 Ransom Payment Amounts Decline as Ransomware becomes a National Security Priority“ (Lösegeldzahlungen im 2. Quartal gehen zurück, nachdem Ransomware als Problem mit nationaler Bedeutung erklärt wurde).

Laut Coveware, einem auf Ransomware-Zwischenfälle spezialisierten Beratungsunternehmen, wurde den Opfern in über drei Viertel der Ransomware-Angriffe im ersten Halbjahr 2021 mit der Veröffentlichung exfiltrierter Daten gedroht.[15] 2020 berichtete Coveware zudem, dass sich 65 % der Opfer einer Datenkompromittierung für die Zahlung eines Lösegeldes entschieden. Dieser Fakt macht das große Risiko von Rufschäden bei krimineller Datenexfiltration deutlich.

Am schwersten lassen sich wohl die Kosten durch den betrieblichen Ausfall abschätzen, die entstehen, wenn Lieferketten zum Stehen kommen, die Vertriebsmitarbeiter bestehende und potenzielle Kunden nicht mehr erreichen können und selbst die einfachsten Kommunikationstools nicht mehr funktionieren. Wie die irische Gesundheitsorganisation Health Service Executive feststellen musste, können die Auswirkungen in Sektoren wie dem Gesundheitswesen noch schwerer wiegen. Ein Angriff der Ransomware-Gruppe Conti führte dort zu Verzögerungen bei Behandlungen sowie zur Absage ambulanter Dienstleistungen wie Röntgenuntersuchungen.[16]

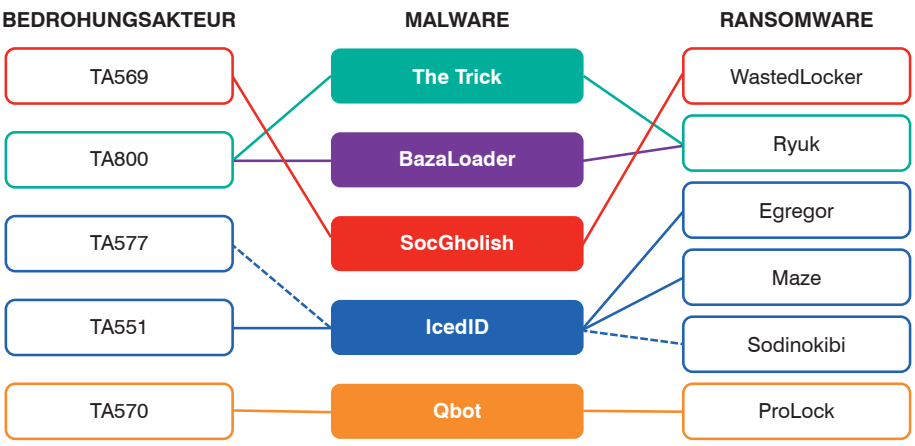
Ransomware und E-Mail

Ein großer Teil der Ransomware-Angriffe beginnt – direkt oder indirekt – mit einer Phishing-E-Mail.

Ein großer Teil der Ransomware-Angriffe beginnt – direkt oder indirekt – mit einer Phishing-E-Mail. Dabei werden die Anwender dazu verleitet, einen schädlichen Anhang zu öffnen oder auf eine schädliche URL zu klicken.

Doch seit Locky vor fünf Jahren millionenfach in Posteingängen zu finden war, hat sich vieles geändert. In letzter Zeit wird Ransomware als sekundäre Infektion übertragen, nachdem ein System bereits mit einem Trojaner oder Loader infiziert wurde. Die für die Verteilung dieser Malware-Typen verantwortlichen Akteure verkaufen den Zugang anschließend an Ransomware-Gruppen, die in infizierten Netzwerken nach den wertvollsten Zielen suchen. Für die Bereitstellung eines Eintrittspunkts ins Netzwerk erhalten die Vermittler entweder eine pauschale Summe oder einen Anteil vom Lösegeld.

Es gibt zwar keine direkte Beziehung zwischen der Erstzugriffs-Malware und der Ransomware-Variante, die an die Opfer verteilt wird, doch haben Proofpoint-Forscher und andere Branchenvertreter einige auffällige Zusammenhänge festgestellt.



16 Danny Palmer *(ZDNet)*: „The human cost of ransomware: Disruption to Irish health service will continue for months“ (Die menschlichen Kosten von Ransomware: Störungen bei der Gesundheitsversorgung in Irland werden noch Monate anhalten), Juni 2021.

Das Beziehungsnetzwerk zwischen cyberkriminellen Gruppen ist kompliziert – die Abfolge der Ereignisse in einem typischen durch E-Mail ausgelösten Ransomware-Angriff ist dagegen simpel: Durch die Infektion mit einem Trojaner oder Loader wird ein Netzwerk anfällig für Ransomware-Gruppen, die nach wertvollen Zielen suchen. Für die meisten Unternehmen besteht also der beste Schutz vor Ransomware in der Vermeidung anderer Malware-Typen.

Mit anderen Worten: Wenn Sie die Loader blockieren, blockieren Sie die Ransomware.

Insider-Bedrohungen

2020 bot jemand einem Tesla-Mitarbeiter 500.000 US-Dollar für die Installation von Ransomware im Firmennetzwerk.

Neben E-Mail-Ködern und technischen Schwachstellen haben Angreifer eine weitere Front im Ransomware-Krieg eröffnet: bereitwillige Kollaborateure. In einer kleinen aber alarmierenden Zahl von Fällen versuchen die Bedrohungsakteure, Mitarbeiter dazu zu bewegen, gegen Bezahlung Ransomware an ihrem Arbeitsplatz zu installieren.

2020 bot jemand einem Tesla-Mitarbeiter 500.000 US-Dollar für die Installation von Ransomware im Firmennetzwerk. Der Mitarbeiter meldete die Tat, woraufhin der Schuldige verhaftet wurde und sich schuldig bekannte – allerdings erst, nachdem er mit einem erfolgreichen Versuch bei einem anderen Unternehmen geprahlt hatte.

Im August 2021 beobachteten wir eine E-Mail-Kampagne, in der Mitarbeitern eine Million US-Dollar für die Installation der Ransomware DemonWare an ihrem Arbeitsplatz geboten wurde. Etwa zur gleichen Zeit fügte LockBit seiner Lösegeldforderung ein Angebot hinzu, das Insidern mehrere Millionen US-Dollar für gültige Kontoanmeldedaten versprach.

