TLP: WHITE

ENJOY SAFER TECHNOLOGY™

RANSOMWARE:
Unternehmen im Visier von Malware und Manipulation

V 2.0

Autor: Ondrej Kubovič

INHALT

ZIELE 2
RANSOMWARE — LÄNGST EIN WELTWEITES PROBLEM 2
RANSOMWARE BRINGT GELD. VIEL GELD. 3
DIE PSYCHOLOGIE HINTER RANSOMWARE 3
DIE TECHNOLOGIE HINTER RANSOMWARE 4
RANSOMWARE PER RDP 6
Serverparasiten 9
Abwehr RDP-basierter Ransomware 10
Ein weiteres Einfallstor: Das SMB-Protokoll 12
Absicherung von RDP gegenüber Ransomware 12
RANSOMWARE VIA EMAIL. 14
RANSOMWARE-ATTACKEN ÜBER DIE SUPPLY CHAIN 16
RANSOMWARE-ANGRIFFE ÜBER UNGEPATCHTE SCHWACHSTELLEN. 16
SEGMENTIERUNG UND AUSLAGERUNG IN DIE CLOUD 18
PATCHING UND BACKUPS: GRUNDLEGENDER SCHUTZ VOR RANSOMWARE . . 18
UND WIE REAGIERT MAN NUN AUF RANSOMWARE? 20
ENDPOINT DETECTION AND RESPONSE 21
EIN WORT ZUM THEMA LÖSEGELD 22
DIE ZUKUNFT von RANSOMWARE 23
FAZIT 24
ÜBER ESET 26

V 2.0

Autor: Ondrej Kubovič
Danksagung: Bei diesem Whitepaper handelt es sich um eine Neuauflage eines Papers von Stephen Cobb aus dem Jahr 2018. Mit eingeflossen sind die neuesten Erkenntnisse (2021) meiner ESET Kollegen Rene Holt, James Shepperd, Nick FitzGerald, Hana Matušková und Klára Kobáková.

Ursprünglicher Autor: Stephen Cobb
Danksagung: Dieses Whitepaper hätte nicht geschrieben werden können ohne die Hilfe meiner ESET Kollegen James Rodewald, Ben Reed, Fer O'Neil und David Harley, und ohne mein herausragendes Team Aryeh Goretsky, Bruce P. Burrell und Cameron Camp.

Anmerkung: Bei diesem Paper handelt es sich um eine Übersetzung im Auftrag der ESET Deutschland GmbH. Das Original-PDF finden Sie *hier*.

August 2021

ZIELE

Dieses Whitepaper verdeutlicht, welche Gefahren von Ransomware ausgehen, beschreibt die neuesten Methoden der Angreifer und gibt Hinweise dazu, wie Unternehmen Ransomware erfolgreich abwehren und potenzielle Schäden minimieren.

Dazu schauen wir uns drei Hauptangriffsvektoren genauer an: Remote-Zugriff, E-Mail und Lieferketten.

RANSOMWARE — LÄNGST EIN WELTWEITES PROBLEM

Ransomware ist eine Form von Schadsoftware, mit der Angreifer Unternehmen den Zugriff auf wichtige Unternehmensdaten entziehen – um dann ein Lösegeld für die Freigabe zu fordern. Schadsoftware wiederum wird hier als Oberbegriff für alle Formen von Computercode verwendet, die auf fremden Rechnern Schaden anrichten sollen. Dazu zählen die bekannten Computerviren, aber auch Würmer und Trojaner.

Längst hat sich Ransomware zu einer der größten Cybergefahren für Unternehmen entwickelt. Der Grund: Im Laufe der letzten Jahre haben Kriminelle nicht nur immer neue und perfidere Formen der Malware entwickelt. Auch „Ransomware as a Service", also die Bereitstellung verschiedenster Angriffsformen als Dienstleistung durch Dritte, wird immer verbreiteter. Die Attacken werden so immer gezielter und gleichzeitig immer schwerer zu quantifizieren.

