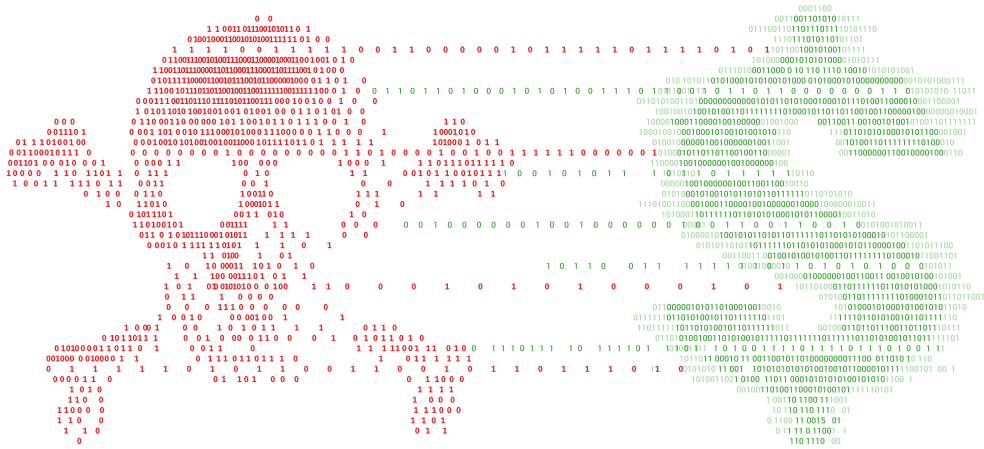
SOPHOS



Ransomware: Die Cyberbedrohung, die nicht tot zu kriegen ist

Auch dreißig Jahre nach dem weltweit ersten Ransomware-Angriff erpressen Cyberkriminelle weiterhin Unternehmen, verschlüsseln mutwillig Daten und fordern horrende Lösegelder für die sichere Rückgabe. Während die Schlagzeilen kommen und gehen, gewinnt Ransomware immer mehr an Fahrt, und sechs- und siebenstellige Lösegeldforderungen gehören mittlerweile zum Alltag.

In diesem Whitepaper untersuchen wir die Gründe für die Langlebigkeit von Ransomware und analysieren, warum diese Bedrohung im Laufe der Jahre immer schneller, intelligenter und gefährlicher werden konnte. Außerdem erläutern wir, was wir aus dieser Geschichte lernen müssen, wenn wir unser Angriffsrisiko in Zukunft erfolgreich senken wollen.

Außerdem gehen wir auf drei neue Bereiche ein, in denen Ransomware aufgrund technologischer und gesellschaftlicher Entwicklungen immer aktiver wird. Abschließend erklären wir, welche Technologien und Verhaltensweisen Unternehmen anwenden sollten, um sich bestmöglich vor Ransomware zu schützen, und zeigen, wie Sophos dabei helfen kann.

Sophos-Whitepaper Dezember 2019

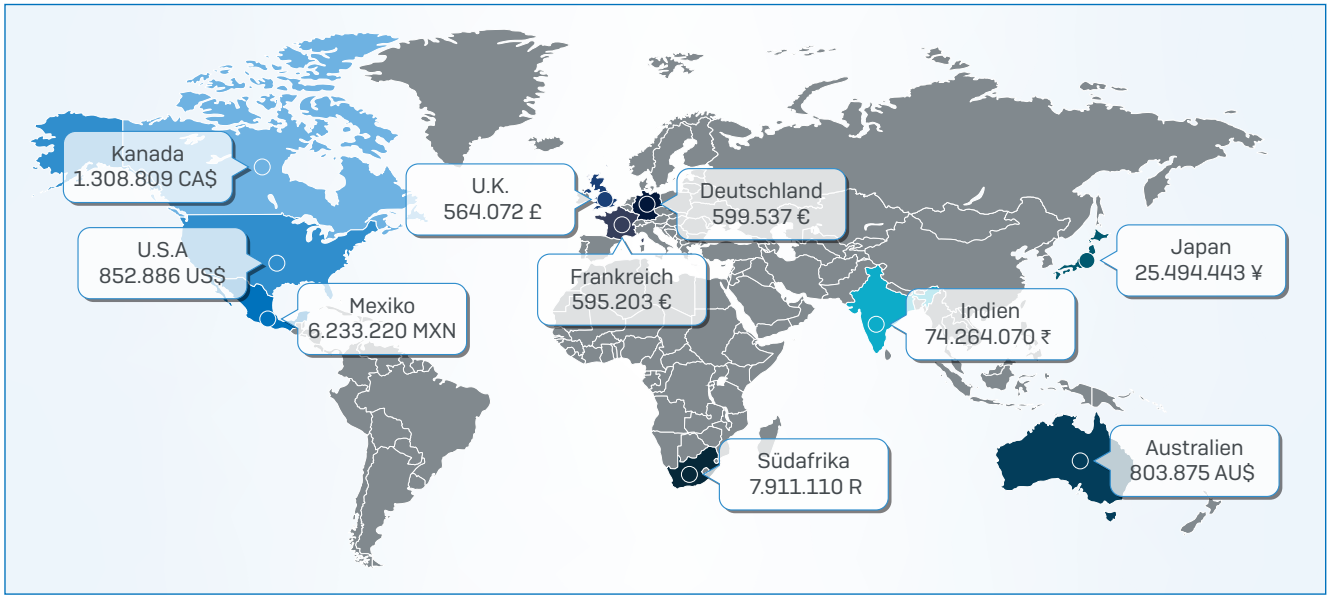
Inhaltsverzeichnis

Die Folgen von Ransomware

Ransomware ist für Unternehmen auf der ganzen Welt eine sehr reale Bedrohung. Eine von Sophos in Auftrag gegebene unabhängige Befragung von 3.100 IT-Managern in 12 Ländern ergab, dass 2018 21 % der Unternehmen von Ransomware betroffen waren. Zudem war bei drei von 10 Unternehmen, die Opfer eines Cyberangriffs wurden, Ransomware im Spiel.

