proofpoint.

E-BOOK

2023

Ransomware-Leitfaden

Prävention, Eindämmung und Wiederherstellung nach Bedrohungen – in jeder Phase der Angriffskette

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. Im Jahr 2022 kam es immer wieder zu Ransomware-Angriffen auf Schulbezirke[1], regionale und nationale Behörden[2] sowie Unternehmen im Gesundheitswesen[3]. Cyberkriminelle sind bei der Wahl ihrer Erpressungsopfer also keinesfalls wählerisch. Angesichts der erheblichen Gefahr dieser Bedrohung ist es wichtiger als je zuvor, einen Plan zur Minimierung von Risiken zu implementieren und sofort zu reagieren, sobald Ihre Systeme mit Ransomware infiziert und Ihre Daten gestohlen werden.

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.

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.

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. Außerdem sollten mit dem Internet verbundene Geräte wie Dateiübertragungs- und VPN-Appliances kontinuierlich gepatcht und Fernverwaltungstools sowie Protokolle (z. B. RDP) abgesichert werden.

Der vorliegende Leitfaden soll als Ausgangspunkt dienen.

1 Howard Blume, Alejandra Reyes-Velarde (Los Angeles Times): „Student information remains at risk after massive cyberattack on Los Angeles Unified“ (Studenteninformationen bleiben nach einem massiven Cyberangriff auf Los Angeles Unified weiterhin gefährdet), September 2022.
2 Kate Conger, David Bolaños (New York Times): „Russian Hacking Cartel Attacks Costa Rican Government Agencies“ (Russische Hackerkartelle greifen Behörden in Costa Rica an), Mai 2022.
3 Naomi Diaz (Becker's Hospital Review): „289 healthcare organizations were impacted by ransomware attacks in 2022“ (289 Unternehmen im Gesundheitswesen im Jahr 2022 mit Ransomware angegriffen), Januar 2023.

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 unveränderbarer 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.

Beachten Sie dabei, dass Backups zwar notwendig, aber keinesfalls stets ausreichend sind. In vielen Fällen kommt es bei Ransomware-Angriffen auch zu Datendiebstahl, sodass Backups die Angreifer nicht davon abhalten können, diese Daten zu veröffentlichen, zu verkaufen oder zu missbrauchen.

Aktualisieren und Patchen von Systemen

Halten Sie Betriebssysteme, Sicherheitssoftware, Anwendungen und Netzwerk-Hardware immer auf dem neuesten Stand, um allzu leicht zugängliche Schwachstellen zu schließen. Das gilt insbesondere für mit dem Internet verbundene Geräte, die gern von Angreifern missbraucht werden, z. B. VPNs und Dateiübertragungs-Appliances.

Investition in zuverlässige personenzentrierte Sicherheitslösungen

Viele Formen von personenzentrierten Angriffen (z. B. schädliche Anhänge, URLs und Phishing-E-Mails) führen zu einer Ransomware-Infektion. Vor einiger Zeit haben Bedrohungsakteure sogar mit so genanntem Callback Phishing begonnen, das auch als TOAD (Telephone-Oriented Attack Delivery, Angriff per Telefon) bezeichnet wird. Bei diesen Angriffen ist der einzige schädliche Teil der E-Mail die angegebene Telefonnummer. Nur die fortschrittlichsten E-Mail-Sicherheitslösungen können vor all diesen Angriffen sowie vor allen Malware-Formen schützen, die per E-Mail übertragen werden.

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.

Absicherung Ihrer Identitätsinfrastruktur

Die meisten Ransomware-Angreifer müssen privilegierten Zugriff erlangen, um ihre Malware auf genügend Geräten installieren und ihre Opfer lahmlegen zu können. In den meisten Fällen geschieht dies über Microsoft Active Directory. Dabei kommen verschiedene leicht zugängliche Tools wie BloodHound, PingCastle, Impacket und Cobalt Strike zum Einsatz. Diese Tools führen Microsoft-Hilfsprogramme – keine Malware – aus, um den ursprünglichen Basiszugriff in so genannte Tier-0-Berechtigungen zu erweitern, wie ihn beispielsweise Domain-Administratoren haben.

Wenn Sie eine Identitätsschutzlösung – oder sogar die gleichen Open-Source-Tools – nutzen, können Sie nachvollziehen, welche Wege ein Angreifer nehmen kann. Das Aufdecken dieser Wege ist von größter Wichtigkeit, da Sie so verstehen, wie Sie die Ausweitung einer einzigen Kompromittierung zu einem massenhaften und unternehmensweiten Ransomware-Zwischenfall verhindern können.

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 abwägen als Unternehmen im Privatkundengeschäft. 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, 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), Januar 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, Telefonanlagen und Netzwerke wieder hochfahren und sich um Lösegeld-forderungen kümmern.

Abtrennung vom Netzwerk

Sobald Ihre Mitarbeiter die Lösegeldforderung sehen oder etwas Ungewöhnliches beobachten, sollten sie die Netzwerkverbindung 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.

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.

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 Tests 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. Für die Reaktion auf Zwischenfälle sollten Sie auch über die Tools verfügen, mit denen Sie Hinweise dafür finden können, wie ein Angreifer privilegierten Zugriff in Ihrer Umgebung erlangt hat (was meist über Active Directory erfolgt). Dadurch können Sie bei zukünftigen Zwischenfällen laterale Bewegungen und Berechtigungseskalation verhindern.

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

ABSCHNITT 1

Einführung

Ransomware ist seit mehr als dreißig Jahren im Umlauf und hat in dieser Zeit mehrere Entwicklungsschritte genommen. Im Laufe des vergangenen Jahres sind die Geldsummen, die an Ransomware-Erpresser gezahlt wurden, stetig zurückgegangen. Dies scheint mit der Stilllegung großer Ransomware-Gruppen – einschließlich einiger Verhaftungen – sowie sinkenden Kryptowährungskursen zusammenzuhängen.[7]

Dabei darf jedoch nicht vergessen werden, dass dieser Rückgang von Ransomware-Zahlungen auf einen enormen Anstieg folgt: Im Jahr 2021 erreichten Angriffsvolumen und gezahlte Geldbeträge ein Rekordhoch.[8] Üblicherweise tauchen Ransomware-Kriminelle, nachdem ihre Aktivitäten von Strafverfolgungsbehörden unterbrochen wurden, an anderer Stelle mit neuen Namen und neuen Strategien wieder auf. Deshalb rechnen wir damit, dass auf den Rückgang ein neuer Anstieg folgen wird. Die Geschwindigkeit, mit der russische Kriminelle ihre Ransomware-Angriffe gegen Ziele in den USA durchführten, ging möglicherweise aufgrund des Ukraine-Krieges zurück. Es ist jedoch davon auszugehen, dass dies nicht von langer Dauer sein wird.

Angesichts laufender Maßnahmen von Regierungen und Strafverfolgern zum Stoppen von Cyberkriminalität wechseln die Bedrohungsakteure ihre Taktiken. 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.

Ransomware-Gruppen sind kreativ und immer auf der Suche nach neuen Möglichkeiten. Sie experimentieren mit neuen Taktiken, sodass die Verteidiger keinen Moment Ruhe haben.