Auch werden die Kriminellen immer besser darin sicherzustellen, dass ihre Lösegeldforderungen auch erfüllt werden – üblicherweise, indem sie den Druck auf das Opfer erhöhen. Seit 2019 etwa arbeiten die Angreifer oft mit dem sogenannten „Doxing" (oder „Double Extortion", etwa „Doppelte Erpressung"): Wichtige Unternehmensdaten werden nicht nur verschlüsselt und damit für das Unternehmen unbrauchbar gemacht. Die Angreifer drohen zugleich damit, die gestohlenen Daten – meist höchst sensibel oder anderweitig wertvoll – an die Öffentlichkeit zu geben oder weiterzuverkaufen.

Zusätzlich sind einige Kriminelle dazu übergegangen, Geschäftspartner oder Kunden derjenigen Opfer zu kontaktieren, die nicht auf die Lösegeldforderung eingehen. Sie informieren darüber, dass ihre sensiblen Daten im Rahmen eines Ransomware-Angriffs kompromittiert wurden. Dies soll den externen Druck auf das Opfer erhöhen. In einigen Fällen wurden sogar die Partner/Kunden selbst aufgefordert, ein Lösegeld zu zahlen.

In letzter Zeit weichen Angreifer davon ab, eine große Anzahl willkürlich ausgewählter Opfer ins Visier zu nehmen und eher kleine Summen zu fordern. Aktuell sind die Angriffe wesentlich gezielter auf eine kleine Gruppe von Opfern ausgerichtet. Im Fokus stehen häufig große Unternehmen, von denen größere Summen gefordert werden können. Selbstverständlich wächst so der potenzielle Schaden bei tatsächlichen Datenverlusten.

Immer wieder berichten Medien über groß angelegte Ransomware-Angriffe auf hochrangige Ziele. Hier eine Auswahl an Artikeln zu Angriffen im Jahr 2021:

- *Kaseya schließt Sicherheitslücke nach Angriff durch REvil-Ransomware*
- *REvil-Ransomware attackiert US-amerikanische Nuklear-Beratungsfirma*
- *Lösegeldforderung von 20 Millionen US-Dollar nach Ransomware-Angriff auf irisches Gesundheitssystem*
- *Cyberangriff verursacht Shutdown von US-amerikanischer Kraftstoff-Pipeline*
- *ADATA wird Opfer von Ransomware Ragnar Locker*
- *Ransomware-Vorfall in US-Stadt Tulsa beeinträchtigt kommunale Online-Dienste*

Es zeigt sich, dass die Attacken sowohl Organisationen der öffentlichen Hand als auch private Unternehmen unterschiedlichster Branchen ins Visier nehmen. Somit wird klar: Gezielte Ransomware-Angriffe können jeden treffen. Dabei arbeiten die meisten Urheber von Ransomware in den seltensten Fällen mit technisch anspruchsvollen Methoden. Dennoch stellen sie eine der größten Gefahren für die IT-Sicherheit von Unternehmen jeglicher Größe dar.

RANSOMWARE BRINGT GELD. VIEL GELD.

Niemand kann genau beziffern, wie viel Geld die Urheber und diejenigen, die sie verbreiten, mit Ransomware verdienen. Eine aktuelle *Studie des Threat-Intelligence-Anbieter Group-IB* schätzt die durchschnittliche Höhe von Lösegeldforderungen auf etwa 170.000 US-Dollar. Gleichzeitig betonen Forscher, dass besonders dreiste Gruppen auch schon mehrere zehn Millionen Dollar gefordert hätten. Die Verschlüsselungssoftware Sodinokibi (aka REvil) beispielsweise verlangte jeweils 50 Millionen US-Dollar von ihren Opfern Acer und Quanta.