Der DemonWare-Angreifer versuchte in keiner seiner Anwerbe-E-Mails, Malware zu verteilen. Einige hochentwickelte E-Mail-Sicherheitslösungen können diese Angebote anhand bestimmter Hinweise erkennen. Dennoch empfiehlt es sich, Mitarbeiter in der Erkennung und zügigen Meldung dieser Bedrohungen zu schulen.

Übertragungswege

Ransomware wird hauptsächlich über die folgenden Angriffsvektoren übertragen:

- E-Mail, einschließlich Ransomware-Anhänge und URLs, die zu schädlichen Dateien führen
- Zugriff über ein kompromittiertes RDP (Remote Desktop Protocol) oder VPN (virtuelles privates Netzwerk)
- Schwachstellen in unternehmenseigener Netzwerktechnik
- Infizierte Websites bzw. Links aus sozialen Netzwerken und mit Malware infizierte Werbung (Malvertising)
- Andere Malware (wie Loader oder Stealer), die bereits kompromittierte Systeme mit Ransomware infizieren

Auch wenn Ransomware durch andere Malware übertragen wird, ist E-Mail häufig der Anfangsvektor.

Die E-Mails erwecken dabei einen legitimen Eindruck und können ahnungslose Mitarbeiter täuschen. Häufig tarnen sich die Nachrichten als offizielle Software-Updates, ungezahlte Rechnungen oder sogar als Mitteilung vom Vorgesetzten, die sich auf eine vorherige Nachricht bezieht.

Warum Ransomware immer noch existiert

Ransomware ist eine Jahrzehnte alte Angriffsmethode, die durch vier Faktoren zu einer größeren Bedrohung geworden ist:

Mehr Übertragungskanäle

Cyberkriminelle können tausende Stellen gleichzeitig angreifen und dabei eine Vielzahl an Angriffsmethoden nutzen, die sekundäre Ransomware-Angriffe ermöglichen.

Konventionelle Cyberschutzmaßnahmen sind durch Bedrohungen aus allen Richtungen überwältigt:

- Massive E-Mail-Kampagnen durch Botnets
- Ausnutzbare Schwachstellen in Netzwerk-Hardware und -Software
- Polymorphe Malware, für die keine neuen Malware-Signaturen erstellt werden können, da sie sich zu schnell verändert
- Malvertising und kompromittierte Websites außerhalb des Unternehmensperimeters

Zusammengenommen machen diese Faktoren eine Infektion wahrscheinlicher und geben Ransomware mehr Möglichkeiten, im System Fuß zu fassen.

Mehr lukrative Ziele

Anstelle von breit angelegten Angriffen richten Cyberkriminelle ihre Aufmerksamkeit zunehmend auf Unternehmen mit vertraulichen Daten bzw. unterdimensionierten IT-Abteilungen oder Firmen, die dazu geneigt sind, das Problem schnell lösen zu wollen.

Erschwerend hinzu kommen Schwierigkeiten bei der Absicherung von Krankenhäusern, Polizeidienststellen, Schulen und lokalen Behörden.

Für diese Einrichtungen ist ein Netzwerkausfall keine Option. Es überrascht daher nicht, dass viele nach einer kurzen Überschlagrechnung das Zahlen des Lösegeldes geschäftlich als die beste Entscheidung ansehen.

Gezieltere Angriffe mit immer raffinierteren Taktiken

Früher kam es bei Ransomware-Attacken nur auf die Menge an: Hunderttausende Empfänger wurden mit umfangreichen E-Mail-Kampagnen und geringen Lösegeldforderungen mit der Hoffnung angegriffen, dass genug Opfer den Köder schlucken.

Heutzutage werden die Angreifer bei ihren Opfern wählerischer. Sie suchen gezielt nach anfälligen geschäftskritischen Daten und Systemen, zu denen die Opfer dringend Zugang benötigen, und erhoffen sich so eine höhere Summe.

Gleichzeitig werden auch die Ransomware-Angriffe immer raffinierter. Anstatt Ransomware gleich in der ersten Angriffsstufe einzusetzen, kompromittieren Cyberkriminelle die Systeme mit robusterer und vielseitiger Malware.

Sobald sie Fuß gefasst haben, installieren sie Ransomware auf vielversprechenden Geräten.

Bitcoin und andere Digitalwährungen

Bitcoin ist seit der Einführung im Jahr 2009 zu einem Segen für Anhänger des zivilen Libertarismus und Cyberkriminelle geworden. Die Zahlungen können weder zum Empfänger noch zum Absender zurückverfolgt werden und bieten eine anonyme reibungslose Möglichkeit für privaten Handel.

Durch die Zahlung in Bitcoin bleiben die Cyberkriminellen anonym und haben es damit sehr viel leichter, Lösegelder zu kassieren. Bei früheren Ransomware-Formen war der Kauf einer im Voraus bezahlten Guthabenkarte nötig. Mit diesem Ansatz konnten zwar die Betrugsschutzmaßnahmen einer Bank umgangen werden, allerdings war dies für beide Seiten sehr viel aufwändiger.

Alle großen Ransomware-Familien verlangen heute eine Zahlung in Bitcoin (siehe **„Die Spur des Bitcoin-Geldes“ auf Seite 13**).

Eine alte und immer noch aktuelle Bedrohung

Ein Beispiel dafür, wie perfide Ransomware-Angriffe heute sind – und wie sie sich direkt auf Verbraucher auswirken können –, ist der Angriff auf Garmin Ltd. an, einen Netzwerkdienstleister, der Daten unter anderem an Smart-Watches und Fitness-Tracker von Garmin übermittelt.

Garmin Ltd. schickt mithilfe der GPS-Technologie Daten an Fitness-Tracker, wie es sie beispielsweise von FitBit und Apple gibt. Am 23. Juli 2020 kam es zu einer Störung dieser Dienste, als Garmin Opfer eines Cyberangriffs wurde, bei dem seine Online-Systeme verschlüsselt wurden. Wie Garmin in einer Pressemitteilung berichtet, waren davon der Kunden-Support sowie kundenseitige Applikationen und das Kommunikationssystem des Unternehmens betroffen.