7 Robert McMillan, Dustin Volz, Aruna Viswanatha (Wall Street Journal): „Hackers Extort Less Money, Are Laid Off as New Tactics Thwart More Ransomware Attacks“ (Hacker erpressen weniger Geld und werden entlassen, da neue Taktiken mehr Ransomware-Angriffe verhindern), Februar 2023.
8 James Rundle, David Uberti, Catherine Stupp (Wall Street Journal): „Cyber Defense Confidence Ebbs as Ransomware Attacks Multiply“ (Vertrauen in die Cyberabwehr nimmt ab, nachdem Ransomware-Angriffe zunehmen), Mai 2022.

In den Schlagzeilen

Weil die Zahl der Ransomware-Angriffe nicht abnimmt und ernsthafte Schäden an landeseigener Infrastruktur durch Cyberangreifer – mit oder ohne deren Absicht – immer wahrscheinlicher werden, wird Regierungen auf der ganzen Welt der Ernst der Lage allmählich bewusst.

Während der ersten Monate des Jahres 2022 verstärkten Aufsichtsbehörden und staatliche Stellen ihre Maßnahmen zur Bekämpfung von Ransomware-Angriffen. Im März veröffentlichte die US-Börsenaufsichtsbehörde SEC neue Vorschläge für Cybersicherheitsvorschriften, die für börsennotierte Unternehmen gelten sollten.[9] Laut diesen Vorschlägen sollen die Unternehmen verpflichtet werden, Ransomware-Angriffe und Datenschutzverletzungen zu melden. Außerdem sollen sie ihre Richtlinien zum Identifizieren und Kontrollieren von Cybersicherheitsrisiken offenlegen.

Noch im gleichen Monat erließ die Biden-Regierung ein Gesetz, das die Betreiber kritischer Infrastrukturen dazu verpflichtet, Cyberangriffe und Ransomware-Zwischenfälle innerhalb von 72 Stunden an die CISA (Cybersecurity and Infrastructure Security Agency) zu melden.[10] Ziel dieses neuen Gesetzes ist ein besserer Informationsaustausch zwischen dem öffentlichen und privaten Sektor, um solche Angriffe an anderer Stelle zu verhindern.

Die Maßnahmen der US-Behörden zur Eindämmung der Ransomware-Flut scheinen keine Auswirkungen auf die bekannte russische Ransomware-Gruppe Conti gehabt zu haben. Einen Monat später, im April 2022, attackierte die Gruppe erfolgreich die Regierung von Costa Rica, was eine der letzten Aktionen von Conti vor ihrem Rückzug aufgrund intensiver Strafverfolgung werden sollte. Von diesem Angriff waren fast 30 Regierungsbehörden betroffen, wobei medizinische Untersuchungen, Steuerzahlungen und grundlegende Bürgerservices beeinträchtigt wurden.[11] Als Reaktion darauf erklärte der neu gewählte Präsident Rodrigo Chaves den nationalen Notstand. Chaves erklärte, dass sein Land „im Krieg“ mit den Cyberkriminellen wäre, die im Dark Web zu seinem Sturz aufgerufen hätten.[12]

Im September 2022 kam es zu weiteren großen Ransomware-Angriffen auf Organisationen im öffentlichen Sektor. Der Los Angeles Unified-Schulbezirk wurde kurz vor dem Beginn des neuen Schuljahres von einem schlagzeilenträchtigen Ransomware-Zwischenfall getroffen. Die Bezirksverantwortlichen verweigerten jedoch die Lösegeldzahlung. Als Reaktion darauf veröffentlichten die Kriminellen, die etwa 500 GB an Daten erbeuten konnten – Dateien mit Sozialversicherungsnummern, Verträgen, Steuerformularen und Studentenakten des zweitgrößten Schulbezirks der USA.[13] Einige Tage später attackierten die Angreifer Suffolk County, abgesehen von den fünf Bezirken von New York City das bevölkerungsreichste County des Bundesstaats New York. Der Ransomware-Angriff führte zu einem kompletten digitalen Shutdown der Bezirksregierung.[14]

9 Paul Kiernan (Wall Street Journal): „SEC Proposes Requiring Firms to Report Cyberattacks Within Four Days“ (SEC möchte, dass Firmen Cyberangriffe innerhalb von 4 Tagen melden), März 2022.
10 David Uberti (Wall Street Journal): „Fearing More Cyberattacks, Congress Requires Key Businesses to Report Digital Breaches“ (Aus Sorge vor weiteren Cyberangriffen will der Kongress, dass wichtige Unternehmen digitale Kompromittierungen melden), März 2022.
11 Dustin Volz (Wall Street Journal): „U.S. Saw Signs of Decline in Russian Ransomware Strikes at Start of Ukraine War“ (USA sehen Hinweise für einen Rückgang russischer Ransomware-Angriffe seit Beginn des Ukraine-Krieges), Mai 2022.
12 Carly Page (TechCrunch): „Fears Grow for Smaller Nations After Ransomware Attack on Costa Rica Escalates“ (Kleinere Staaten in Sorge nach eskaliertem Ransomware-Angriff auf Costa Rica), Mai 2022.
13 Howard Blume (Los Angeles Times): „L.A. Unified data breach last year includes at least 2,000 student records, officials say“ (Datenschutzverletzung bei L.A. Unified im vergangenen Jahr betrifft mindestens 2.000 Studenten), Februar 2023.
14 James Rundle (Wall Street Journal): „Suffolk County, N.Y., Hack Shows Ransomware Threat to Municipalities“ (Hackerangriff auf Suffolk County, New York, verdeutlicht Ransomware-Bedrohung für Gemeinden), November 2022.

Bald darauf wurde die Mitfahrplattform Uber zum neuesten Opfer der berüchtigten Bedrohungsgruppe Lapsus$ und reihte sich damit ein hinter Microsoft, Nvidia, Okta, Samsung und weitere bekannte Technologiefirmen.[15] Die Angriffe von Lapsus$ umfassen meist Social Engineering, um an Anmeldedaten für Mitarbeiterkonten zu gelangen. Auch wenn die Gruppe häufig versucht, Geld von ihren Opfern zu erpressen, installiert sie dazu nur selten Malware auf deren Computern.

Ein Ransomware-Angriff auf den Cloud-Dienstanbieter Rackspace im Dezember 2022 bildete den Abschluss des Jahres. Der Angriff führte zum Ausfall der unternehmenseigenen Hosting-Plattform für Microsoft Exchange, sodass die Kunden keinen Zugriff mehr auf ihre E-Mails hatten. Rackspace bestätigte später, dass die Bedrohungsgruppe Play für den Zwischenfall verantwortlich war.[16]

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.

Die Opfer werden häufig mehrfach erpresst: Zunächst für einen Verschlüsselungsschlüssel zur Entschlüsselung der Daten und danach erneut als Gegenleistung dafür, dass die Angreifer nicht Kopien davon veröffentlichen oder im Dark Web veräußern. Heute umfassen fast alle Ransomware-Zwischenfälle auch Datendiebstahl. Viele Gruppen konzentrieren sich mittlerweile einzig und allein auf Datendiebstahl und versuchen gar nicht, Ransomware zu installieren, Daten zu verschlüsseln oder Informationen zu zerstören.