Die finanziellen Folgen von Ransomware sind verheerend. Addiert man die kompletten Kosten für die Bereinigung, einschließlich Ausfallzeiten, zusätzlicher Arbeitsstunden, Gerätekosten, Netzwerkkosten, entgangener Verkaufschancen und gezahlter Lösegeldbeträge, kommen pro Opfer erhebliche Summen zusammen.

Kosten für die Bereinigung nach einem Ransomware-Angriff



Quelle: The State of Endpoint Security Today, Sophos, 2018

Angesichts der Omnipräsenz von Ransomware und der hohen Kosten eines Angriffs stellt sich die Frage: Warum ist Ransomware so hartnäckig? Warum ist es uns trotz aller technologischen Fortschritte bisher nicht gelungen, Ransomware ein für alle mal aus der Welt zu schaffen? Warum hat Ransomware nach wie vor so verheerende Folgen?

Um diese Fragen zu beantworten, müssen wir zunächst verstehen, wie wir zur heutigen Situation gelangt sind. Hierzu müssen wir in der Zeit zurückgehen und uns ansehen, wie und warum sich Ransomware im Laufe der Jahre weiterentwickelt hat.

Die Evolution von Ransomware

Die Entstehung von Ransomware

Ransomware ist nicht neu. Tatsächlich wurde der erste Cyber-Ransomware-Angriff im Dezember 1989 veröffentlicht. Dr. Joseph V. Popp verschickte 20.000 Disketten, die mit dem „AIDS Information"-Trojaner infiziert waren. Das Programm gab vor, ein Expertensystem zur Aufklärung über das HIV- und AIDS-Ansteckungsrisiko zu sein, nach 90-maliger Ausführung verschlüsselte es jedoch die Festplatte.

Viele von uns werden sich erinnern: 1989 schaltete noch jeder seinen Computer am Ende des Tages aus, sodass der 90. Neustart in der Regel vier bis fünf Monate nach dem ersten Ausführen des Programms stattfand. Dem Benutzer wurde dann eine Lösegeldforderung präsentiert, in der 189 US-Dollar für die einjährige Nutzung des Programms oder 378 US-Dollar für die lebenslange Nutzung verlangt wurden. Die Zahlung erfolgte per Scheck an ein Unternehmen in Panama.

Ransomware-Lösegeldforderung in „AIDS Information"-Trojaner

Bedauerlicherweise für Dr. Popp ließ sich die verwendete Chiffre leicht knacken und kostenlose Entschlüsselungstools waren bald verfügbar. Außerdem war die Idee, Zahlungen per Scheck nach Panama zu schicken, wenig praxistauglich. Infolgedessen konnte das Unternehmen keine Einnahmen generieren und der Urheber landete stattdessen vor Gericht.

Cyberkriminelle müssen drei wesentliche Hindernisse überwinden, um einen erfolgreichen Ransomware-Angriff durchzuführen: Sie müssen die Ransomware auf die Geräte der Opfer schleusen, die Dateien verschlüsseln/entschlüsseln und die Zahlung erhalten.

Dr. Popp hatte zwar einen effektiven, wenn auch nicht wirklich skalierbaren Ansatz gefunden, um seine Bedrohung auf die Geräte der Opfer zu schleusen (er musste diese 20.000 Disketten manuell beschreiben), sein Konzept versagte jedoch bei der Verschlüsselung und Zahlungsabwicklung.

☑ Installation der Ransomware

☒ Verschlüsseln und Entschlüsseln der Dateien

☒ Zahlungseingang

Ausnutzung neuer Entwicklungen

Der Angriff mit dem „AIDS Information"-Trojaner konnte jedoch einen Erfolg verbuchen: Er griff ein in der Gesellschaft allgegenwärtiges Thema auf, nämlich die damals weit verbreitete Besorgnis um HIV/AIDS. Seitdem greifen Cyberkriminelle immer wieder technologische und gesellschaftliche Entwicklungen auf, um ihre Ransomware-Angriffe weiterzuentwickeln und zu verbessern, u. a.:

- **Kostenlose E-Mail-Dienste wie AOL und Yahoo:** Diese Dienste ermöglichten Hackern erstmals, unbegrenzt nicht nachverfolgbare E-Mail-Adressen einzurichten, was zum Start umfangreicher Spam-Kampagnen führte, mit denen Ransomware in Umlauf gebracht wurde.
- **Die Umstellung von DFÜ- auf ADSL-Verbindungen:** Diese technologische Weiterentwicklung ermöglichte einem breiteren Personenkreis, das Internet über längere Zeiträume zu nutzen, und bot Angreifern damit eine größere Angriffsfläche.
- **Geo-Targeting:** Durch die Möglichkeit, den Standort von Benutzern zu ermitteln, konnten Cyberkriminelle ihre Angriffe auf ein bestimmtes Land/eine bestimmte Region zuschneiden. Geo-Targeting erhöhte die Erfolgsraten, da Angreifer lokale Themen bei E-Mail-Angriffen ausnutzen und gleichzeitig die Sprache auf ihre Zielgruppe anpassen konnten.
- **Prepaid-Kreditkarten:** Mit diesen Karten konnten Cyberkriminelle Lösegeldzahlungen anonym entgegennehmen.
- **Kryptowährungen**: Insbesondere Bitcoin entwickelte sich für Kriminelle zu einer weiteren zuverlässigen und offen zugänglichen Zahlungsmethode.