Garmin konnte viele seiner Dienste nicht mehr bereitstellen, da die Dienste und das Callcenter-Netzwerk verschlüsselt wurden und für die Endnutzer und das Unternehmen nicht mehr zugänglich waren. Berichten zufolge konnten die Dienste erst entschlüsselt werden, nachdem Garmin den Angreifern ein Lösegeld in Höhe von 10 Millionen US-Dollar zahlte.

„Eine dem Notfallreaktionsteam bei Garmin nahestehende Person und ein Mitarbeiter des Unternehmens bestätigten, […] dass Garmin durch die Ransomware WastedLocker angegriffen wurde“, berichtete die Technologienachrichten-Webseite BleepingComputer am 1. August.

> „Die IT-Abteilung von Garmin versuchte, während der Verschlüsselung alle Rechner im Netzwerk, einschließlich der per VPN angebundenen Heim-PCs, aus der Ferne abzuschalten“, schrieb BleepingComputer. „Nachdem dies gescheitert war, wurden die Mitarbeiter angewiesen, alle Rechner im Netzwerk, zu denen sie Zugang hatten, herunterzufahren.“

Garmin gab an, dass die Online-Dienste nach vier Tagen wieder in Betrieb genommen werden konnten.

Wie BleepingComputer erfuhr, wurde die Ransomware WastedLocker der russischen Cybercrime-Gruppe Evil Corp zugeordnet. Der Name mag zwar nach einem Cartoon-Bösewicht klingen, doch Evil Corp wurde im Dezember 2019 von der US-Regierung für ihre Rolle im Zwischenfall mit der Malware Dridex und für den Einsatz von Ransomware in anderen Angriffen (darunter die Ransomware Locky und ihre eigene Ransomware-Variante mit dem Namen BitPaymer) sanktioniert.

Die Spur des Bitcoin-Geldes

Beim traditionellen Kidnapping zum Erpressen von Lösegeld war das größte Problem stets, das Geld zu kassieren und damit zu entkommen. Leider verfügen Ransomware-Cyberkriminelle über eine sehr viel einfachere Möglichkeit.

Die beliebteste Zahlungsform besteht aus nicht zurückverfolgbaren Kryptowährungen, von denen Bitcoin die bekannteste ist. Bitcoin ermöglicht die Online-Geldüberweisung zwischen zwei Personen, wobei keine Bank oder Regierung zwischengeschaltet ist.

Vereinfacht gesagt kann man sich Kryptowährungen als elektronischen Casino-Chip vorstellen. Die Token an sich haben in der realen Welt keinen Wert. Die Nutzer können sie jedoch im Tausch mit ihrer lokalen Währung erwerben und in der Einrichtung – in diesem Fall dem Internet – verwenden. Beim Austritt können sie sie gegen eine Währung umtauschen.

Analog dazu können Kryptowährungen online über eine Kreditkarte oder ein Bankkonto aus legitimen Quellen erworben werden. Im Falle eines Ransomware-Angriffs konvertiert das Opfer seine lokale Währung in Bitcoin und schickt die Bitcoins dann an die vom Angreifer angegebene anonyme Adresse einer Kryptowährungs-Geldbörse.

Nicht immer gehen die Bitcoins direkt an den Angreifer. In der Regel landen die Token bei einem sogenannten „Tumbler“, einem digitalen Service, der die Bitcoins mit anderen vermischt und diese dem Angreifer zurückgibt (mit anderen Nummern, aber dem gleichen Wert, abzüglich Kommission).

Ähnlich wie bei Geldwäsche in der physischen Welt erhalten die Angreifer am Ende eine nicht zurückverfolgbare Zahlung. Diese Zahlung können sie dann in ihre lokale physische Währung konvertieren, indem sie die Bitcoins in Bargeld umtauschen.

Im Gegensatz zu staatlich gestützten Währungen werden Kryptowährungen nicht überall als Zahlungsmittel anerkannt. Sie werden stattdessen mit Pokerchips, Spielmarken oder ähnlichen Systemen gleichgestellt. Das Übertragungssystem und die Tumbler werden daher nicht reguliert und gelten auch nicht als Geldwäsche – obwohl das Ergebnis im Prinzip das gleiche ist.

Der Reiz von Bitcoin lässt sich leicht erklären: Angreifer verfügen damit über eine schwer nachverfolgbare, weltweit verfügbare Cyberwährung, die sich direkt in lokale Hartwährung – also „unmarkierte Scheine“ – konvertieren lässt.

Gegenüber dem Einsatz gestohlener Kreditkarten bringt dieser Ansatz klare Vorteile mit sich. Letztere verlieren mit jedem Tag an Wert, da die Finanzinstitute immer zügiger Konten von Opfern sperren.

Zudem haben Bitcoins in den letzten Jahren an Wert zugelegt, wobei der Höchststand bei beinahe 65.000 US-Dollar je Bitcoin lag. Dies kann den Angreifern einen zusätzlichen finanziellen Vorteil verschaffen.

Nach dem Angriff auf Colonial Pipeline berichtete das FBI, das etwa die Hälfte der Bitcoins, die als Lösegeld gezahlt wurden, zurückgeholt werden konnte. Die Behörde ließ offen, wie genau dies erfolgte, und es bleibt unklar, ob sich derartige Aktionen wiederholen lassen.[17]

17 Katie Brenner und Nicole Perlroth *(New York Times)*: „U.S. Seizes Share of Ransom From Hackers in Colonial Pipeline Attack“ (USA können Teil des Lösegelds aus Colonial Pipeline-Angriff von Hackern zurückholen), Juni 2021.

Vor dem Angriff

Die beste Sicherheitsstrategie besteht darin, eine Erpressung vollständig zu vermeiden. Für die meisten Unternehmen ist dies sehr wohl möglich, erfordert jedoch viel Planung und Aufwand – und zwar bevor der Ernstfall eintritt.

Backup und Wiederherstellung

Der wichtigste Bestandteil jeder Sicherheitsstrategie gegen Ransomware ist das regelmäßige Anlegen von Daten-Backups. Viele Unternehmen tun dies bereits, doch überraschend wenige führen Übungen zu ihren Backup- und Wiederherstellungsprozessen durch. Beides ist wichtig: Erst diese Übungen zeigen, ob der Backup-Plan wirklich funktioniert.