Einige weitere Zahlen von verschiedenen Quellen:

- *European Union Agency for Cybersecurity (ENISA)*: rund 10 Milliarden Euro tatsächlich gezahlte Lösegelder im Jahr 2019,
- *FBI*: 144 Millionen US-Dollar Lösegeld im Zeitrahmen von 2013 bis 2019 an Ryuk,
- *Sodinokibi*: 100 Millionen US-Dollar „Gewinn" in 2020 allein aus Lösegeldern (vermutlich übertrieben),
- *AdvIntel*: 150 Millionen US-Dollar Lösegeld an Ryuk (2020),
- Zahlung von 40 Millionen US-Dollar Lösegeld an *Phoenix Locker durch CNA Financial* im Jahr 2021 – die höchste bisher bekannte Summe, die im Rahmen eines Ransomware-Angriffs gezahlt wurde,
- 17,5 Millionen US-Dollar Lösegeld an Darkside im Rahmen des *Angriffs auf die Colonial Pipeline*,
- *Chainanalysis*: geschätzte 350 Millionen US-Dollar tatsächlich gezahlte Lösegelder insgesamt in 2020 und
- 70 Millionen US-Dollar Lösegeldforderung durch Sodinobiki für einen Universal-Schlüssel zur Freigabe von Daten nach dem Angriff auf *Kaseya VSA* 2021.

DIE PSYCHOLOGIE HINTER RANSOMWARE

Ransomware-Kampagnen fokussieren sich vor allem darauf, psychischen Druck auf ihre Opfer aufzubauen. Egal, welcher Methode sie sich im Detail bedienen: Immer sorgt die Schadsoftware dafür, dass wertvolle Daten verschlüsselt und dem Zugriff des Opfers entzogen werden. Dabei ist es unerheblich, um welche Informationen es sich konkret handelt. Personenbezogene, unternehmerisch relevante Daten oder geistiges Eigentum: Wertvoll und schützenswert sind sie letztlich alle.

Schon allein der Verlust von Daten kann das Opfer massiv unter Druck setzen. Dieser steigt jedoch weiter an, wenn der Verlust der Daten den Ruf einer Person oder eines Unternehmens schädigen, Geschäftsabläufe behindern oder gar rechtliche Folgen nach sich ziehen kann. Diesen Effekt nutzen Cyberkriminelle zunehmend aus. Immer häufiger bedienen sie sich dabei des oben erwähnten „Doxings": Hierbei suchen die Kriminellen gezielt nach besonders „pikanten" Daten und Informationen auf dem Rechner oder im Netzwerk des Opfers und drohen, diese öffentlich zu machen. Nur die Zahlung einer zusätzlichen Summe zum eigentlichen Lösegeld kann das Opfer dann vermeintlich davor bewahren, in aller Öffentlichkeit sein Gesicht zu verlieren.

Als Urheber des Doxing-„Trends" seit November 2019 gilt die Gruppe Maze, die ihre Methodik seitdem noch „verfeinerte" und eine eigene Leak-Seite für die Veröffentlichung privater Daten ins Darknet stellte. Für die Betroffenen wurde es so noch schwieriger, einmal veröffentlichte Daten zurückzubekommen. Zwar hat sich Maze nach eigenen Angaben aus dem „Geschäft" zurückgezogen – die Technik des Doxing ist geblieben.

Durch diesen psychischen Druck – der sich beinahe beliebig steigern lässt – erhöhen die Angreifer ihre Chancen, ihr Ziel – Geld verdienen – zu erreichen. Um ihre Opfer bei Bedarf immer stärker unter Druck setzen zu können, beschränken sich die Kriminellen oftmals nicht nur auf ein Element der digitalen Infrastruktur eines Unternehmens. Das Spektrum ist weit und reicht von DDoS-Angriffen auf die Unternehmenswebsite bis zu Manipulationen durch Hacker, mit denen sie sich im internen Netzwerk bemerkbar machen und so ihre Macht demonstrieren.