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

Das macht diese Angriffe für ihre Opfer umso gefährlicher. Nachdem die Daten gestohlen wurden, gibt es keine Gewährleistung dafür, dass sie jemals wieder in ihren Besitz bekommen. Und selbst wenn das gelingt, ist es kaum möglich herauszufinden, ob sie bereits verkauft wurden oder ob das in der Zukunft geschehen kann. Das macht die Entscheidung über die Zahlung des Lösegeldes noch schwieriger.

Noch perfider wird die ganze Angelegenheit dadurch, dass Cyberkriminelle immer häufiger dazu übergehen, gleich dreifach abzukassieren, d. h. sie erpressen ein Lösegeld für die Rückgabe oder Entsperrung der gestohlenen Daten, ein zweites Lösegeld für die Zerstörung dieser gestohlenen Daten sowie ein drittes Lösegeld für Informationen über Manipulationen an den zurückgegebenen Daten.

15 Robert McMillan (Wall Street Journal): „Uber Says Breach Was by Lapsus$, a Teenage Hacking Group Motivated by Fame Over Money“ (Uber-Kompromittierung wurde von Lapsus$ durchgeführt, einer Teenager-Hackergruppe, die es mehr auf Ruhm statt auf Geld abgesehen hat), September 2022.
16 Eric J. Savitz (Barron’s): „Rackspace Ransomware Attack Reveals the Cloud’s Vulnerability“ (Ransomware-Angriff auf Rackspace verdeutlicht Anfälligkeit der Cloud), Dezember 2022.

64 %
der Unternehmen wurden 2022 mit Ransomware infiziert.

64 %
haben das Lösegeld gezahlt.

Die realen Kosten

Fast zwei Drittel aller weltweiten Unternehmen verzeichneten im Jahr 2022 mindestens einen Ransomware-Angriff. 64 % davon zahlten das Lösegeld.[17] Die finanziellen Folgen eines Angriffs können beträchtlich sein, wobei durchschnittliche Lösegeldsummen bei mehr als 400.000 US-Dollar liegen.[18]

Laut Cybersicherheitsanalysten gingen die Zahlungen an Ransomware-Gruppen im Jahr 2022 um 40 % zurück, lagen jedoch immer noch bei insgesamt 457 Millionen US-Dollar.[19] Auch die durchschnittliche Höhe der Lösegeldforderungen ist gesunken – von durchschnittlich 5,7 Millionen US-Dollar im Jahr 2021 auf 4,1 Millionen im Folgejahr.[20] Experten gehen davon aus, dass immer mehr Opfer die Zahlung verweigern, insbesondere nachdem die US-Behörde OFAC (U.S. Department of the Treasury's Office of Foreign Assets Control) erklärt hatte, dass Unternehmen Strafen riskieren, wenn sie Geld an sanktionierte Gruppen zahlen.[21] Viele Lösegeldzahlungen bleiben jedoch nicht gemeldet – und die Androhung von Strafen kann dazu führen, dass noch mehr Zahlungen im Verborgenen ablaufen werden. Die wahren finanziellen Kosten durch Ransomware sind sehr schwierig zu ermitteln, da einige Unternehmen einen Zwischenfall eher im Stillen zu bewältigen versuchen.

Die betrieblichen Kosten beschränken sich jedoch nicht nur auf den finanziellen Aspekt. Bei der überwiegenden Mehrzahl der Ransomware-Angriffe besteht mittlerweile das Risiko, dass die exfiltrierten Daten geleakt werden. Das führt dazu, dass alle Ransomware-Zwischenfälle die gleichen Konsequenzen wie eine Datenschutzverletzung nach sich ziehen und von Reputationsschäden für das Unternehmen bis zu Offenlegungspflichten und potenziellen Strafzahlungen reichen.

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. Noch schwerwiegender können die Konsequenzen in kritischen Sektoren wie dem Gesundheitswesen sein. Der katholische gemeinnützige Gesundheitsanbieter CommonSpirit Health stellt das auf die harte Tour fest, nachdem es bei ihm zu einem wochenlangen Ausfall der Netzwerke und IT-Systeme in Folge eines Ransomware-Angriffs gekommen war. Nach dem Zwischenfall wurde eine Sammelklage gegen die Organisation erhoben, da diese ihre Patientendaten nicht ausreichend geschützt haben soll.[22]

17 Proofpoint: „State of the Phish 2023", Februar 2023.
18 Coveware: „Improved Security and Backups Result in Record Low Number of Ransomware Payments" (Verbesserungen bei Sicherheit und Backups führen zu einem Rekordtief bei Lösegeldzahlungen), Januar 2023.
19 Robert McMillan, Dustin Volz, Aruna Viswanatha (Wall Street Journal): „Hackers Extort Less Money, Are Laid Off as New Tactics Thwart More Ransomware Attacks" (Hacker erpressen weniger Geld und werden entlassen, da neue Taktiken mehr Ransomware-Angriffe verhindern), Februar 2023.
20 ebd.
21 Department of the Treasury: „Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments" (Hinweise zu potenziellen Sanktionsrisiken bei gezahlten Ransomware-Lösegeldern), Oktober 2022.
22 Annie Burky (Fierce Healthcare): „Class action accuses CommonSpirit Health of negligence following major ransomware attack and data breach" (Sammelklage gegen CommonSpirit Health wegen Fahrlässigkeit nach einer großen Ransomware-Attacke und Datenschutzverletzung), Januar 2023.

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)
- Kompromittierte Cloud-Konten, die Malware-Uploads ermöglichen
- 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.