Eventuell stellen Sie fest, dass Sie Schwachstellen ausbügeln müssen. Sofern Backup und Wiederherstellung regelmäßig getestet werden, zieht eine Ransomware-Infektion keine gravierenden Folgen nach sich, da Sie einen sicheren aktuellen Wiederherstellungspunkt haben.

Aktualisieren und Patchen von Systemen

Sorgen Sie dafür, dass die Betriebssysteme, Sicherheitssoftware, Anwendungen und Netzwerk-Hardware immer auf dem neuesten Stand sind. Eigentlich klingt es ganz einfach, doch in einer aktuellen Umfrage erklärte mehr als die Hälfte der Unternehmen, dass es für sie keine einfache Möglichkeit gibt, das zeitnahe Patchen von Schwachstellen sicherzustellen. Zudem gaben die Teilnehmer an, dass die Updates in Bezug auf Komplexität und Veröffentlichungsintervalle stark variieren.[18]

Es gibt jedoch Institutionen, die die Verwaltung von Patches unterstützen, wie zum Beispiel das Center for Internet Security (CIS). Diese gemeinnützige Organisation gibt bewährte Methoden für IT-Sicherheitsmanagement heraus, darunter auch zu Ransomware-Bedrohungen.

Vermeiden Sie Überlastung durch zu viele Patches, denn nur so kann eine sichere Umgebung gewährleistet werden. Die Deaktivierung von RDP-Verbindungen (Remote Desktop Protocol) und das Patchen von VPNs können eine entscheidende Rolle spielen, wenn Sie Bedrohungsakteuren einfache Einfallstore für Ransomware-Angriffe verwehren wollen.

Planen der Reaktion

Überlegen Sie sich im Voraus, wie Sie reagieren werden, sodass Sie sich im Falle eines Angriffs auf die Eindämmung und Wiederherstellung konzentrieren können. Die Bewältigung eines gerade stattfindenden Ransomware-Angriffs ist eine nervenaufreibende Erfahrung. Wenn die Angreifer immer weiter ins Netzwerk vordringen, um noch mehr Schäden anzurichten, zählt jede Sekunde.

18 Ponemon Institute: „Today's State of Vulnerability Response: Patch Work Demands Attention" (Aktueller Stand der Reaktion auf Schwachstellen: Patchwork erfordert Aufmerksamkeit), April 2018.

Wichtige Fragen wie „Wer muss informiert werden?“, „Wie kann die Kommunikation aufrechterhalten werden?“ und „Wie viel wäre ich bereit zu zahlen (wenn überhaupt)?“ lassen sich schwer in ad-hoc beantworten. Dieser Druck kann die Entscheidungsfindung verlangsamen und zu kostspieligen Verzögerungen führen. Falls Sie sich zur Zahlung des Lösegeldes entschließen, sollten Sie einen angemessenen Ablauf planen und dabei wichtige Führungskräfte, Mitarbeiter sowie Rechtsberater einbeziehen.

Es gibt keinen universellen Reaktionsplan für einen Ransomware-Angriff. Krankenhäuser und andere Einrichtungen der Grundversorgung werden die Kosten durch eine Störung ganz anders als Unternehmen im Privatkundengeschäft abwägen. Wenn Sie den theoretischen Ernstfall durchspielen, können Sie jede Phase Ihrer Reaktion angemessen planen.

Investition in zuverlässige personenzentrierte E-Mail-, Web- und Cloud-Sicherheitslösungen

Phishing-E-Mails sind heute raffiniert gestaltet und werden äußerst gezielt verschickt. Die Angreifer forschen ihre Opfer gründlich aus und erstellen E-Mails, die legitim erscheinen und menschliche Schwächen ausnutzen, um Anwender zum Klicken zu bringen.

E-Mail: der wichtigste Vektor

Herkömmliche E-Mail-Gateways, Web-Filter und Virenschutz-Softwareprogramme sollten auf dem neuesten Stand gehalten werden und in allen Netzwerken aktiv sein. Allerdings können diese Lösungen allein die Ransomware-Bedrohung nicht aufhalten – eine effektive E-Mail-Sicherheitslösung muss schon vorher aktiv werden.

Da in den meisten Fällen E-Mail der erste Infektionspunkt ist, der zu Ransomware-Angriffen führt, benötigen Sie eine hochentwickelte Lösung zum Schutz dieses Vektors.

Diese muss auch eingebettete URLs und Anhänge analysieren und verhindern, dass schädliche Inhalte das System kompromittieren können. Cyberdiebe sind immer einen Schritt voraus und die typischen E-Mail-Sicherheitskonfigurationen setzen zu sehr auf das veraltete Signaturprinzip.

Hochentwickelte E-Mail-Sicherheitslösungen schützen vor schädlichen Anhängen, Dokumenten und URLs in E-Mails, die zu Ransomware-Infektionen führen können. Zudem kann auf DMARC basierende E-Mail-Authentifizierung Angriffe mit Domänen-Spoofing stoppen (bei dem die E-Mail-Domäne Ihres Unternehmens imitiert wird, um das Vertrauen der Anwender zu gewinnen). Ihre E-Mail-Sicherheitslösung sollte auch vor anderen Arten der Identitätstäuschung wie Display Name-Spoofing und Doppelgänger-Domänen schützen.

Schutz Ihrer Cloud-Konten

Cloud-basierte E-Mail-Konten sind ein weiterer häufig genutzter Vektor für die Verteilung von Malware. Cyberkriminelle können die Kontrolle über die Cloud-Konten Ihrer Anwender übernehmen, um auf diese Weise Anwender innerhalb Ihres Unternehmens anzugreifen. E-Mail-Konten können unter anderem auf folgenden Wegen kompromittiert werden:

- Automatisierte Brute-Force-Angriffe, die zahllose Kombinationen von Benutzernamen und Kennwörtern ausprobieren
- Externer Diebstahl von Anmeldedaten (da Angreifer wissen, dass Anwender ihre Kennwörter häufig für andere Konten wiederverwenden)

- Malware, die Anmeldedaten stiehlt
- Unzureichende Cloud-Kontrollen

Die Absicherung von Anwender-Cloud-Konten spielt beim Schutz vor Ransomware-Angriffen eine wichtige Rolle.

