LogRhythm®
The Security Intelligence Company

Ransomware der nächsten Generation

Eine Bedrohung, die sich unaufhörlich weiterentwickelt

Lange Zeit relativ unbeachtet, hat sich Ransomware in den letzten Jahren zu einem der größten IT-Sicherheitsrisiken entwickelt, mit denen Unternehmen heute konfrontiert sind.

Ransomware ist keine neuartige Bedrohung: Sie existiert in unterschiedlichen Formen schon seit mehr als einem Jahrzehnt. Jüngst hat sie jedoch massiv an Bedeutung gewonnen – durch eine wachsende Zahl kursierender Varianten, denen auch eine Reihe bekannter Unternehmen zum Opfer gefallen sind. Insbesondere in der ersten Jahreshälfte 2017 erhöhten die WannaCry- und Petya/NotPetya-Ausbrüche das Bewusstsein für Ransomware, da sie Schäden an den Firmensystemen verursachten, von denen sich manche Unternehmen und Behörden monatelang nicht erholten.

Die Verluste aufgrund von Ransomware beliefen sich 2016 auf schätzungsweise 1 Mrd. US-Dollar[1]

Mittlerweile sind sich die Unternehmen über die Bedrohung durch Ransomware im Klaren und wissen, dass sie ihre Systeme vor E-Mails und kompromittierten Websites schützen müssen, in denen sich Schadprogramme verbergen, die Systeme sperren und die Dateien verschlüsseln können.

Wenngleich die Zahl der Ransomware-Arten in den letzten Jahren laufend gestiegen ist, gelangen die meisten Varianten weiterhin an ihr Ziel, indem sie ungepatchte Systeme ausnutzen. Die Wiederherstellung nach einem erfolgreichen Ransomware-Angriff ist schwierig, doch können IT-Abteilungen Ransomware relativ leicht vorbeugend abwehren, indem sie gute Software-Hygiene betreiben und die Mitarbeiter aufklären. Dass Unternehmen inzwischen besser mit Ransomware umzugehen wissen, heißt allerdings noch lange nicht, dass sie sie weniger ernst nehmen dürfen. Sobald Unternehmen mit den üblichen Angriffen von Cyberkriminellen vertraut werden, entwickeln diese ihre Taktiken weiter, um ihren anvisierten Opfern eine Nasenlänge voraus zu bleiben.

Tatsächlich bedienen sich Ransomware-Gruppen mittlerweile einer Reihe neuer Strategien, um Unternehmen kalt zu erwischen.

Wie sich Ransomware verändert

Gezielte Ransomware-Angriffe:
Ransomware-Gangs gehen bei der Verbreitung ihrer Produkte immer raffinierter vor und suchen sich diejenigen Unternehmen aus, bei denen am meisten zu holen ist, wie zum Beispiel Finanzinstitute. In der Vergangenheit arbeiteten Ransomware-Gruppen mit „Fire and forget"-Methoden, um möglichst viele Benutzer zu überlisten und so an ihr Geld zu kommen. Heute suchen sie dagegen nach Unternehmen, die es sich schlicht nicht leisten können, dass kritische Dateien auf unbestimmte Zeit nicht zugänglich sind – in der Hoffnung, von diesen höhere Lösegelder erpressen zu können.

Mobile Ransomware:
Bei den meisten Cybercrime-Trends verbreitet sich das, was auf dem Desktop beginnt, irgendwann auch auf das Smartphone und Tablet. Mobile Ransomware funktioniert auf andere Weise als ihr Desktop-Gegenstück, doch das Ziel bleibt das gleiche – die Benutzer sollen nicht mehr auf ihre Dateien zugreifen können. Mobile Ransomware spielt derzeit noch eine vergleichsweise geringe Rolle, doch tauchen vermehrt Varianten auf, die es auf mobile Plattformen abgesehen haben.

17 Prozent der Unternehmen sind Opfer von Ransomware geworden[2]

Zombie-Ransomware:
Ransomware-Arten, die als ausgestorben galten, werden wiederbelebt und mit neuen Angriffsmethoden ausgestattet. Um mit minimalem Aufwand mehr Opfer in die Falle zu locken, verwenden Ransomware-Gruppen ihre bestehenden Malware-Varianten erneut und rüsten sie mit anderen Verschlüsselungsmethoden oder bösartigen Erweiterungen auf, damit sie sich effektiver verbreiten und Dateien ohne Lösegeldzahlung nicht entschlüsselt werden können.