Entwicklung

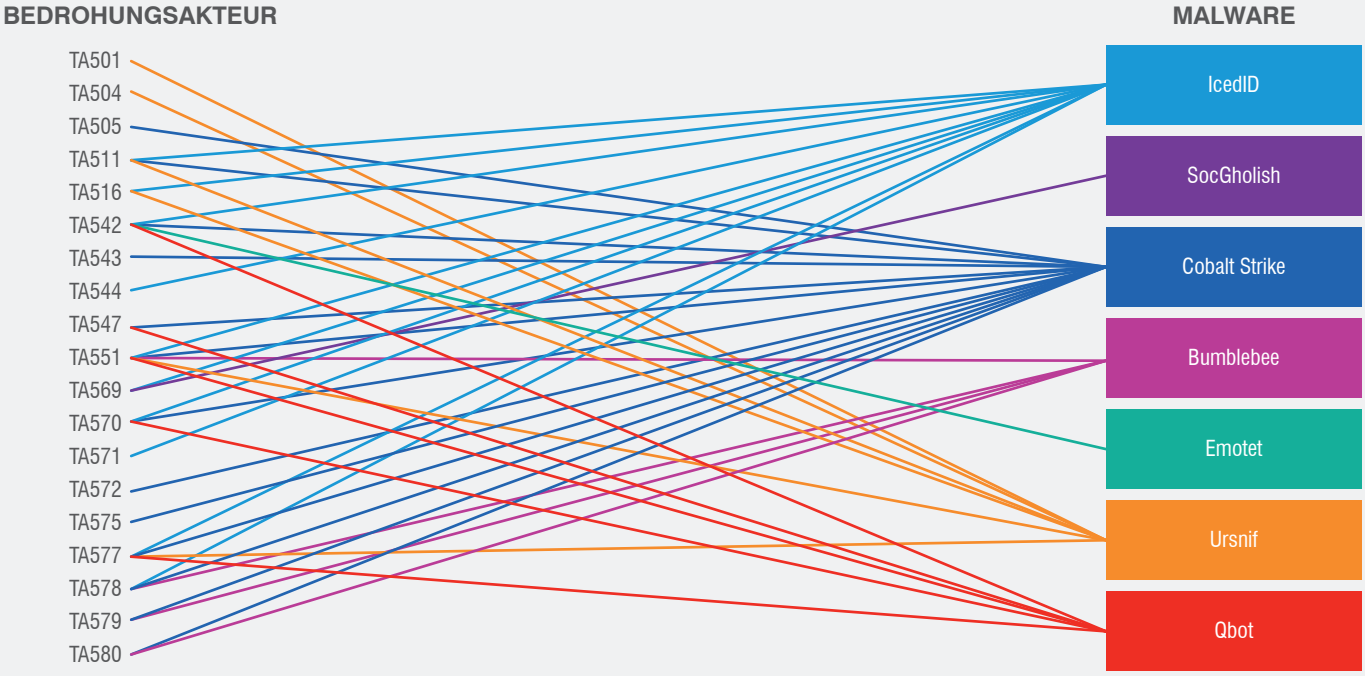
Ransomware wird aktiv weiterentwickelt, da die Angreifer sich an neue Schutzmaßnahmen anpassen, neue Vorgehensweisen entwickeln und neue Tools einsetzen. Im Folgenden zeigen wir die Bereiche, in denen sich die Bedrohungslandschaft verändert.

Ransomware und 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 sieben 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, die als Erstzugriffsvermittler (Initial Access Broker) bezeichnet werden, 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 viele Malware-Familien, die aktiv für diesen Erstzugriff genutzt werden, und mehrere Cybercrime-Gruppen sind für deren Verbreitung bekannt. Seit 2022 fanden Proofpoint-Forscher potenzielle Erstzugriffs-Malware in den Kampagnen folgender Gruppen:



Wir müssen darauf hinweisen, dass wir nicht beobachtet haben, wie diese kriminellen Gruppen selbst Ransomware verteilt haben. Es lassen sich auch keine direkten Beziehungen zwischen Malware und Ransomware-Familien finden. Alle Malware-Varianten auf dieser Liste führen jedoch zu einer Ransomware-Infektion und werden regelmäßig von den aktivsten Angreifern der Welt verteilt.

In den meisten Unternehmen besteht die erste Verteidigungslinie gegen Ransomware darin, die Anwender am Herunterladen von Remote-Zugriffs-Trojanern (RATs), Botnets und sonstiger Malware zu hindern. Wenn Sie die Loader blockieren, blockieren Sie die Ransomware.

Das Beziehungsnetzwerk zwischen Cybercrime-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.

Insider-Bedrohungen

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.

Seither hat die Ransomware-Familie LockBit nach einer Reihe schlagzeilenträchtiger Attacken auf große Unternehmen und Behörden einige Bekanntheit erlangt.[23] Die Betreiber von LockBit werben aktiv um Insider, die ihnen helfen sollen, die Malware in den Netzwerken der Opfer zu platzieren. Dafür, so das Versprechen, würden sie Zahlungen in Millionenhöhe erhalten. LockBit bietet auch hohe Zahlungen für Insider, die ihnen Netzwerkzugriff oder gültige Kontodaten liefern.

Rekrutierungsversuche erfolgen meist per E-Mail, wobei die Nachrichten selbst keine Malware-Anhänge enthalten, sodass sie nur von fortschrittlichen E-Mail-Sicherheitslösungen erkannt werden. Es ist daher sinnvoll, Mitarbeiter in der Erkennung und zügigen Meldung dieser Bedrohungen zu schulen.

Doppelte (und dreifache) Erpressung

Die Tage, an denen Systeme nach einem Ransomware-Angriff einfach gesperrt und verschlüsselt wurden, sind vorbei. Die Bedrohungsakteure sind nun darauf aus, ihre Ausbeute zu erhöhen, indem sie mehrere Zahlungen verlangen, mehrere Datenschutzverletzungen durchführen, ihre Opfer auf Leak-Websites öffentlich bloßstellen und Verbraucher im Rahmen von doppelten oder dreifachen Erpressungen unter Druck setzen.

Vor Kurzem hat Proofpoint festgestellt, dass 64 % aller Unternehmen, die mit Ransomware infiziert wurden, sich auf die Lösegeldzahlung einlassen.[24] 41 % von ihnen mussten mehr als einmal zahlen. Zudem hatte ein kleiner Teil der Gruppe Pech und erhielt trotz der Zahlung keinen Zugang mehr zu den eigenen Daten, was leider nicht selten vorkommt.

In den letzten Jahren sehen wir, dass Ransomware-Angreifer ihre Opfer immer häufiger doppelt erpressen. Dabei werden Kundendaten exfiltriert und als Druckmittel benutzt, anstatt lediglich die Geschäftsabläufe stillzulegen. In einigen Fällen verschlüsseln die Bedrohungsakteure gar nicht erst, sondern gehen gleich zu Erpressungstaktiken über.

Die Zahl der böswilligen Akteure, die Datendiebstahl und Erpressung bevorzugen – und keine Ransomware nutzen – wächst, im Jahr 2022 um ganze 20 %.[25] Außerdem haben sich die Erpressungstechniken weiterentwickelt, wodurch die Zahl dreifacher Erpressungen gestiegen ist. In diesen Fällen umgehen die Ransomware-Gruppen die Unternehmen und wenden sich mit den gestohlenen Daten direkt an die Verbraucher, um sie auf eine Kompromittierung aufmerksam zu machen.

23 Aaron Sandeen (Dark Reading): „Everything You Need to Know About LockBit“ (Alles, was Sie über LockBit wissen müssen), November 2022.
24 Proofpoint: „State of the Phish 2023“, Februar 2023.
25 Crowdstrike: „Global Threat Report“, 2023.

Dadurch sollen die Verbraucher dazu gebracht werden, zusätzlichen Druck auf das betroffene Unternehmen auszuüben. In seltenen Fällen werden auch die Verbraucher selbst erpresst. Diese Technik kam beispielsweise im Dezember 2022 beim Knox College im US-amerikanischen Illinois zum Einsatz.[26] Die Ransomware-Gruppe Hive, der vor Kurzem das Handwerk gelegt wurde, erlangte Zugang zu vertraulichen Studenteninformationen und kontaktierte die Studenten direkt mit dem Wortlaut „Für uns ist heute ein normaler Werktag. Für euch ist es ein trauriger Tag“ – und zählte anschließend ihre Forderungen auf.

Konventionelle Cyberschutzmaßnahmen sind durch Bedrohungen aus allen Richtungen überwältigt.

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
- Massenhafter Einsatz von Active Directory, der Angreifern die Wiederholung ihrer lateralen Bewegungen und Methoden zum Ausweiten von Berechtigungen erlaubt

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.