Zudem sollten sich Remote-Anwender über ein Firmen-VPN mit dem Internet verbinden, sodass sie an jedem Ort durch Cyberschutzmaßnahmen geschützt sind.

Ihre Mitarbeiter als starke letzte Verteidigungslinie

Die meisten Malware-Infektionen beginnen mit einem einzigen arglosen Mitarbeiter, der eine scheinbar arbeitsbezogene E-Mail öffnet.

Deshalb ist die Schulung und Sensibilisierung der Mitarbeiter so entscheidend. Diese sollten wissen, was sie tun bzw. lassen müssen und wie sie Ransomware vermeiden sowie melden können. Ein Schulungsprogramm, das reale Angriffe nachempfindet und ein Rückmeldungssystem zur Meldung verdächtiger Nachrichten umfasst, erleichtert die Schulung der Anwender beim Erkennen verdächtiger E-Mails und verstärkt positives Verhalten.

Wenn Mitarbeiter eine Lösegeldforderung erhalten, sollten sie wissen, dass sie sich sofort an das Sicherheitsteam wenden müssen – und niemals versuchen sollten, die Forderung selbst zu bezahlen. Eine Zahlung hat erhebliche Auswirkungen auf den Ruf Ihrer Marke sowie die Sicherheit Ihres Unternehmens und kann in einigen Fällen zum Verstoß gegen behördliche Sanktionen führen. Diese Entscheidung sollte von der Unternehmensführung zusammen mit Rechtsberatern sorgfältig abgewogen werden.

Unsere Untersuchungen zeigen, dass Cyberkriminelle menschliche Fehler und Neugier rigoros ausnutzen. Damit folgen sie einem allgemeinen Trend in der Cyberkriminalität: In dem Bestreben, Daten zu verschlüsseln und Lösegeld zu verlangen, werden Menschen unwissentlich zu Komplizen gemacht.

Die Angriffe nutzen die Ahnungslosigkeit der Anwender aus. In der Regel werden die Anwender dazu gebracht, schädliche Dokumente im Anhang zu öffnen, Dokumente oder Skripte herunterzuladen und auszuführen oder etwas anderes zu tun. Sobald Anwender beispielsweise in einem schädlichen Dokument auf die Schaltfläche „Inhalte aktivieren“ klicken und damit Makros aktivieren, kann Ransomware heruntergeladen und ein Angriff gestartet werden.

Die effektivsten Schulungsprogramme vermitteln Anwendern Wissen über reale Angriffstechniken und Kampagnen. Zudem berücksichtigen sie die aktuellsten Bedrohungsdaten, durch die die Anwender mehr über die Bedrohungen erfahren, die ihnen wahrscheinlich begegnen werden. In Phishing-Simulationen können Anwender identifiziert werden, die besonders anfällig für Ransomware und andere Angriffstaktiken sind.

Technische Aspekte: Empfehlungen der US-Behörden

Neben der in diesem Leitfaden erläuterten Strategie empfiehlt das FBI folgende technische Maßnahmen zum Schutz vor Ransomware-Angriffen.

Audits und Verwaltung von Anwenderberechtigungen

Vergeben Sie Berechtigungen für Dateien, Ordner und Netzwerkfreigaben nach dem Least-Privilege-Prinzip.

Anwender, die beispielsweise Dateien nicht bearbeiten müssen, sollten nur Lesezugriff haben. In vielen Fällen sollten Anwender gar keinen Zugriff haben. Ein Kassierer benötigt keinen Zugriff auf die Finanzdaten des Unternehmens und der Geschäftsführer eines Krankenhauses muss sich keine Krankenakten von Patienten ansehen können.

Geben Sie Ihren Anwendern nur die Zugriffsrechte, die sie für ihre Arbeit benötigen.

Ausführung von Code an bestimmten Orten verhindern

Richten Sie Software-Kontrollen ein, die die Ausführung von Code in von Ransomware häufig genutzten Orten verhindern. Dazu gehören von Browsern erstellte temporäre Ordner und komprimierte Dateiverzeichnisse in den Windows-Ordnern AppData bzw. LocalAppData.

Einschränkung unbekannter Software

Sinnvoll ist die Einrichtung einer Richtlinie für vertrauenswürdige Software, die Systemen nur die Ausführung von bekannten und geprüften Programmen erlaubt. Eine solche Richtlinie würde die Ausführung von Ransomware in den meisten Fällen verhindern. Eventuell ist dies jedoch nicht an jedem Arbeitsplatz möglich.

Einsatz von VM-Technologie

Mithilfe von virtuellen Maschinen (VMs) können Anwendungen und sogar komplette Betriebssysteme in einer isolierten Umgebung ausgeführt werden.

VMs dienen dabei als eine Art Detonationskammer im Software-Format. Das Ausführen von vertraulichem oder ungeprüftem Code in einer VM-Umgebung oder einem VM-Container stellt sicher, dass dadurch entstehende Sicherheitsprobleme auf die virtuelle Umgebung begrenzt sind und andere Teile des Systems unberührt bleiben.

Segmentierung von Systemen und Daten

Trennen Sie wertvolle Daten und Systeme voneinander, damit ein Sicherheitsproblem auf einem System keine anderen Systeme beeinträchtigt. Vertrauliche Forschungs- oder Unternehmensdaten zum Beispiel sollten sich nicht im gleichen Server und Netzwerksegment wie die E-Mail-Umgebung des Unternehmens befinden.

Alle Empfehlungen der US-Regierung finden Sie unter **fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf**.

Während des Angriffs

Sie sind Opfer eines Ransomware-Angriffs geworden. Wie geht es weiter?

Obwohl die beste Strategie gegen Ransomware die Vermeidung von Infektionen ist, haben die immer raffinierteren Angriffe gezeigt, dass es auch sehr gut aufgestellte Unternehmen treffen kann. Häufig ist Ransomware nicht die erste Malware-Payload in Ihrem System, da viele Ransomware-Gruppen mittlerweile verstärkt Zugänge zu Opfersystemen erwerben, die bereits mit Trojanern oder Loadern infiziert sind.

Während des Angriffs müssen Sie dringende Probleme bewältigen, zum Beispiel Rechner, Telefone und Netzwerke wieder hochfahren und sich um Lösegeldforderungen kümmern.