Demokratisierung von Ransomware:
Früher war Ransomware eine Domäne erfahrener Praktiker, doch heute kann jeder sie verbreiten, ungeachtet seiner technischen Fähigkeiten. Menschen mit kriminellen Absichten können in Ransomware-as-a-Service investieren und sich den Zugriff auf ein bestehendes Ransomware-Setup erkaufen, das sie dann wunschgerecht anpassen können. Kommerzielle Ransomware-as-a-Service-Anbieter im Dark Web offerieren ähnliche Dienstleistungen wie legitime Online-Anbieter, zum Beispiel Live-Kundensupport. Im Gegenzug erhalten sie Anteil an den Profiten, die ihre Kunden erzielen.

Anatomie einer Ransomware-Attacke

Ransomware gelangt meist dadurch in Unternehmensnetze, dass Benutzer bösartige E-Mail-Anhänge öffnen oder befallene Websites besuchen, die auch als Wasserstellen bezeichnet werden. In letzter Zeit wurden jedoch auch einige Ransomware-Varianten entwickelt, die sich lateral in Netzwerken ausbreiten.

Die Malware wird versuchen, eine vorhandene Antivirus-Software zu umgehen. Wenn sie sich erfolgreich installieren konnte, wird sie damit beginnen, die Dateien eines Benutzers zu verschlüsseln, sodass er keinen Zugriff mehr darauf hat.

Dann wird die Ransomware ein Lösegeld für die Freigabe der Dateien fordern, meist in Höhe von einigen hundert Dollar. Wenn sich das Opfer zur Zahlung entschließt, muss es das Lösegeld in einer Kryptowährung, zum Beispiel Bitcoin, an den Ransomware-Autor überweisen. Sobald die Zahlung eingegangen ist, erhält der Benutzer einen kryptographischen Schlüssel, um die Dateien zu entschlüsseln und wieder Systemzugriff zu erhalten. Allerdings gibt es auch manchmal Fälle, in denen die Dateien trotz Zahlung nicht freigegeben werden.

LogRhythm
The Security Intelligence Company

Bedrohung durch Wiper:
NotPetya ähnelte zwar in vieler Hinsicht einer herkömmlichen Ransomware, war aber eigentlich ein Schädling, der letztlich wohl noch wesentlich gefährlicher ist: ein Wiper, also ein Schadprogramm, das Daten zerstört.

Ransomware hat seit jeher Profit zum Ziel, doch einige Malware-Autoren richten genauso gern Chaos an, wie sie Geld verdienen. Wenngleich NotPetya tatsächlich eine Ransomware-Komponente besaß, wird vermutet, dass die Akteure politische Motive hatten und hauptsächlich darauf aus waren, wirtschaftliche Schäden anzurichten, indem sie wichtige Systeme betriebsunfähig machten – womit die Unternehmen im Kreuzfeuer standen.

Ransomware ist und bleibt für alle Unternehmen ein Problem, auch wenn sich die Sicherheitsteams mit der Bedrohung inzwischen besser auskennen. Angesichts der Entwicklung neuer Varianten, Technologien und Social-Engineering-Methoden dürfen sich Unternehmen nie in falscher Sicherheit wiegen. Mit Ransomware können Cyberkriminelle schnell Gewinn machen. Die Angreifer werden ihre Methoden verändern und anpassen, sobald die Abwehr gegen gängige Attacken verstärkt wird und die Mitarbeiter aufgeklärt werden, um sich besser schützen zu können. Sie werden nicht willens sein, so einfach auf den Zahltag zu verzichten.

Über LogRhythm

LogRhythm ist der Pionier für Threat Lifecycle Management™ (TLM) und befähigt Unternehmen auf sechs Kontinenten, gefährliche Cyberbedrohungen schnell zu erkennen, abzuwehren und zu neutralisieren. Die TLM-Plattform von LogRhythm vereint führende Data-Lake-Technologien, künstliche Intelligenz, Sicherheitsanalysen sowie Sicherheitsautomatisierung und -orchestrierung in einer einzigen, durchgängigen Lösung. LogRhythm schafft die Grundlagen für das KI-gestützte Security Operations Center und hilft den Kunden, ihre Cloud-, physischen und virtuellen Infrastrukturen für IT- wie auch OT-Umgebungen zu schützen.

LogRhythm hat eine Reihe von Auszeichnungen erhalten, darunter die Einstufung als „Leader" in Gartners SIEM Magic Quadrant.

www.logrhythm.com

[1] Cyber-extortion losses skyrocket, says FBI http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/
[2] Cyber security breaches survey 2017 (Department for Culture, Media & Sport): https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_ Security_Breaches_Survey_2017_main_report_PUBLIC.pdf

+49 89 919292 - 200 | europe@logrhythm.com | www.logrhythm.com