26 Kevin Collier (NBC): „Ransomware hackers take demands directly to college students: ‘For you, it’s a sad day’“ (Ransomware-Hacker richten ihre Forderungen direkt an College-Studenten: ‚Für euch ist es ein trauriger Tag‘), Dezember 2022.

Gezieltere Angriffe und raffiniertere Vorgehensweisen

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 Lösegeldsumme.

Gleichzeitig werden auch die Ransomware-Angriffe immer raffinierter. Anstatt Malware bereits in der ersten Angriffsphase einzusetzen, haben sich die Cybercrime-Gruppen stärker spezialisiert: Einige konzentrieren sich auf das Erlangen von Zugriff auf Unternehmensnetzwerke, während andere ihre Ransomware zur Miete anbieten. Eine dritte Gruppe ist in erster Linie mit Datenexfiltration und Erpressung beschäftigt.

Einerseits sind die Ransomware-Tools, die bei diesen Angriffen zum Einsatz kommen, erheblich zuverlässiger geworden, und einige Kriminelle veranstalten sogar Bug-Bounty-Programme zur Aufdeckung neuer Zero-Day-Exploits. Andererseits sind Angriffe häufiger geworden, bei denen es ausschließlich um den Diebstahl von Daten geht und die Opfer aufgefordert werden, dafür zu bezahlen, dass die Daten nicht verkauft oder geleakt werden. Dabei kommt häufig überhaupt keine Malware zum Einsatz.

13 Mio. USD

Karakurt, eine ausschließlich auf Erpressung spezialisierte Gruppe, hat Lösegeldforderungen von bis zu 13 Millionen US-Dollar gestellt.

Ransomware ohne „Ware“

Klassischerweise blockiert Ransomware den Zugriff der Opfer auf geschäftskritische Dateien und Systeme. Bei Unternehmen, deren Abläufe von digitalen Technologien abhängen (was heutzutage für fast alle gilt), führt ein solcher Angriff nicht nur zu Ausfällen und hohen Kosten, sondern mitunter auch zu verheerenden Konsequenzen.

Im Gesundheitswesen können Ausfälle beispielsweise die Patientenversorgung gefährden und lebensrettende Maßnahmen blockieren. Ein solcher Angriff kann auch zu Klagen wegen Fahrlässigkeit führen. Das geschah beispielsweise in einem Krankenhaus in Alabama, als ein Baby mit einem schweren Hirnschaden geboren wurde und später starb, weil die Klinik mit einem Ransomware-Angriff zu kämpfen hatte. Die Mutter erhob Anklage gegen das Krankenhaus.[27] Es überrascht daher nicht, dass Ransomware-Opfer sehr motiviert sind, so schnell wie möglich zu zahlen und solche Auswirkungen und möglicherweise schwerwiegenden Konsequenzen zu vermeiden.

Wie bereits oben erwähnt, ergänzen Ransomware-Gruppen ihre Angriffe mit weiteren Ebenen wie Datendiebstahl, um doppelte und dreifache Erpressung zu ermöglichen. Bei diesen Angriffe fordern die Kriminellen Geld selbst von den Unternehmen, die über zuverlässige Backups der verschlüsselten Daten verfügen. Weitere Geldzahlungen sollen sicherstellen, dass die vertraulichen Daten nicht veröffentlicht werden, da die potenzielle Weitergabe von Kunden-, Partner- und Anbieterdaten zu Gerichtsverfahren oder Geldstrafen führen kann. Diese Bedrohungen schaffen es häufig auch, die Opfer zuverlässig aus ihren eigenen Netzwerken auszusperren.

Aktuell setzen immer mehr Cybercrime-Gruppen auf Datendiebstahl und reine Erpressungsangriffe, ohne überhaupt dateienverschlüsselnde Malware zu installieren. Stattdessen exfiltrieren sie einfach die Daten und drohen damit, sie im Dark Web zu veröffentlichen oder das Opfer auf andere Weise öffentlich zu erniedrigen. Diese Angriffsstrategie ist schneller und hängt nicht von dateienverschlüsselnder Malware ab, die sich möglicherweise nur schwer im Netzwerk verbreiten lässt oder mitten in einem Angriff versagt.

LockBit, eine der aktivsten Ransomware-Gruppen des Jahres 2022, konzentriert sich in erster Linie auf Datenexfiltration. Ihr neuestes Ransomware-as-a-Service-Angebot war LockBit 3.0 (auch als LockBit Black bekannt). Parallel dazu veröffentlichte die Gruppe eine Reihe von „Partnerregeln“. Eine dieser Regeln verbietet explizit die Verwendung von Verschlüsselung bei Angriffen auf kritische Infrastrukturen.[28]

Parallel dazu hat Karakurt, eine ausschließlich auf Erpressung spezialisierte Gruppe, Lösegeldforderungen von bis zu 13 Millionen US-Dollar gestellt. Mitte des Jahres 2022 veröffentlichten das FBI und CISA eine gemeinsame Presseerklärung, in der sie vor Karakurt warnten.[29] Die Cybercrime-Gruppe wurde später mit der mittlerweile stillgelegten russischen Gruppe Conti in Verbindung gebracht.

Conti scheint die Aktivitäten eingestellt zu haben, nachdem ein Insider die internen Chats der Gruppe geleakt hatte, was Bedrohungsforschern die Kompromittierung der Conti-Server erlaubte. Später zeigte sich, dass Karakurt als Nebengeschäft entwickelt wurde, um die Daten zu monetarisieren, die bei den verschlüsselungsbasierten Conti-Angriffen erbeutet wurden.[30]

27 Kevin Collier (NBC News): „Baby died because of ransomware attack on hospital, suit says“ (Baby nach Ransomware-Angriff auf Krankenhaus gestorben), September 2021.
28 Lawrence Abrams (Bleeping Computer): „LockBit 3.0 introduces the first ransomware bug bounty program“ (LockBit 3.0 führt als erste Ransomware-Gruppe ein Bug-Bounty-Programm ein), Juni 2022.
29 Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), Department of the Treasury (Treasury) und Financial Crimes Enforcement Network (FinCEN): „Joint Cybersecurity Advisory: Karakurt Data Extortion Group“ (Gemeinsame Cybersicherheitsempfehlung: Datenerpresser-Gruppe Karakurt), Juni 2022.
30 Ionut Ilascu (Bleeping Computer): „Karakurt revealed as data extortion arm of Conti cybercrime syndicate“ (Karakurt erweist sich als als Datenerpresser-Arm des Cybercrime-Syndikats Conti), April 2022.

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.