Durch die erfolgreiche Ausnutzung dieser (und weiterer) Entwicklungen war es Cyberkriminellen bis zum Jahr 2010 gelungen, die drei wichtigsten Hürden von Ransomware zu überwinden und diese Bedrohung damit zu einem tragfähigen Geschäftsmodell zu machen.

☑ Installation der Ransomware

☒ Verschlüsseln und Entschlüsseln der Dateien

☒ Zahlungseingang

Katz-und-Maus-Spiel

Seit Ransomware sich zum Mainstream entwickelt hatte, konzentrierten sich die Cyberkriminellen auf die Weiterentwicklung und Verbesserung ihrer Angriffe, um ihre Umsätze maximal zu steigern. Dazu nutzten sie folgende Hilfsmittel:

- **Branding**: Versierte Cyberkriminelle erkannten, dass Betroffene nur dann zahlen würden, wenn die Wahrscheinlichkeit einer Datenwiederherstellung groß genug war. Daher wurde ein zuverlässiges Ransomware-Entschlüsselungstool für die kontinuierliche Umsatzgenerierung unerlässlich. Nicht alle Entschlüsselungstools funktionierten jedoch gleich gut. Ransomware-Angreifer mit einem effektiven Tool wollten nicht mit weniger effektiven Tools in Verbindung gebracht werden. Sie bedienten sich daher einer Marketing-Technik, die in der kommerziellen Welt seit Jahrzehnten gängige Praxis ist: Branding. Eine schnelle Internet-Suche nach einem Ransomware-Namen informiert das Opfer über die Wahrscheinlichkeit, beim Begleichen des Lösegelds seine Daten zurück zu erhalten.
- **Ransomware-as-a-Service:** Ransomware-Experten nutzten die Geschäftschance, anderen Cyberkriminellen, die zwar nicht über die erforderlichen Verschlüsselungskenntnisse oder Zahlungssysteme verfügten, sehr wohl jedoch über die kriminelle Energie zur Verbreitung von Bedrohungen, sogenannte Ransomware-„Pakete" zu verkaufen. Im Gegenzug zu einer Gewinnbeteiligung von 30 % umfasste der Service die Malware und Backend-Zahlung über eine zentrale Website.

- **Ransomware mit hohem Wirkpotenzial**: Diese Form der Ransomware versetzte Angreifer in die Lage, ihren Return on Investment (ROI) zu erhöhen, indem sie gezielt eine kleine Anzahl von Opfern mit besonders verheerenden Angriffen attackierten. Gezielte Angriffe waren weniger aufwendig und erregten weniger Aufsehen. Zudem richteten diese Angriffe mehr Schaden an, sodass die Opfer mit höherer Wahrscheinlichkeit bereit waren, den Lösegeldforderungen nachzukommen.

Gleichzeitig arbeitete die Cybersecurity-Branche mit Hochdruck daran, ihre Abwehr-Technologien weiterzuentwickeln und herauszufinden, wie man Ransomware-Angriffe erkennen und blockieren kann, um den Cyberkriminellen einen Schritt voraus zu bleiben.

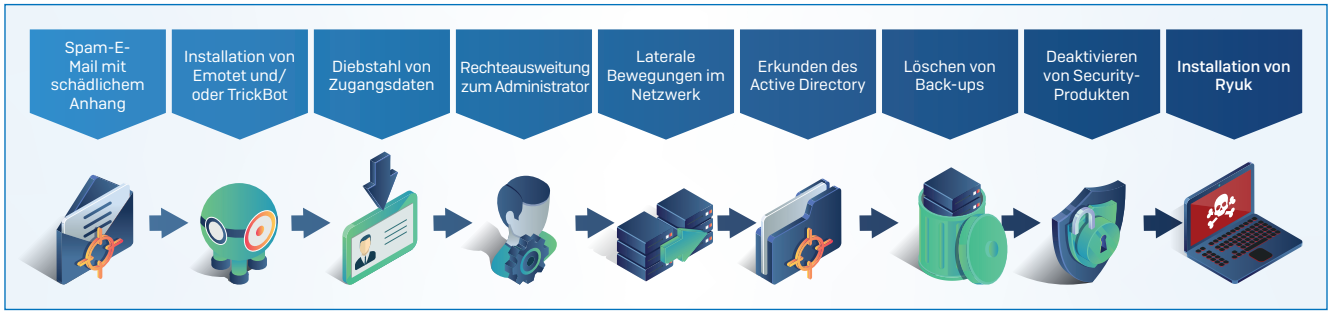
Ransomware entwickelt sich weiter: Ryuk

Ryuk ist nach einer Figur in der Manga-Serie Death Note benannt und wohl die derzeit am weitesten entwickelte Form von Ransomware. Die Akteure hinter Ryuk richten sich in der Regel an Unternehmen, die keine Ausfallzeiten verkraften können, z. B. Zeitungen, Kommunen und Versorgungsunternehmen. So steigen die Chancen, Lösegeldzahlungen einzustreichen, und es können Summen im sechs- und siebenstelligen Bereich gefordert werden.

