Der große Beutezug

Warum Cybergangster mit Ransomware immer höhere Lösegelder erpressen

Binnen weniger Jahre haben sich Verschlüsselungstrojaner von einer lästigen Randerscheinung zu einer mächtigen Bedrohung gewandelt. Die Lösegelder wirken als Brandbeschleuniger, aber auch weitere Faktoren spielen eine Rolle.

Von Uli Ries und Christian Wölbert

Beinahe putzig wirken heutzutage die 200 US-Dollar, die Opfer des damals dominierenden Verschlüsselungstrojaners CryptoWall im Jahr 2014 als Lösegeld zahlen mussten. Mittlerweile geht es bei Ransomware-Attacken um andere Summen: 2020 lag die durchschnittliche Lösegeldzahlung laut einer Studie von Palo Alto Networks bei 313.000 US-Dollar – 2019 waren es erst 115.000 Dollar.

In den vergangenen Monaten häuften sich spektakuläre Fälle, in denen Firmen ihre verschlüsselten Daten sogar mit Millionensummen freikauften. Im Juni bestätigte der Fleischverarbeiter JBS USA, dass er elf Millionen US-Dollar an eine Ransomware-Gang überwiesen hat. Der Pipeline-Betreiber Colonial hatte zuvor über vier Millionen Dollar gezahlt, das Versicherungsunternehmen CNA Financial laut einem Bloomberg-Bericht sogar 40 Millionen.

Im Jahr 2020 flossen insgesamt gut 400 Millionen US-Dollar an bekannte Kryptowährungsadressen von Ransomware-Gangs, ergab eine Analyse des Dienstleisters Chainalysis. Im Vergleich zu 2019 hat sich die Summe mehr als vervierfacht. Der insgesamt durch Ransomware angerichtete Schaden – inklusive Umsatzausfällen der Opfer – liegt nach Schätzungen im zweistelligen Milliardenbereich, pro Jahr.

Mittlerweile hat das Thema die höchsten Ebenen der Politik erreicht. Im Juni konfrontierte US-Präsident Joe Biden den russischen Präsidenten Wladimir Putin mit dem Vorwurf, Cybergangstern freie Hand zu lassen. „Ich habe ihn angesehen und gesagt: Wie würden Sie sich fühlen, wenn Ransomware die Pipelines auf Ihren Ölfeldern angreifen würde“, berichtete Biden nach dem Treffen in Genf.

Bild: Saul Loeb/Pool AFP/dpa

US-Präsident Joe Biden wirft dem russischen Präsidenten Wladimir Putin vor, Cybergangster gewähren zu lassen.

Großwildjagd

Beigetragen zu der „Ransomware-Epidemie“ haben mehrere Entwicklungen. Infizierten die Kriminellen bis vor drei, vier Jahren noch weitgehend automatisch und daher wahllos per Schwachstellen-Scan, suchen sie sich ihre Opfer inzwischen gezielter aus – und nehmen bevorzugt zahlungskräftige Organisationen ins Visier. „Big Game Hunting“ nennt das BKA dies im Cybercrime-Bundeslagebild 2020. Daher sehen sich kaum noch Privatpersonen einer Lösegeldforderung gegenüber. Sie sind schlicht nicht finanzstark genug und daher uninteressant.

Kriminelle trieben heute mehr Aufwand vor der initialen Infektion eines Unternehmens, sagt Michael Veit, Technology Evangelist beim britischen Cybersecurity-Unternehmen Sophos, im Gespräch mit c’t. Nötig sei dies, da massenhaft verteilte Schädlinge regelmäßig von Antivirensoftware abgefangen würden. Daher verlegten sich die Ransomware-Gruppen beispielsweise auf den Versand von im Spear-Phishing-Stil erzeugten, vergifteten Word-Dateien oder PDFs mit vermeintlichen Lebensläufen an Personalabteilungen. Das Recherchieren der Stellenausschreibungen und Ansprechpartner ist vergleichsweise aufwendig.

Ist der erste Rechner infiziert, schalten sich laut Veit in der Regel menschliche Operatoren ein und kartografieren das Netzwerk. Nur menschliche Angreifer könnten sich unbemerkt mit an sich legitimen Tools wie PowerShell mehr Rechte verschaffen und bis zum Herz des Netzwerks, dem Active Directory (AD), durchhangeln. Durch das Manipulieren des AD legen sie die Grundlage für den nächsten Schritt.

Verhöhnen und leaken

Seit Ende des Jahres 2019 besteht dieser nächste Schritt nicht mehr im blindwütigen Verschlüsseln der Daten auf Servern und Endgeräten. Die Kriminellen saugen stattdessen zunächst sensible Daten ab –

und erpressen das Opfer hinterher auf einem zweiten Weg: Will ein Unternehmen nicht für die Entschlüsselung bezahlen, weil es sich beispielsweise auf seine Offline-Backups verlassen kann, drohen die Cyber-Verbrecher mit der Veröffentlichung der vertraulichen Daten. Im Fall des Apple-Fertigers Quanta wurden beispielsweise Konstruktionszeichnungen geleakt.

Auf Webseiten, die typischerweise nur über das anonymisierende Tor-Netzwerk erreichbar sind, listen und verhöhnen die Ransomware-Gruppen ihre Opfer. Zahlen die betroffenen Unternehmen nicht, stellen die Kriminellen die erbeuteten Daten zum Download bereit – Mails, Patientendaten, Forschungsergebnisse, Verträge, Labor-Reports, Ausweiskopien, Bankbelege und so weiter. So fanden sich beispielsweise rund 20 Gigabyte an Finanzdaten sowie 90 Gigabyte an E-Mails der Software AG auf der Seite der Cl0P genannten Gang. Die Ragnar-Locker-Gruppe hat weit mehr als 1,5 Terabyte an internen Daten des taiwanischen Speicherherstellers Adata ins Netz gestellt.