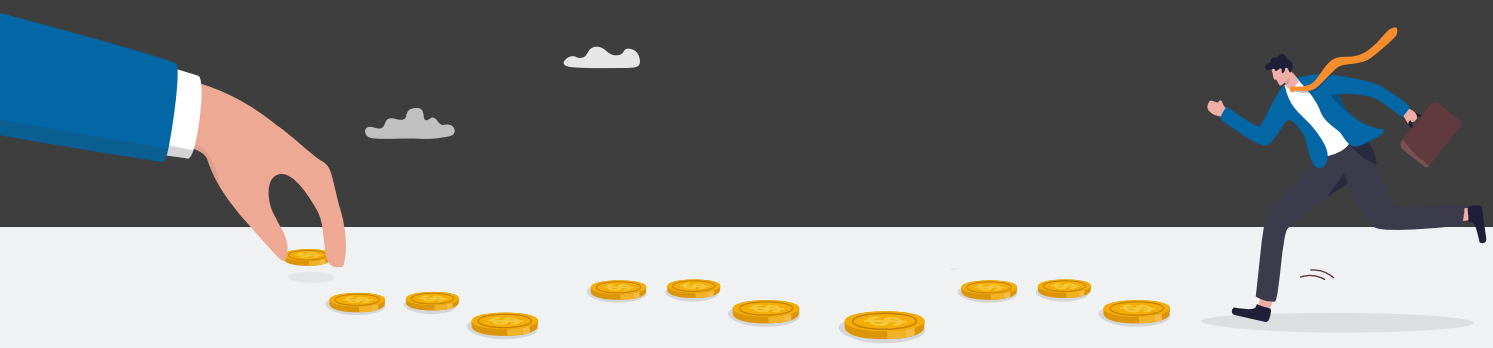
Im Gegensatz zu staatlich gestützten Währungen werden Kryptowährungen nicht überall als Zahlungsmittel anerkannt. Sie werden stattdessen mit Pokerchips, Spielmarken oder ähnlichen Systemen gleichgestellt. Das Übertragungssystem und die Tumbler werden daher nicht reguliert und gelten auch nicht als Geldwäsche – 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 bietet dieser Ansatz klare Vorteile. Letztere verlieren mit jedem Tag an Wert, da die Finanzinstitute immer zügiger Konten von Opfern sperren.

Der Wert von Bitcoin – sowie der weiterer Kryptowährungen – fiel im Jahr 2022 ins Bodenlose, nachdem sich Investoren aus diesen riskanten Assets zurückgezogen hatten. Durch diesen Crash Mitte Mai wurden mehr als 300 Milliarden US-Dollar an Wert für digitale Assets vernichtet.[31] Das hatte erhebliche Auswirkungen auf Cyberkriminelle sowie andere finanziell motivierte Verbrecher. Ransomware-Zahlungen – und die kriminellen Profite, sind immer noch auf einem Tiefpunkt.

Gleichzeitig haben die Strafverfolgungsbehörden die Nachverfolgung und Rückforderung von Kryptowährungszahlungen verbessert. Das FBI konnte 2,3 Millionen US-Dollar Lösegeld aus dem Angriff auf Colonial Pipeline zurückholen, der 2021 die Treibstoffversorgung weiter Teile der US-amerikanischen Ostküste unterbrochen hatte.[32] Ebenso konnte das FBI 130 Millionen US-Dollar an Ransomware-Profiten sicherstellen, nachdem es Zugriff auf die Server der Ransomware-Gruppe Hive erlangt hatte.[33]



31 David Yaffe-Bellany, Erin Griffith, Ephrat Livni (New York Times): „Cryptocurrencies Melt Down in a ‘Perfect Storm’ of Fear and Panic“ (Kryptowährungen verlieren an Wert in einem ‚Orkan‘ aus Angst und Panik), Mai 2022.
32 Dustin Volz, Sadie Gurman, David Uberti (Wall Street Journal): „U.S. Retrieves Millions in Ransom Paid to Colonial Pipeline Hackers“ (USA stellen Millionenbetrag aus Lösegeldzahlung nach Colonial-Pipeline-Hack sicher), Juni 2021.
33 Aruna Viswanatha, Dustin Volz (Wall Street Journal): „FBI Disrupts ‘Hive’ Ransomware Group“ (FBI legt Ransomware-Gruppe Hive still), Januar 2023.

ABSCHNITT 2

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. Backups sollten extern und unveränderbar gespeichert werden. Viele Unternehmen tun dies bereits, doch überraschend wenige führen Übungen zu ihren Backup- und Wiederherstellungsprozessen durch. Erst diese Übungen zeigen, ob der Backup-Plan wirklich funktioniert. Bei der Planung und Durchführung der Backup-Wiederherstellung sollte sichergestellt werden, dass die Backups in eine isolierte Umgebung wiederhergestellt werden können. Dadurch ist es möglich, übersehene Malware-Infektionen zu identifizieren und zu verhindern.

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. Es gibt jedoch einen Haken: Angreifer drohen immer häufiger damit, die Daten der Opfer zu veröffentlichen, wenn diese nicht zahlen. Auch wenn Sie also den GAU in Bezug auf Datenverlust verhindern können, haben Sie wahrscheinlich keine Kontrolle über die sonstigen Folgen wie Markenschäden, Gerichtsverfahren oder Geldstrafen.

70 %

der Sicherheitsverantwortlichen bezeichnen das Schwachstellenverwaltungs-programm ihres Unternehmens als mäßig effektiv – oder sogar noch schlechter.

In der Vergangenheit gingen die IT- und Sicherheitsteams häufig davon aus, dass Cloud-Speicher besser vor Ransomware-Angriffen geschützt wären als Endpunkte oder Netzwerklaufwerke. Aktuelle Untersuchungen zeigen jedoch den umgekehrten Fall: Bedrohungsforscher von Proofpoint haben eine potenziell gefährliche Funktion in Microsoft 365 entdeckt, mit der Ransomware Dateien in SharePoint und OneDrive so verschlüsseln kann, dass sie ohne spezielle Backups oder einen Entschlüsselungsschlüssel der Angreifer nicht wiederhergestellt werden können.[34] Deshalb können Ransomware-Attacken nun Unternehmensdaten in der Cloud angreifen, insbesondere wenn sie mithilfe kompromittierter Anmeldedaten Zugriff auf die SharePoint Online- oder OneDrive-Konten erlangen konnten.

Beachten Sie, dass Backups kein Allheilmittel vor Ransomware-Angriffen sind. In vielen Fällen liegt der Preis für die Wiederherstellung von Daten aus Backups – einschließlich geschäftlicher Ausfallzeiten, IT-Arbeitsstunden und Opportunitätskosten – deutlich über dem Lösegeld. Zudem kommt es bei vielen Ransomware-Attacken zu Datendiebstahl, und selbst die umfassendsten Backups können die Angreifer nicht daran hindern, die gestohlenen Daten zu leaken oder zu missbrauchen.

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 viele Unternehmen haben große Probleme, ihre Software zeitnah zu aktualisieren. Dieser Trend ist beunruhigend, da die Zahl der als kritisch bewerteten Schwachstellen in den letzten Jahren in die Höhe geschossen ist. Laut einer aktuellen Umfrage betrachten 70 % der Sicherheitsverantwortlichen das Schwachstellenverwaltungsprogramm ihres Unternehmens als mäßig effektiv – oder sogar noch schlechter. Nur 18 % konnten kritische Schwachstellen innerhalb von 24 Stunden nach deren Bekanntwerden patchen.[35]

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.

34 Proofpoint: „Proofpoint Discovers Potentially Dangerous Microsoft Office 365 Functionality that can Ransom Files Stored on SharePoint and OneDrive“ (Proofpoint deckt potenziell gefährliche Microsoft Office 365-Funktion auf, die Lösegelddateien in SharePoint und OneDrive speichern kann), Juni 2022.
35 Cyentia Institute: „The State of Vulnerability Management“ (Der Stand bei der Schwachstellenverwaltung), 2022.