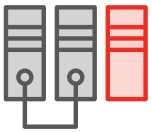
Eine vorschnelle Reaktion ist dabei wenig hilfreich und könnte die Lage noch verschlimmern.

Anruf bei den Strafverfolgungsbehörden

Ransomware ist wie jede Form von Diebstahl oder Erpressung eine Straftat. Niemand hat das Recht, Geräte, Netzwerke oder Daten in Beschlag zu nehmen, geschweige denn, dafür Lösegeld zu verlangen. Das Einschalten der zuständigen Behörden ist daher ein erster wichtiger Schritt.

Kontaktieren Sie bei einem Angriff sofort die Strafverfolgungsbehörden. Zögern Sie nicht, den Telefonhörer in die Hand zu nehmen und dort anzurufen. Die Behörden sind da, um Ihnen zu helfen.

Ebenso sollten Sie Ihren Ransomware-Versicherer kontaktieren und in Erfahrung bringen, ob der Schaden von der Versicherung gedeckt wird. Er kann Sie auch beim Koordinieren der Zwischenfallreaktion und -untersuchung unterstützen.



Isolierung infizierter Systeme

Sobald Mitarbeiter die Lösegeldforderung sehen oder etwas Ungewöhnliches beobachten (z. B. den plötzlichen Verlust von Zugriffsrechten auf die eigenen Dateien), sollten sie sich vom Netzwerk trennen und den infizierten Rechner zur IT-Abteilung bringen.

Wir raten davon ab, den Neustart von den Mitarbeitern selbst durchführen zu lassen, sondern das dem IT-Sicherheitsteam überlassen. Und auch das funktioniert nur, wenn es sich um Scareware oder gefälschte Ransomware handelt.

Dabei handelt es sich um Malware, die sich als Ransomware ausgibt. Sie sperrt den Bildschirm eines Anwenders und zeigt eine Lösegeldforderung sowie Zahlungsanweisungen an. Die Daten sind jedoch nicht wirklich verschlüsselt. In dieser Situation können normale Malware-Schutz-Tools Abhilfe schaffen.

Es ist jedoch nicht immer ganz einfach, den Unterschied zu erkennen. Sie sollten daher das Ausmaß des Problems basierend auf Bedrohungsdaten bestimmen. Ransomware ist zwar immer gefährlich, doch nicht alle Angriffe haben gravierende Folgen. Ihre Reaktion – und dazu gehört auch, ob Sie Lösegeld zahlen oder nicht – hängt von mehreren Faktoren ab.

Stellen Sie sich folgende Fragen:

- **Um welche Angriffsart handelt es sich?** Ist der Angriff eine sekundäre Infektion? Stammt er von Downloadern, Remote-Zugriffs-Trojanern oder anderer Malware, die auf dem infizierten Rechner oder auf anderen Geräten im Netzwerk installiert ist?
- **Welche Anwender in Ihrem Netzwerk sind kompromittiert?** Wie weit haben sich die Infektionen ausgebreitet? Späht ein Bedrohungsakteur aktiv Ihr Netzwerk aus, exfiltriert Daten oder will Ransomware auf anderen Geräten installieren?
- **Welche Netzwerkberechtigungen besitzen die kompromittierten Konten oder Geräte?** Möglicherweise wurde die Ransomware erst installiert, nachdem sich die Angreifer bereits lateral im Netzwerk bewegt oder Anmeldedaten bzw. andere Daten gestohlen haben.

Die Antworten sollten den Netzwerk-Administratoren helfen, das Ausmaß des Problems zu erfassen, einen Aktionsplan zu entwickeln und die Verbreitung möglichst zu stoppen.

Bedenken Sie, dass Ransomware sich schnell verbreitet und häufig gemeinsam mit anderen Bedrohungen auftritt. Wenn Sie eine Infektion bemerken, gibt es dort wahrscheinlich noch weitere, die Sie nicht sehen. Suchen Sie proaktiv nach weiteren Problemen in Ihrer Umgebung.

Umsetzung des Reaktionsplans

Je nach Netzwerkkonfiguration lässt sich die Infektion eventuell auf einen einzelnen Arbeitsplatz eindämmen.

Im besten Fall wird der infizierte Rechner durch einen neuen ersetzt und ein Backup eingespielt. Im schlimmsten Fall sind alle Rechner im Netzwerk infiziert. In einer solchen Situation ist eine Kosten-Nutzen-Rechnung notwendig, in der die Zeit und Ressourcen für die Wiederherstellung der Daten gegen eine Zahlung des Lösegeldes abgewogen werden.

Hat die Ransomware Ihre Server bereits infiziert, müssen Sie die betroffenen Systeme isolieren. Bei der Eindämmung der Bedrohung kann eine Netzwerksegmentierung hilfreich sein.

Ein wichtiger Teil Ihrer Reaktion ist die Entscheidung, ob Sie das Lösegeld zahlen sollten. Es gibt darauf keine einfache Antwort. Gegebenenfalls sollten Sie dazu den Rat der Behörden und Ihrer Rechtsberater einholen. Für einige Opfer gibt es möglicherweise keine andere Option als die Zahlung (siehe **„Zahlen oder nicht zahlen: das ethische und rechtliche Dilemma von Ransomware“ auf Seite 21**).

Verlassen Sie sich nicht auf kostenlose Ransomware-Entschlüsselungstools. Einige Sicherheitsanbieter verteilen kostenlose Entschlüsselungsprogramme für Ransomware. In einigen Fällen können Sie Ihre Daten damit zurückholen, ohne das Lösegeld zu zahlen.

Die meisten kostenlosen Tools funktionieren jedoch nur für eine einzelne Ransomware-Variante oder sogar nur für eine einzige Angriffskampagne. Da die Angreifer ihre Ransomware weiterentwickeln, sind die kostenlosen Tools oft nicht mehr aktuell und für Ihren Fall wahrscheinlich nutzlos.

Es kann sein, dass Sie mit einem kostenlosen Entschlüsselungstool Glück haben – es sollte jedoch nicht Bestandteil Ihres Reaktionsplans auf Zwischenfälle sein.

Wiederherstellung aus Backups

Eine vollständige Wiederaufnahme des Betriebs nach einer Ransomware-Infektion ist nur durch Wiederherstellung aus einem – am besten täglich durchgeführten – Backup möglich. Dies ist sicher der letzte Schritt, wenn Sie eine Infektion bekämpfen. Bei der Prävention sollte er jedoch an erster Stelle stehen.