Einige Methoden scheinen gezielt darauf ausgelegt zu sein, Angst zu verbreiten. Beim sogenannten *Print Bombing* kapern Kriminelle alle Drucker im Netzwerk und drucken darauf ihre Lösegeldforderung. Hier geht es den Angreifern allein um die Demonstration ihrer Macht. Sie können die Sicherheitslücke jederzeit sowohl innerhalb des Unternehmens als auch nach außen hin sichtbar machen – ohne dass die Geschäftsführung sich dagegen wehren könnte.

Es geht sogar noch perfider, indem Angreifer auf Unternehmensdaten zugreifen und die Eigentümer dann direkt kontaktieren, beispielsweise *telefonisch*. Sie drohen und versuchen, die Betroffenen zu unbedachten Handlungen zu verleiten, während die IT-Abteilung noch damit beschäftigt ist, die Sicherheitslücke zu schließen.

Dies sind nur einige Methoden moderner Ransomware-Kampagnen. Mittlerweile ist die Schadsoftware längst zu einem Mittel psychologischer Kriegsführung geworden. Aus einem Malware-Vorfall wird so schnell ein viel größeres Problem, indem die Opfer zu Handlungen bewegt werden, die ihnen selbst oder dem Unternehmen schaden. Im Gegensatz zu Erpressern in der realen Welt, die meist nur ein Ass im Ärmel haben, können Cyberkriminelle mehrere Trümpfe ausspielen. Haben sie einmal Zugriff auf ein Netzwerk erlangt, können sie beliebige und immer neuere Methoden anwenden. Und ihre Opfer potenziell über schier endlos lange Zeiträume weiter erpressen.

Cyberkriminelle bedienen sich einer Vielzahl von Techniken, um Zugriff auf fremde Rechner zu erhalten und die Aktivitäten von Nutzern auszuspähen. So ermitteln sie neuralgische Punkte, an denen es besonders lohnenswert erscheint, Druck auszuüben. Die Macht, die Cyberkriminelle potenziell über die Daten, Netzwerke, Geschäftsabläufe und letztlich das öffentliche Ansehen ihrer Opfer erlangen können, ist immens. Dabei müssen sie sich nicht einmal ausgeklügelter Malware, bisher unbekannter Schwachstellen oder langfristig angelegter und durchdachter Kampagnen bedienen. Oft reichen schon fehlende Security Awareness von Mitarbeitern, schlecht abgesicherte Netzwerkprotokolle oder andere Tools für den Fernzugriff sowie Lücken in Gewohnheiten und Prozessen sowohl im Unternehmen selbst als auch bei externen Dienstleistern oder anderen Stufen der Lieferkette.

DIE TECHNOLOGIE HINTER RANSOMWARE

Zwar ist Ransomware schon seit mehr als 10 Jahren ein bekanntes Problem. Sie hat jedoch durch die COVID 19-Pandemie und die damit einhergehende Verschiebung des sozialen und Arbeitslebens in die digitale Welt weiteren Vorschub erhalten. So führten unter anderem die Sorgen von Unternehmen um Geschäftschancen – und letztlich ihre Existenz – während der verschiedenen Corona-Lockdowns zu einer Welle an Phishing-Mails, die sich genau dieser Ängste bedienten.

Aber auch der Umzug vieler Mitarbeiter ins Homeoffice war ein gefundenes Fressen für Cyberkriminelle: Viele Mitarbeiter mussten – teilweise zum ersten Mal – von außen (beispielsweise per Remote Desktop Protocol, RDP) auf unternehmensinterne Systeme zugreifen. Dies wurde zu einem der beliebtesten Angriffsvektoren für Ransomware. Über die Adminrechte, die oftmals für den schnellen und unkomplizierten Zugriff per RDP vergeben wurden, hatte Ransomware – ebenso wie viele andere Malware – leichtes Spiel.