Um Anti-Ransomware-Technologien zu überlisten, kombinieren diese Angreifer modernste Angriffstechniken mit interaktivem Hacking. Ryuk-Angriffe beginnen oft mit einer Spam-E-Mail, die einen schädlichen Anhang enthält. Der Anhang löst einen Emotet- oder TrickBot-Angriff aus, über den sich die Cyberkriminellen Zugriff auf das Netzwerk des Opfers verschaffen.

Im Netzwerk stehlen die Hacker dann Zugangsdaten und weiten ihre Rechte bis zum Administrator aus. Mit ihren Administrator-Rechten bewegen sich die Hacker anschließend lateral im Netzwerk und wenden mehrere Techniken an, darunter Remote Desktop Protocol (RDP), Durchsuchen von Active Directory und Löschen aller Back-ups.Da sie nun das komplette Sicherheitsnetz des Opfers ausgeschaltet haben, versuchen die Angreifer anschließend, Cybersecurity-Produkte zu deaktivieren, bevor sie schließlich die Ryuk-Ransomware installieren, Dateien verschlüsseln und hohe Lösegeldforderungen stellen.

Typische Angriffskette von Ryuk-Ransomware



Was erwartet uns in Sachen Ransomware als Nächstes?

Die große Lektion, die wir aus dem Blick auf die Geschichte der Ransomware lernen können: **Cyberkriminelle werden auch weiterhin technologische und gesellschaftliche Veränderungen ausnutzen, um ihre Ransomware-Angriffe in Umlauf zu bringen**. Ransomware wird sich auch in Zukunft weiterentwickeln. In diesem Zusammenhang möchten wir auf drei Bereiche eingehen, in denen Ransomware aufgrund technologischer Fortschritte immer präsenter wird.

Public Cloud Ransomware

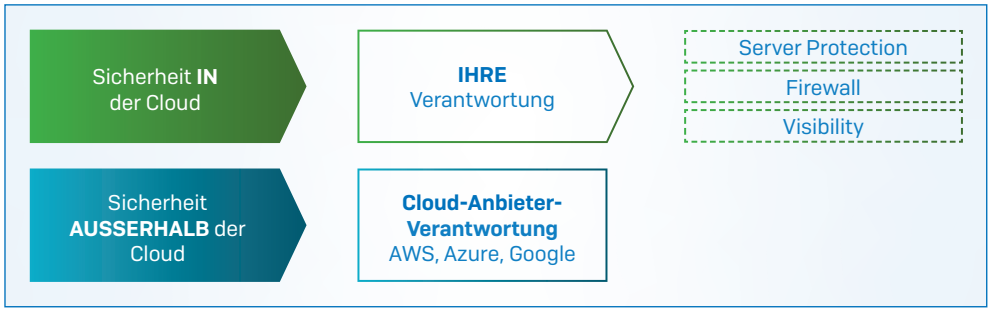
Ganz oben auf der Liste steht Public Cloud Ransomware. Damit meinen wir Ransomware, die Daten ins Visier nimmt und verschlüsselt, die in öffentlichen Cloud-Diensten wie Amazon Web Services (AWS), Microsoft Azure (Azure) und Google Cloud Platform (GCP) gespeichert sind. Die Public Cloud wird immer beliebter und Unternehmen nutzen sie auf unterschiedliche Weise.

Für viele ist die Public Cloud einfach ein **Ersatz für die physischen Server vor Ort**, auf denen in der Vergangenheit Daten gespeichert wurden. Während Mitarbeiter Dateien früher auf dem Server im Büro speicherten, speichern sie sie jetzt auf Servern in der Cloud. Besonders beliebt ist die Public Cloud auch zum **Ausführen von Web-Anwendungen**, z. B. zur Bereitstellung einer Website oder webbasierter Services. Der dritte Hauptanwendungsfall für die Public Cloud ist die **Software-Entwicklung**. Software-Entwickler schreiben zunehmend Code auf Public-Cloud-Servern, da die Einrichtung eines Servers in der Cloud schneller und einfacher ist als die Erstellung physischer Umgebungen.

Die Public Cloud bietet viele Vorteile. Was die Sicherheit angeht, gibt es jedoch eine Menge offener Fragen und Verwirrung in Bezug auf die Verantwortlichkeiten. Viele wissen nicht, welche Sicherheitsverantwortung bei den Public-Cloud-Anbietern und welche beim Kunden liegt. Diese Unsicherheit führt zu Sicherheitslücken, die sich wiederum als gefundenes Fressen für Ransomware-Angreifer erweisen, da viele wertvolle Daten offen zugänglich sind und demzufolge einfach verschlüsselt werden können.

Die Public Cloud bietet Angreifern noch viele weitere Anreize. Da immer mehr und immer wertvollere Daten in der Cloud gespeichert werden, bietet sich Cyberkriminellen eine stetig wachsende Angriffsfläche. Zudem erleichtern eine schwache Konfiguration und ein öffentlicher Zugriff auf Cloud-Ressourcen (Storage Buckets, Datenbanken, Benutzerkonten usw.) Kriminellen den Zugriff auf offene Datenbanken.