Unheilvolle Lösegelder

Ein weiterer Treiber der Entwicklung sind die Lösegelder selbst. Aus Sicht der Opfer mögen die Zahlungen nachvollziehbar erscheinen, denn diese fallen in aller Regel günstiger aus als der Umsatzverlust bis zum Neuaufbau der betroffenen IT-Systeme. Häufig legt die Verschlüsselung von Daten die betroffenen Firmen komplett lahm. Im Fall von Symrise, einem deutschen Hersteller von Duft- und Geschmacksstoffen, beziffert das Bundeskriminalamt den durch einen „Produktions- und Kommunikationsausfall“ verursachten Schaden auf „mehrere Millionen Euro pro Ausfalltag“. Symrise war von der Cl0p-Gruppe mit Ransomware angegriffen worden.

Doch langfristig wirken die Lösegelder unheilvoll. Sprechen sich solche Zahlungen im Untergrund herum, steigt die Motivation anderer Krimineller, sich ebenfalls an einer Ransomware-Attacke zu versuchen. Je mehr Geld im Untergrund landet, desto leichter kommen die Kriminellen an neue Exploits, Dienstleister zum Verschleiern der Bitcoin-Transaktionen oder Social-Engineering-Spezialisten, die die initiale Infektion der Opfer erledigen. Und je mehr Unternehmen sich freikaufen, desto normaler erscheint der Vorgang anderen Betroffenen.

Seit 2019 stellen die Erpresserbanden auch sensible Daten ihrer Opfer zum Download bereit.

Versicherungen als Treiber?

Eine Rolle spielen dabei nach Meinung einiger Experten auch Versicherungen. Denn immer mehr Organisationen schließen spezielle Cyber-Policen ab, die auch Ransomware-Attacken abdecken. Aus Sicht der Kriminellen ist eine vorhandene Versicherung jedoch ein sehr gutes Argument dafür, die Lösegeldforderung noch weiter in die Höhe zu schrauben.

Strafverfolger und Cybersicherheitsbehörden raten in der Regel davon ab, Lösegelder zu zahlen. Manche Experten in den USA und Europa fordern sogar, Ransomware-Zahlungen gesetzlich zu verbieten, um die Angreifer finanziell auszutrocknen. Als erste große Versicherung entschied im Mai Axa, in Frankreich künftig keine Policen mit Lösegeld-Erstattung anzubieten. Damit habe man auf Bedenken der französischen Regierung reagiert, erklärte der Konzern gegenüber US-Medien.

Nach einer Umfrage des Security-Anbieters Sophos sind die Lösegelder außerdem oft nur vermeintlich eine einfache Lösung: Nur acht Prozent von mehr als 1000 befragten Unternehmen, die ein Lösegeld zahlten, hätten dadurch sämtliche Daten zurückerhalten. „Viele mussten sich mit dem Wiederherstellen von Backups oder gar dem händischen Abtippen von Daten retten, trotz vorheriger Zahlung“, berichtet der Sophos-Experte Michael Veit gegenüber c’t.

Schwachstelle Homeoffice

Als weiteren Treiber sehen Experten den coronabedingten Wechsel ins Homeoffice. Diese Entwicklung habe „unzweifelhaft die potenzielle Angriffsfläche von Zielorganisationen vergrößert“, schreibt die britische Denkfabrik RUSI in einer im März veröffentlichten Studie. Die Gefahr von Schwachstellen und Fehlkonfigurationen sei durch die Installation neuer Hard- und Software gestiegen, hinzu kämen mögliche Lücken in der Heim-IT der Angestellten.

Strafverfolger konnten gegen den Beutezug der Erpresser bislang wenig ausrichten. Es gab zwar Ermittlungserfolge, etwa den Schlag europäischer Behörden gegen die Emotet-Infrastruktur im Januar. Die Angriffe mit der Emotet-Malware hatten Verschlüsselungstrojanern den Weg bereitet. Doch die Erfolge der Fahnder wirken im Rückblick wenig nachhaltig – der Ransomware-Hydra wachsen zuverlässig neue Köpfe.

Immer wieder sehen Ermittler Hinweise darauf, dass viele Banden tatsächlich aus Russland und anderen Ex-Sowjetstaaten heraus agieren. Ein weiteres Indiz liefert der Thinktank RUSI in seiner Studie. Die Forscher haben 1200 Blogeinträge von Ransomware-Gangs ausgewertet und festgestellt, dass die angegriffenen Organisationen aus insgesamt 63 Ländern stammten, es jedoch kein einziges Opfer mit Hauptsitz in Russland gab.

An diesem Muster dürfte sich auch in Zukunft wenig ändern, trotz der Versuche von US-Präsident Biden, Russland zur Kooperation zu bewegen. In seiner Genfer Pressekonferenz widersprach Putin dem Vorwurf, dass die Angriffe aus Russland kämen, und erklärte, seine Behörden hätten stets auf Anfragen amerikanischer Ermittler reagiert. Nicht überliefert ist, was Putin auf Bidens Frage antwortete, wie er sich bei einer Ransomware-Attacke auf russische Pipeline-Betreiber fühlen würde. *(cwo@ct.de)* c't