Doch selbst mit aktuellen Backups kann es aus finanzieller und betrieblicher Hinsicht günstiger sein, das Lösegeld zu zahlen. Die Wiederherstellung mit Backups erfordert viel Zeit und Arbeit – und einige Unternehmen können sich den Ausfall möglicherweise nicht leisten.

Zahlen oder nicht zahlen: das ethische und rechtliche Dilemma von Ransomware

Ein Ransomware-Angriff an sich ist bereits schlimm genug. Ein besonders perfider Aspekt dabei ist jedoch, dass die Opfer zu einer unumgänglichen, aber ethisch problematischen Entscheidung gezwungen werden. Wer unter dem Druck einer Ransomware-Bedrohung steht, hat häufig nicht die Zeit, die ethischen Feinheiten einer Lösegeldzahlung abzuwägen. Der Angriff findet statt – hier und jetzt.

Die Zahlung ist dabei nicht nur ein schlimmes, aber notwendiges Übel, sondern finanziert zudem den Angreifer, der gerade ins Netzwerk eingebrochen ist und Daten gestohlen hat. Die Opfer geben sich quasi als jemand zu erkennen, der ein anfälliges Netzwerk und Gründe für eine Zahlung hat. Zudem ermöglicht das Lösegeld es dem Cyberkriminellen, zukünftige Angriffe zu finanzieren.

Doch die jüngsten Angriffe bringen eine unangenehme Tatsache ans Tageslicht: Die Antwort auf die Frage der Zahlung ist nicht immer eindeutig.

Kein Unternehmen möchte erpresst werden, geschweige denn kriminelle Organisationen finanzieren. Und doch haben viele Opfer das Gefühl, keine andere Wahl zu haben. In gewisser Hinsicht ist dies der Preis für eine unterbezahlte IT-Abteilung, die mit ungepatchter oder veralteter Software arbeitet. Es gibt immer noch Krankenhäuser, die veraltete Geräte mit Windows XP nutzen. Zudem ist das Zahlen der Lösegeldforderung häufig ein relativ geringer Preis, wenn es um Menschenleben geht.

In einigen Fällen empfiehlt sogar das FBI, „einfach das Lösegeld zu zahlen“. Offiziell rät die Behörde zwar von einer Zahlung ab. Kürzlich hat sie dem US-Kongress jedoch empfohlen, von einem Zahlungsverbot abzusehen.[19] Gleichzeitig weist das FBI darauf hin, dass auch die Zahlung keine Garantie bietet, dass Sie Ihre Daten zurückerhalten.

2020 gab das US-Finanzministerium eine Warnung heraus, in der die US-amerikanischen Bürger und Unternehmen daran erinnert wurden, dass sie mit der Zahlung eines Lösegeldes gegen Sanktionen oder Finanzvorschriften verstoßen könnten. Die Konsequenzen der Warnung werden von den Versicherungen und Unterhändlern für Zwischenfallreaktion noch ausgearbeitet, doch mögliche rechtliche Risiken erhöhen die Komplexität der Entscheidungsfindung.

Auch Europol, die Polizeibehörde der Europäischen Union, fordert in einer Kampagne dazu auf, Lösegelder nicht zu zahlen. Die Initiative „No More Ransom“, die vor fünf Jahren gestartet wurde, ist eine öffentlich-private Partnerschaft, die Opfern von Cyberangriffen hilft, Dateien wiederherzustellen und zu entschlüsseln, ohne Lösegeld zahlen zu müssen.

Durch die Initiative konnten bereits sechs Millionen Ransomware-Opfer ihre Dateien zurückerlangen und die Zahlung von beinahe 1 Milliarde Euro Lösegeld vermeiden. (Die „No More Ransom“-Tools stehen auch Personen außerhalb der Europäischen Union zur Verfügung.)

Bei der Entscheidung über die beste Vorgehensweise müssen Unternehmen einige gegensätzliche Überlegungen gegeneinander abwägen, zum Beispiel:

- Zeitaufwand und Ressourcen für die Wiederherstellung des Geschäftsbetriebes
- Verantwortung gegenüber den Anteilseignern für das Weiterlaufen des Geschäftsbetriebes
- Die Sicherheit der Kunden und Mitarbeiter
- Kriminelle Aktivitäten, die das Lösegeld finanzieren kann
- Gesetzliche Haftpflichten, die durch die Geldüberweisung an sanktionierte Personen oder Staaten drohen

Wie bei den meisten komplizierten Fragen kommt jedes Unternehmen zu individuellen Antworten.

Die jüngsten Angriffe bringen eine unangenehme Tatsache ans Tageslicht: Die Antwort auf die Frage der Zahlung ist nicht immer eindeutig.

19 Maggie Miller *(The Hill)*: „Top FBI Official Advises Congress Against Banning Ransomware Payments“, (Top-FBI-Mitarbeiter rät Kongress vom Verbot von Ransomware-Zahlungen ab), Juli 2021.

Nach dem Angriff

Abgesehen von den durch Ransomware verursachten Schäden deckt ein Angriff auch Sicherheitsfehler auf, die zur Kompromittierung eines Geräts oder Netzwerks geführt haben. Nachdem nun alles wieder normal läuft, haben Sie die Gelegenheit, aus der Kompromittierung zu lernen und zukünftige Attacken zu verhindern.

Wir empfehlen Ihnen, eine gründliche Sicherheitsbewertung – eventuell von einem externen Dienstleister – durchzuführen, damit Sie Bedrohungen finden, die sich noch in Ihrer Umgebung befinden könnten. Werfen Sie nun ebenfalls einen kritischen Blick auf Ihre Sicherheitstools sowie -abläufe und ermitteln Sie, was genau dort schiefging.

Bereinigung

Einige Ransomware-Varianten enthalten andere Bedrohungen oder Backdoor-Trojaner, die zu weiteren Angriffen führen können. In anderen Fällen hat eine bereits bestehende Kompromittierung eine Ransomware-Infektion ermöglicht. Sie sollten deshalb unbedingt jedes Gerät löschen und ein sauberes Backup einspielen. Suchen Sie sorgfältig nach verborgenen Bedrohungen, die Sie im Chaos möglicherweise übersehen haben.