Um sich vor Ransomware in der Public Cloud schützen zu können, müssen Sie zunächst das Shared-Responsibility-Modell der Public Cloud verstehen. Kurz gesagt: Sie sind verantwortlich für die Sicherheit aller Inhalte, die Sie in die Cloud verlagern (einschließlich aller Ihrer Daten), sowie für die Sicherheit des Zugriffs auf die Public Cloud. Für die Sicherheit der Cloud selbst sind jedoch die Public-Cloud-Anbieter verantwortlich. Dazu gehört auch die Sicherheit der physischen Einrichtung, in der sich die Rechenzentren befinden.



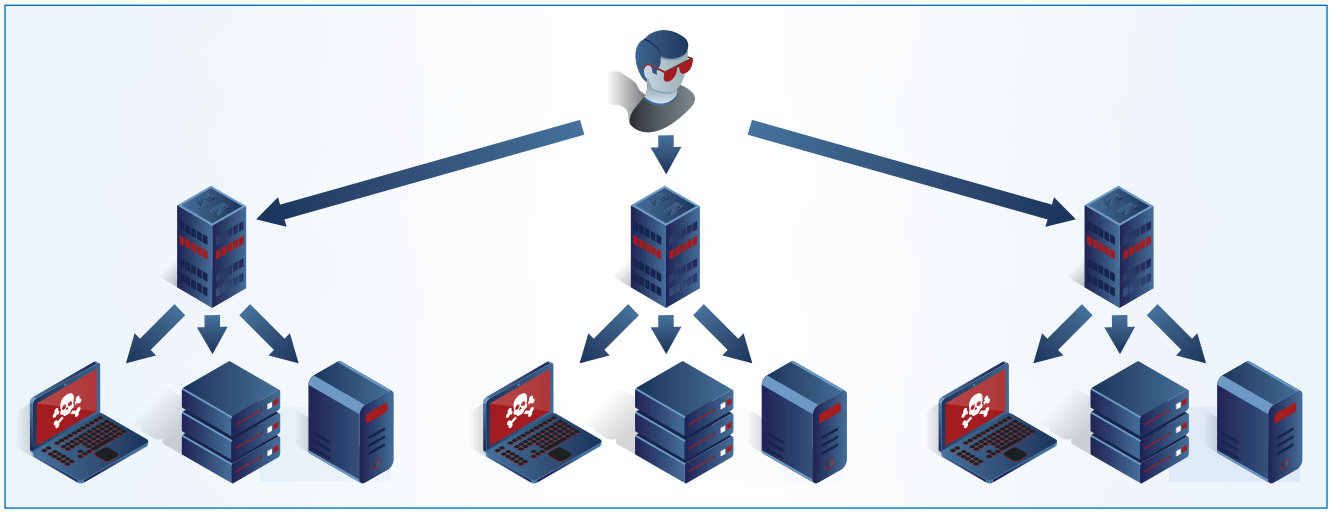
Sie sollten auf Ihre cloudbasierten Daten dieselben grundlegenden Prinzipien anwenden wie auf Ihre lokalen Daten. Genau wie Sie vor Ort Server-Schutz und eine Firewall nutzen, sollten Sie dies auch bei Daten in der Public Cloud tun. Außerdem müssen Sie wissen, was sich in der Public Cloud befindet, damit Sie für die Sicherheit dieser Inhalte sorgen können.

Angriffe auf Service-Provider

Der zweite Bereich, in dem wir einen Anstieg von Ransomware erwarten, sind Angriffe auf Service-Provider. Da Technologien und Bedrohungen immer komplexer werden, lagern Unternehmen ihre IT zunehmend an spezialisierte Managed Service Provider (MSPs) aus. Diese MSPs verwalten alle IT-Aspekte für ihre Kunden, von Druckern bis hin zu Sicherheitslösungen. Dazu müssen sie direkten Zugang zu den Netzwerken ihrer Kunden haben.

In der Vergangenheit haben sich Ransomware-Akteure meist auf ein Unternehmen pro Angriff konzentriert: ein Opfer, eine Lösegeldzahlung. Cyberkriminelle sind jedoch immer bestrebt, ihren Return on Investment zu maximieren, und haben erkannt, dass sie mit einem Angriff gleich mehrere Unternehmen erpressen können, wenn sie MSPs ins Visier nehmen: ein Angriff, viele Lösegeldzahlungen.

Angriffsmodell bei Service-Providern



Die Lösung für dieses Problem heißt nicht, Ihre IT-Sicherheit intern zu verwalten. MSPs, die sich auf IT-Sicherheit spezialisiert haben, bieten ein sehr hohes Maß an Know-how, das für viele Unternehmen schwer zu replizieren ist. Machen Sie stattdessen **Sicherheit zu einem zentralen Auswahlkriterium**, wenn Sie sich für einen MSP entscheiden. Fragen Sie den MSP, welche Sicherheitsprodukte und -praktiken dieser in seinem eigenen Unternehmen einsetzt. Ein guter MSP wird Ihre Fragen gerne beantworten.