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.

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 ad-hoc beantworten. Dieser Druck kann die Entscheidungsfindung verlangsamen und zu kostspieligen Verzögerungen führen. In die Entscheidungsfindung können viele Verantwortliche involviert sein, beispielsweise Mitarbeiter, Rechtsberater, Entscheidungsträger für Finanzen sowie der Vorstand. Diese Personen sollten am Planungsprozess beteiligt sein, noch bevor ein Angriff stattgefunden hat, damit im Notfall eine reibungslose und schnelle Reaktion gewährleistet ist.

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

Investieren Sie in zuverlässige personenzentrierte E-Mail-, Web- sowie Identitätsschutz-Lösungen.

Ransomware existiert nicht im luftleeren Raum. Sie ist Teil einer Abfolge von Ereignissen bei einem Cyberangriff auf die IT-Umgebung eines Unternehmens. Diese „Cyber-Angriffskette“ ist ein Modell, mit dem Forscher den Angriffsablauf verstehen, erklären und kommunizieren können.

Wenn Sicherheitsteams wissen, wie Angriffe erfolgen, können sie Technologien einsetzen, die Bedrohungen überall im IT-Ökosystem stoppen.

Schritte in der Cyber-Angriffskette

Auch wenn Cyberkriminelle nicht jedes Mal die gleichen Schritte befolgen, sind die grundlegenden Phasen eines Angriffs im Prinzip jedes Mal gleich:

- Während der **Initial-Kompromittierung** kann ein Anwender zum Klicken auf eine schädliche E-Mail oder einen Malware-Link verleitet bzw. dazu gebracht werden, seine Anmeldedaten weiterzugeben.
- Sobald die Angreifer einen Fuß in der Tür haben, können sie ihre **Berechtigungen erweitern** und sich lateral im Netzwerk bewegen.
- In der **Auswirkung-Phase** missbrauchen die Angreifer ihre Berechtigungen zum Beschädigen oder Zerstören von Daten, Verändern des Netzwerks und für weitere Aktivitäten.

Die effektivste Strategie ist daher die Investition in Technologien, die Cyberkriminelle in jeder Phase der Angriffskette stoppen.

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.

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.

In der Initial-Kompromittierungsphase eines Angriffs werden schädliche E-Mails versendet, die zu den meisten Ransomware-Infektionen führen. Aus diesem Grund benötigen Sie eine fortschrittliche Technologie, um diesen kritischen Vektor zu schützen.

Sie benötigen also eine E-Mail-Lösung, die auch eingebettete URLs und Anhänge analysiert und verhindert, dass schädliche Inhalte das System kompromittieren können. Cyberkriminelle 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. Sie nutzen auch fortschrittliches Machine Learning und verhaltensbasierte KI zum Identifizieren schwer erkennbarer Social-Engineering- und Phishing-E-Mails, die zu Malware-Infektionen führen. Zudem kann auf DMARC basierende E-Mail-Authentifizierung Angriffe mit Domain-Spoofing stoppen (bei denen die E-Mail-Domain Ihres Unternehmens imitiert wird, um das Vertrauen der Anwender zu gewinnen). Und schließlich sollte Ihre E-Mail-Sicherheitslösung auch vor anderen Arten der Identitätstäuschung wie Display Name-Spoofing und Doppelgänger-Domains schützen.

Schließen typischer Angriffspfade in Ihrer Identitätsinfrastruktur

Die Ransomware-Akteure benötigen einen Ansatzpunkt, und die schnellste Möglichkeit ist die Kompromittierung so vieler Endpunkte und Daten wie möglich. In einem typischen Unternehmen führt der Weg in ein Unternehmen über Active Directory oder ein unsicher verwaltetes privilegiertes Konto.

Eine Identitätsschutz-Lösung kann beispielsweise folgende Angriffspfade automatisch erkennen und blockieren:

- Im Cache gespeicherte Anmeldedaten
- Unzureichend geschützte lokale Administratorkonten
- Weitere Schwachstellen, nach denen Angriffstools in anderen kompromittierten Endpunkten suchen

Viele Unternehmen haben damit Schwierigkeiten, da sie mitunter über tausende Active Directory- oder Azure AD-Konten verfügen. Ein weiteres Hindernis ist die Vernetzung vieler Active Directory-Konten, die sich häufig sogar über mehrere, einander vertrauende Domains erstreckt.

Die Vorteile einer konsequenten Umsetzung der Identitätsschutzmaßnahmen sind den Aufwand jedoch wert. Wenn Sie die Möglichkeit haben, gefährdete Anwenderidentitäten zu identifizieren und abzusichern, können Sie laterale Bewegungen von Angreifern im Netzwerk stoppen und verhindern, dass diese auf sonst unzugängliche privilegierte Konten zugreifen können.

Ausführung von Code an bestimmten Orten verhindern

Richten Sie Software-Kontrollen ein, die die Ausführung von Code an 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.

Ihre Mitarbeiter als starke Verteidigungslinie

Die meisten Malware-Infektionen beginnen mit einem einzigen arglosen Mitarbeiter, der eine scheinbar arbeitsbezogene E-Mail öffnet. Die Angriffe nutzen die Ahnungslosigkeit der Anwender aus. In der Regel wird jemand dazu gebracht, schädliche Anhänge 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.

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 Feedback-System 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 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.

ABSCHNITT 3

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, Telefonanlagen und Netzwerke wieder hochfahren und sich um Lösegeld-forderungen kümmern.

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

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 die Netzwerkverbindung trennen und den infizierten Rechner zur IT-Abteilung bringen.

Damit Sie bei diesem Szenario nicht unvorbereitet sind, empfehlen wir die Trennung wertvoller Daten und Systeme voneinander, damit ein Sicherheitsproblem auf einem System keine anderen Systeme beeinträchtigt. Zum Beispiel sollten sich Ihre vertraulichen Forschungs- oder Unternehmensdaten nicht im gleichen Server und Netzwerksegment wie Ihre E-Mail-Umgebung befinden.

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.

Scareware ist eine Malware, die sich als Ransomware ausgibt, ohne deren Schadfunktionen zu besitzen. 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. Ermitteln Sie mithilfe von Bedrohungsdaten und – sofern erforderlich – externen Sicherheitsverantwortlichen oder forensischen Analysten den Umfang des Problems. 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.

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. Es wurden spezielle Abteilungen für die Unterstützung von Cybercrime-Opfern eingerichtet. Scheuen Sie sich also nicht, dort anzurufen. Die Spezialisten dort können Ihnen helfen und verfügen möglicherweise über Entschlüsselungsschlüssel oder Möglichkeiten zur Sicherstellung gezahlter Lösegelder.

Fragen Sie auch beim Anbieter Ihrer Cyberversicherung nach, ob Ransomware abgedeckt ist und welche Konditionen dabei gelten. Er kann Sie auch beim Koordinieren der Zwischenfallreaktion und -untersuchung unterstützen.

Wichtige Fragen während eines Angriffs

- 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.