Rückschau-Sicherheitsanalysen

Prüfen Sie, wie gut Sie auf die Bedrohung vorbereitet waren und wie Sie darauf reagiert haben. Wurde der Krisenplan umgesetzt? Können die Netzwerkkonfigurationen verbessert werden, um zukünftige Angriffe einzudämmen? Kann eine zuverlässigere E-Mail-Sicherheitslösung implementiert werden? Sollte allgemein ein ganz anderer Cybersicherheitsansatz gewählt werden?

Prüfen Sie die aktuellen Sicherheitsmaßnahmen und fragen Sie sich, ob diese zur Bekämpfung heutiger Bedrohungen ausreichen. Lernen Sie unbedingt aus dieser Erfahrung, denn es kann Sie jederzeit wieder treffen.

Wenn Sie nicht wissen, wie die Ransomware Ihre Schutzmaßnahmen überwunden hat, lässt sich auch der nächste Angriff nicht stoppen.

Bewertung des Sicherheitsbewusstseins der Anwender

Viele Ransomware-Familien sind zur Übertragung von Schaddaten auf Interaktionen von Anwendern angewiesen – entweder als direkte Infektion oder als spätere Übertragung durch einen anderen Malware-Typ. Sollten die bestehenden Sicherheitsmaßnahmen versagen und es kommt eine gefälschte „unbezahlte Rechnung“ zum E-Mail-Server durch, entscheidet ein gut geschulter Anwender als letzte Verteidigungslinie, ob ein Unternehmen, ein Krankenhaus oder eine Schule den Betrieb aufrecht erhält oder in die Ransomware-Statistik eingeht. Sorgen Sie dafür, dass Ihre Mitarbeiter dieser Aufgabe gewachsen sind.

Es ist sicher auch sinnvoll, in Tools für Phishing-Simulationen zu investieren, mit denen Sie die Sensibilisierung der Mitarbeiter verbessern, besonders gefährdete Anwender identifizieren und die allgemeine Sicherheit erhöhen können. Phishing-Simulationen spiegeln reale Angriffe sowie die neuesten Social-Engineering-Techniken und -Methoden wider und unterstützen Sie im Vorfeld eines Angriffs bei der Analyse und Identifizierung personenzentrierter Sicherheitsschwachstellen.

Schulungen

Nachdem Sie das Sicherheitsbewusstsein bewertet haben, sollten Sie einen Schulungsplan entwickeln, der auf die Schwachstellen der Mitarbeiter bei Cyberangriffen, einschließlich der Erfahrungen aus vorangegangenen Zwischenfällen, eingeht. Planen Sie regelmäßige Folgeschulungen für Mitarbeiter, die anfälliger sind, häufiger angegriffen werden oder umfassende Zugriffsrechte für vertrauliche Daten, Systeme und andere Ressourcen besitzen.

Zudem sollten Sie Ihr Schulungsprogramm in andere Cyberschutzmaßnahmen integrieren, sodass Ihre Mitarbeiter Angriffe nicht nur identifizieren, sondern umgehend melden können.

Investition in moderne Schutzmaßnahmen

Heutige Angriffe haben nicht die Infrastruktur, sondern den Menschen im Visier. Entscheiden Sie sich daher für Sicherheitslösungen, die für den Schutz Ihrer Mitarbeiter einen personenzentrierten Ansatz wählen.

Angreifer sehen die Welt nicht als Netzwerkdiagramm. Verwenden Sie daher eine Lösung, die Ihnen zeigt, wer wie angegriffen wird und ob die angegriffene Person geklickt hat. Berücksichtigen Sie dabei das individuelle Risiko der einzelnen Anwender, einschließlich der Informationen dazu, wie sie angegriffen werden, auf welche Daten sie zugreifen können und wie leicht sie sich täuschen lassen.

Halten Sie riskante Webinhalte von Ihrer Umgebung fern, indem Sie Webseiten von verdächtigen und nicht verifizierten URLs in einem geschützten Container innerhalb des normalen Webbrowsers des Anwenders darstellen lassen. Eine solche Web-Isolierungstechnologie ist ein wichtiger Schutz für E-Mail-Konten, die von mehreren Personen genutzt werden und daher nur schwer mit Mehrfaktor-Authentifizierung abgesichert werden können. Außerdem können Sie auf diese Weise das private Surfverhalten sowie die Webmail-Services Ihrer Anwender isolieren und die Freiheit und Privatsphäre Ihrer Mitarbeiter gewährleisten, ohne das Unternehmen zu gefährden.

Für kleinere, gezielte Angriffe benötigen Sie erweiterte Bedrohungsinformationen. Entscheiden Sie sich für eine Lösung, die mithilfe von statischen und dynamischen Techniken Angriffs-Tools, -Taktiken und -Ziele aufdeckt und daraus Erkenntnisse zieht.

Nächste Schritte

Solange die Cyberkriminellen mit Ransomware Geld machen können, wird sie in irgendeiner Form weiterbestehen. Die Empfehlungen in diesem Leitfaden helfen Ihnen bei der Bewältigung einer Ransomware-Infektion vor, während und nach einem Angriff.

Natürlich besteht der einfachste Weg im Kampf gegen Ransomware darin, bereits das Eindringen zu verhindern. Dies erfordert Cyberschutzmaßnahmen, die für moderne Bedrohungen entwickelt wurden.

Zuverlässige Cybersicherheit muss personenzentriert sein. Sie umfasst Schulungen zur Sensibilisierung für Sicherheit auf Basis realer Angriffstechniken, damit Anwender widerstandsfähiger Anwender werden. Sie identifiziert und beseitigt Ransomware, die es auf Ihre Mitarbeiter abgesehen hat. Zudem dämmt sie Bedrohungen ein und hilft Ihnen, im Ernstfall schnell und effektiv zu reagieren.

Weitere Informationen zur Abwehr von Ransomware finden Sie unter **www.proofpoint.com/de**.

WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter **proofpoint.com.de**.

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. ist ein führendes Unternehmen für Cybersicherheit und Compliance. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter mehr als die Hälfte der Fortune-1000-Unternehmen, setzen auf die personenzentrierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter **www.proofpoint.de**.

proofpoint.

0501-006-01-01 11/21