Überlegen Sie sich außerdem, **wo Ihre Prioritäten liegen**. Hat der Schutz für Sie höchste Priorität? Kosten sind für praktisch jedes Unternehmen ein relevanter Faktor. Sie sollten jedoch keine Kompromisse beim langfristigen Schutz eingehen, nur um kurzfristig Kosten zu sparen. Wie wir zu Beginn gesehen haben, überwiegen die Kosten für die Bereinigung eines Ransomware-Angriffs viele andere Ausgaben.

Verschlüsselungsfreie Angriffe

Ransomware umfasst nun das volle Spektrum. Die Fähigkeit, Dateien zu verschlüsseln, war eine der wichtigsten Funktionen, die benötigt wurde, um Ransomware zu einer praktikablen Cyberbedrohung zu machen. Mittlerweile müssen Cyberkriminelle Dateien jedoch nicht mehr verschlüsseln, um Lösegeld zu erpressen. Warum? Weil viele auch bereit sind zu zahlen, um eine Veröffentlichung ihrer Daten zu verhindern.

Zwei Arten von Daten stehen bei dieser Angriffsart in besonderem Fokus: personenbezogene Daten, also Informationen über eine Person, manchmal auch „persönliche Daten" genannt. In den letzten Jahren haben sich die Rechtsvorschriften zum Schutz personenbezogener Daten erheblich verschärft, und es wurden nationale, regionale und branchenspezifische Gesetze zum Schutz von Daten erlassen (z. B. DSGVO).

Verstöße gegen diese Gesetze und Vorschriften werden mit empfindlichen Geldstrafen geahndet – die DSGVO sieht maximale Strafzahlungen in Höhe von bis zu 4 % des jährlichen globalen Umsatzes oder 20 Mio. € vor, je nachdem, welcher Betrag höher ist. Cyberkriminelle erpressen Unternehmen und andere Organisationen immer häufiger mit der Drohung, personenbezogene Daten zu veröffentlichen, da diese in diesem Fall hohe Strafen zahlen müssen.

Im Oktober 2019 erlitt die Stadt Johannesburg in Südafrika einen verschlüsselungsfreien Ransomware-Angriff. Hinter diesem steckte eine Gruppe, die sich die „Shadow Kill Hacker" nannte. Einer Notiz auf Twitter zufolge wurden in diesem Fall keine Daten verschlüsselt. Stattdessen stahlen die Angreifer Daten und drohten, diese ins Internet hochzuladen, wenn die Stadt nicht zahlte. Ihre Nachricht lautete:

> *Alle Ihre Server und Daten wurden gehackt. Wir haben Dutzende von Hintertüren in Ihrer Stadt. Wir haben die Kontrolle über alles in Ihrer Stadt. Außerdem haben wir alle Passwörter und vertraulichen Daten wie Finanzdaten und persönliche Bevölkerungsdaten kompromittiert.*

Angeblich forderte die Gruppe ein Lösegeld in Höhe von vier Bitcoins (30.347 £), das allerdings bis zum heutigen Tag nicht beglichen worden zu sein scheint.

Ein weiterer Datentyp, der besonders durch diese Angriffe gefährdet ist, ist geistiges Eigentum. Der Erfolg vieler Unternehmen gründet auf geistigem Eigentum – sei es ein geheimes Rezept, eine proprietäre Technologie oder einzigartige Daten. Wenn diese Daten in die Öffentlichkeit gelangen, könnte dies das Aus für ein Unternehmen bedeuten.

Das öffentlichkeits-wirksamste Beispiel für diese Art von Ransomware war der Angriff auf die Band Radiohead Mitte 2019. Das Archiv von Frontmann Thom Yorkes wurde gehackt, und die Angreifer stahlen 18 Stunden ungehörte Musik aus der Zeit der Veröffentlichung des Albums OK Computer im Jahr 1997. Der Erpresser drohte damit, die Musik zu veröffentlichen, und forderte ein Lösegeld von 150.000 US-Dollar – eine Bitte, der Radiohead nicht nachkam und stattdessen die Musik selbst veröffentlichte – im Gegenzug zu einer Spende von 18 GBP (rund 20 Euro) zur Unterstützung der Klimagruppe Extinction Rebellion.

Um verschlüsselungsfreie Angriffe zu stoppen, müssen Sie verhindern, dass Hacker an Ihre Daten gelangen. Hierzu sind viele derselben Technologien und Verhaltensweisen erforderlich, die auch zur Verschlüsselung bei Ransomware zum Einsatz kommen – eine gute Überleitung zu unserem nächsten Abschnitt.