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 aus Backups erfordert viel Zeit und Arbeit – und einige Unternehmen können sich den Ausfall möglicherweise nicht leisten.

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“).

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.

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.

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. 2021 hat sie dem US-Kongress jedoch empfohlen, von einem Zahlungsverbot abzusehen.[36] Gleichzeitig weist das FBI darauf hin, dass auch die Zahlung keine Garantie bietet, dass Sie Ihre Daten zurückerhalten. Schlimmer noch: Bei einer doppelten Erpressung könnten Sie gezwungen sein, ein zweites Mal zu zahlen. Dieser Fall ist nicht selten – 41 % der Opfer, die ein erstes Lösegeld gezahlt haben, gingen auch auf zusätzliche Lösegeldforderungen ein.[37]

36 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.
37 Proofpoint: „State of the Phish 2023“, Februar 2023.

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.

Seither haben Behörden striktere Maßnahmen eingeführt, mit denen Unternehmen von Lösegeldzahlungen abgehalten werden sollen. So empfahl die US-Börsenaufsichtsbehörde SEC (Securities and Exchange Commission) im Jahr 2022 eine neue Vorschrift, nach der gelistete Unternehmen Datenschutzverletzungen und Ransomware-Angriffe innerhalb eines bestimmten Zeitrahmens melden müssen.[38] Kurz danach unterzeichnete US-Präsident Joe Biden ein Gesetz, das die Betreiber kritischer Infrastrukturen dazu verpflichtet, Lösegeldzahlungen zu melden.[39] Zudem veröffentlichten die US-Transportsicherheitsbehörde TSA (Transportation Security Administration)[40] sowie die US-Bundeskommunikationskommission FCC (Federal Communications Commission)[41] kürzlich Vorschriften für Offenlegungspflichten. Die neuen Regeln läuten Maßnahmen ein, mit denen die unzureichende Meldung von Ransomware-Angriffen – eine derzeit allzu häufige Erscheinung – verhindert werden soll. Mit mehr Informationen über aktuelle Bedrohungen werden Unternehmen bessere Entscheidungen treffen können, um die Sicherheit ihrer Mitarbeiter, Systeme und Daten zu gewährleisten.

Gleichzeitig diskutieren die Vereinten Nationen ein internationales Abkommen, das die Cyberresilienz verbessern soll.[42] Außerdem hat Europol die Initiative „No More Ransom“ fortgesetzt, eine öffentlich-private Partnerschaft, die Opfern von Cyberangriffen hilft, ihre Dateien wiederherzustellen und zu entschlüsseln, ohne Lösegeld zahlen zu müssen. Mehr als 30 Länder arbeiten zusammen, um die Zahlungsnetzwerke stillzulegen, mit denen Cyberkriminelle Gelder waschen.[43] Zudem haben einige Länder vorgeschlagen, Ransomware-Zahlungen generell zu verbieten.

Einer der restriktivsten Vorschläge stammt aus Australien, wo die Regierung angekündigt hat, Lösegeldzahlungen unter Strafe zu stellen.[44]

Unternehmen müssen bei der Wahl der besten Vorgehensweise verschiedene Faktoren berücksichtigen, 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.

38 Paul Kiernan (Wall Street Journal): „SEC Proposes Requiring Firms to Report Cyberattacks Within Four Days“ (SEC möchte, dass Firmen Cyberangriffe innerhalb von 4 Tagen melden), März 2022.
39 David Uberti (Wall Street Journal): „Fearing More Cyberattacks, Congress Requires Key Businesses to Report Digital Breaches“ (Aus Sorge vor weiteren Cyberangriffen will der Kongress, dass wichtige Unternehmen digitale Kompromittierungen melden), März 2022.
40 US-Heimatschutzministerium: „DHS Announces New Cybersecurity Requirements for Surface Transportation Owners and Operators“ (US-Heimatschutzministerium gibt neue Cybersicherheitsanforderungen für Transportunternehmen bekannt), Dezember 2021.
41 US-Bundeskommunikationskommission: „Chair Rosenworcel Circulates New Data Breach Reporting Requirements“ (Chef der US-Bundeskommunikationskommission stellt neue Vorschriften für die Meldung von Datenschutzverletzungen vor), Januar 2022.
42 Vereinte Nationen: „A UN treaty on cybercrime is en route“ (Vereinte Nationen: Ein UN-Abkommen zu Cyberkriminelle ist unterwegs), April 2022.
43 Jonathan Greig (ZDNet): „More than 30 countries outline efforts to stop ransomware after White House virtual summit“ (Mehr als 30 Länder stellen nach virtueller Konferenz im Weißen Haus Maßnahmen zur Abwehr von Ransomware vor), Oktober 2021.
44 Reuters: „Australia to consider banning paying ransoms to cybercriminals“ (Australien will Lösegeldzahlungen an Cyberkriminelle verbieten), November 2022.

ABSCHNITT 4

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 durch einen 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 auch 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.

Identität und insbesondere Active Directory ist das nächste Einfallstor fast aller Ransomware-Angriffe. Wenn Ihr Team über die nötige Expertise verfügt, bieten Open Source-Tools Ihnen einen Überblick über die Angriffswege in Ihrer Umgebung. Falls Sie jedoch Veränderungen an AD vornehmen, um die identifizierten Angriffswege zu blockieren, lassen sich die Auswirkungen auf Ihre Geschäftsanwendungen oft nur schwer vorhersagen. Eine Identitätsschutzlösung kann fast alle diese Schwachstellen schließen und Erkennungsmöglichkeiten für diejenigen bereitstellen, die Sie – wegen der geschäftlichen Auswirkungen – nicht durch eine AD-Konfigurationsänderung blockieren können.

Eine große Hilfe ist auch ein proaktiver Ansatz. Für die Abwehr aktueller gezielter 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 Cyberkriminelle 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.

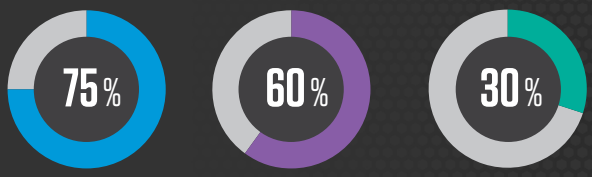
Zuverlässige Cybersicherheit muss personenzentriert sein. Sie umfasst Schulungen zur Sensibilisierung für Sicherheit auf Basis realer Angriffstechniken, damit Anwender widerstandsfähiger Anwender werden. Sie identifiziert und beseitigt Ransomware, die es auf Ihre Mitarbeiter abgesehen hat. Zudem dämmt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

Gründe für Proofpoint

Wir analysieren täglich mehr als:

2,6 Mrd. E-MAILS	**49 Mrd.** URLs	**1,9 Mrd.** ANHÄNGE
1,7 Mrd. MOBILGERÄTE-NACHRICHTEN	**430 Mio.** WEB-DOMAINS	**143.000** SOCIAL-MEDIA-KONTEN

Auf unsere Lösungen vertrauen mehr als:



8.000 GROSSUNTERNEHMEN

200.000 KLEINE UNTERNEHMEN

WEITERE INFORMATIONEN

Weitere Informationen zur Abwehr von Ransomware finden Sie unter **www.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 75 Prozent der Fortune-100-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.