Wie Sie sich gegen Ransomware verteidigen

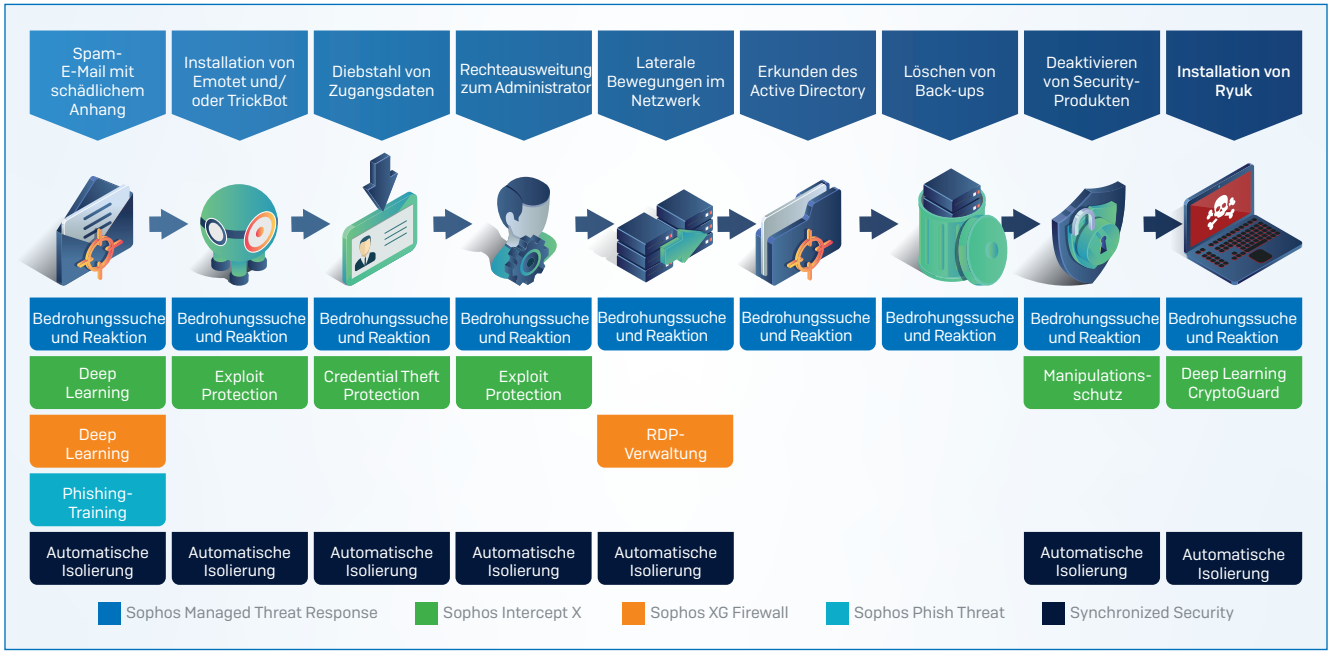
Ransomware hat sich zu einer hochentwickelten, hochkomplexen Bedrohung entwickelt – und diese Entwicklung wird weiter fortschreiten. Wie können Sie also das Risiko minimieren, von Ransomware heimgesucht zu werden? Sie müssen es Ransomware-Angreifern so schwer wie möglich machen, ihre komplexen Angriffe auszuführen und technologische und gesellschaftliche Entwicklungen aufzugreifen. Unsere Empfehlungen:

- Einsatz führender Cybersecurity-Technologie mit Fokus auf die Ausschaltung der gesamten Angriffskette, statt nur einzelner Malware-Elemente
- Durchgängige Anwendung von Security Best Practices
- Aufklärung Ihrer Mitarbeiter in regelmäßigen Security-Awareness-Trainings über die Risiken und erforderlichen Verhaltensweisen

Bedrohungsschutz, der die gesamte Angriffskette ausschaltet

Der beste Schutz erfordert die besten Schutzmaßnahmen, sowohl für lokal als auch in der Public Cloud gespeicherte Daten.

Am Beispiel Ryuk können wir sehen, wie verschiedene Technologien in unterschiedlichen Phasen der Angriffskette funktionieren.



Sophos Intercept X
Sophos Intercept X verfügt über modernste Schutztechnologien, die Ransomware auf Ihren Endpoints und Servern in mehreren Phasen der Angriffskette stoppen.

- KI-basierter Bedrohungsschutz erkennt Bedrohungen in schädlichen E-Mails.
- Exploit-Schutz erkennt und blockiert mehr als zwei Dutzend Exploit-Techniken, einschließlich derer, die verwendet werden, um Ransomware zu verbreiten und zu installieren und Berechtigungen auszuweiten.
- Indem Sie den Diebstahl von Zugangsdaten unterbinden, verhindern Sie auch, dass Hacker an wertvolle Anmeldeinformationen gelangen, unbefugt auf Systeme zugreifen oder Administratorrechte erlangen können.
- Manipulationsschutz verhindert, dass die Ransomware Ihren Endpoint-Schutz deaktiviert.
- Deep Learning analysiert die „DNA" der Datei, um festzustellen, ob es sich um Ransomware handelt. Sollte dies der Fall sein, wird die Ransomware von der Ausführung gestoppt.
- Die Verhaltenserkennung von CryptoGuard blockiert unbefugte Dateiverschlüsselungen und setzt betroffene Dateien innerhalb von Sekunden in ihren sicheren Ursprungszustand zurück.

Sophos XG Firewall
Die Sophos XG Firewall bietet ein leistungsstarkes Schutzpaket, mit dem Ransomware-Angriffe erkannt und blockiert und Hacker gestoppt werden, die sich lateral im Netzwerk fortbewegen, um Berechtigungen auszuweiten.

- KI-basierter Bedrohungsschutz, einschließlich Sandboxing, erkennt Ransomware am Gateway.
- Mit RDP-Verwaltungstools können Sie Ihr RDP einfach und komfortabel verwalten und verhindern, dass Hacker RDP zur lateralen Bewegung in Ihrem Netzwerk verwenden.
- IPS kann alle Versuche erkennen, Netzwerkschwachstellen auszunutzen – u. a. in RDP und jedem anderen Teil des Netzwerk-Stacks.

Synchronized Security
Intercept X und die XG Firewall arbeiten gut eigenständig, jedoch dank Synchronized Security noch besser zusammen. Wenn in einem der Produkte eine Erkennung ausgelöst wird, arbeiten die XG Firewall und Intercept X zusammen, um die betroffenen Geräte automatisch zu isolieren und so eine weitere Ausbreitung der Bedrohung zu verhindern.

Managed Threat Response (MTR)
Sophos Managed Threat Response (MTR) – viele Unternehmen verfügen weder über das Know-how noch die Ressourcen oder den Wunsch, ihr Netzwerk 24/7 zu überwachen. Der Sophos MTR-Service ist ein Team von Bedrohungsexperten, die ständig nach verdächtigen Aktivitäten suchen und auf diese reagieren.

Starke Sicherheitspraktiken

Neben leistungsstarken Technologien zur Abwehr von Angriffen gibt es auch eine Reihe von Best Practices, die Sie anwenden sollten, um Ihre Verteidigungsmaßnahmen zu verbessern:

- Verwenden Sie eine mehrstufige Authentifizierung (2FA).
- Nutzen Sie komplexe Passwörter und verwalten Sie diese über einen Passwort-Manager.
- Beschränken Sie die Zugriffsrechte; gewähren Sie Benutzerkonten und Administratoren nur wirklich erforderliche Zugriffsrechte.
- Fertigen Sie regelmäßig Back-ups an und verwahren Sie diese extern und offline, wo Angreifer sie nicht finden können – sie könnten Ihr letzter Rettungsanker gegen eine sechsstellige Lösegeldforderung sein.
- Installieren Sie Patches rechtzeitig und regelmäßig: Ransomware wie WannaCry und NotPetya konnten sich durch ungepatchte Schwachstellen weltweit ausbreiten.
- Deaktivieren Sie RDP: Schalten Sie das Remote Desktop Protocol (RDP) aus, wenn Sie es nicht brauchen, und verwenden Sie ansonsten eine Durchsatzbegrenzung, 2FA oder ein VPN.
- Stellen Sie sicher, dass der Manipulationsschutz aktiviert ist – Ryuk und andere Ransomware-Stämme versuchen, den Endpoint-Schutz zu deaktivieren, und Manipulationsschutz ist darauf ausgelegt, dies zu verhindern.

Kontinuierliche Schulung der Mitarbeiter

Menschen sind immer das schwächste Glied in der Cybersecurity, und Cyberkriminelle sind Experten, wenn es darum geht, das normale menschliche Verhalten zu ihrer persönlichen Bereicherung auszunutzen. Die meisten Ryuk-Angriffe werden über eine E-Mail mit einem schädlichen Anhang übertragen. Wenn Sie verhindern, dass Ihre Mitarbeiter auf solche Anhänge klicken, kann Ransomware gar nicht erst ins Netzwerk gelangen. Wir empfehlen Ihnen daher, kontinuierlich in die Mitarbeiterschulung zu investieren. Sophos Phish Threat bietet Ihnen flexible, individuell anpassbare Vorlagen und Trainings, mit denen Sie ganz einfach eine positive Security-Awareness-Kultur in Ihrem Unternehmen fördern können.

Weitere Informationen unter: www.sophos.de/phish-threat

Fazit

Ransomware ist eine Cyberbedrohung, die einfach nicht tot zu kriegen ist. Warum? Weil Kriminelle immer wieder neue technologische und gesellschaftliche Entwicklungen aufgreifen, um ihre Ransomware-Angriffe weiterzuentwickeln und zu verbessern. Wenn wir eine Lektion aus unserer 30-jährigen Geschichte der Ransomware-Bekämpfung lernen können, dann ist es, dass Ransomware sich auch in Zukunft weiterentwickeln wird.

Das beste Rezept gegen Ransomware ist eine Kombination aus mehrstufigem Schutz an Endpoint und Gateway, der die

gesamte Angriffskette ausschaltet, eine sorgfältige und durchgängige Anwendung von Security Best Practices und eine kontinuierliche Sensibilisierung der Benutzer.

☑ Bedrohungsschutz, der die gesamte Angriffskette ausschaltet

☑ Starke Sicherheitspraktiken

☑ Kontinuierliche Schulung der Mitarbeiter

Weitere Informationen

Eine detaillierte Aufschlüsselung der Verhaltensmuster der zehn häufigsten, schädlichsten und hartnäckigsten Ransomware-Familien finden Sie in dem technischen Paper How Ransomware Attacks von Mark Loman, Sophos Director of Engineering.

Weitere Informationen über Sophos-Lösungen zum Schutz vor Ransomware finden Sie unter:

- Sophos Intercept X
- Sophos XG Firewall
- Sophos Managed Threat Response
- Sophos Phish Threat

Um über die neuesten Ransomware-Nachrichten auf dem Laufenden zu bleiben, folgen Sie unserem Security News Service **Naked Security**.

- Täglicher E-Mail-Newsletter: Melden Sie sich an unter nakedsecurity.sophos.com
- Wöchentlicher Podcast. Finden Sie uns überall da, wo Sie Ihre Podcasts abrufen
- Regelmäßige Beiträge in sozialen Netzwerken: Folgen Sie uns auf Twitter, Facebook, Instagram und YouTube

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

19-12-05 WP-DE (DD)

SOPHOS