Es scheint, als sei Ransomware vor allem für ambitionierte Cyberkriminelle interessant. Während technisch weniger versierte Akteure mit schnell dahingehackten Skripten einzelne Opfer per Spam täuschen können, versuchen fortgeschrittene Hacker Malware (darunter auch Ransomware) per Downloader oder Botnet zu verbreiten. Ehrgeizigere Kriminelle bauen ganze Geschäftsmodelle aus illegalen Praktiken auf: So kaufen sie zum Beispiel fertige Ransomware und bieten diese als Teil eines „Ransomware as a Service“ (RaaS)-Pakets an.

Besonders ausgeklügelte RaaS-Modelle nutzen Schwachstellen in einzelnen Rechnern, um darüber Zugriff auf Server und ganze Netzwerke zu erhalten. Erst zu einem späteren Zeitpunkt wird

Ransomware aufgespielt oder der Zugriff anderweitig missbraucht. Finanziell gut ausgestattete Gruppen kaufen oder entwickeln eigene Zero Day-Exploits, gegen die selbst moderne Security-Systeme oft nur wenig ausrichten können. Besonders ambitionierte Gruppen, sei es durch Glück, Können oder große personelle wie finanzielle Ressourcen, legen *komplette IT-Infrastrukturen lahm, indem sie Angriffe auf Dienstleister* oder andere Stufen der Lieferkette fahren („Supply Chain-Attacken"). Durch die Übernahme verbreiteter MSP- (Managed Service Provider) Plattformen und -Tools können Angreifer verhältnismäßig leicht mehrere Netzwerke (und damit Unternehmen) infiltrieren und beispielsweise Ransomware aufspielen. Es erscheint nicht unwahrscheinlich, dass solche groß angelegten Supply Chain-Angriffe in den nächsten Jahren zunehmen werden.

Um auf Attacken vorbereitet zu sein und Geschäftsausfälle effektiv zu verhindern, sollten Unternehmen die Vielfalt der Methoden und die Geschwindigkeit, mit der sich Ransomware weiterentwickelt, nicht unterschätzen. Und letztere kann wirklich beeindruckend sein, wie der Fall *Sodiboniki* (aka REvil) zeigt: Zunächst wurde die Ransomware dabei beobachtet, wie sie Dateien im sogenannten „abgesicherten Modus" des Rechners verschlüsselte. Dadurch war sie zwar schwer zu entdecken, benötigte für ihre tatsächliche Ausführung aber noch immer Login-Daten. *Innerhalb eines einzigen Monats* entwickelte sich die Ransomware dahingehend weiter, dass sie das Login-Passwort entsprechend der Vorgaben des Angreifers änderte und den Rechner automatisch im abgesicherten Modus neu starten ließ. Kriminelle erhielten so umfangreichen Zugriff auf gekaperte Rechner und konnten groß angelegte Kampagnen fahren.

NAS-Speicher, die üblicherweise für den Dateitransfer und zum Ablegen von Backups genutzt werden, gelangten ebenfalls ins Visier von Ransomware-Gruppen. 2021 informierte der NAS-Hersteller *QNAP* seine Kunden darüber, dass die Ransomware eCh0raix deren NAS-Systeme angreife. Besonders betroffen seien diejenigen mit schwachen Passwörtern. ESET Telemetrie-Daten aus dem vierten Quartal 2020 zufolge war cCh0raix die häufigste auf NAS beobachtete Ransomware.

RANSOMWARE PER RDP

Ein RDP-Endpoint ist ein Windows-Rechner, auf dem eine RDP (Remote Desktop Protocol)-Software läuft und so über ein Netzwerk, z.B. das Internet, erreichbar ist. RDP erlaubt Firmenadministratoren, alle Windows-Rechner in einem Unternehmen aus der Ferne zu steuern. Das ist generell sehr nützlich, um beispielsweise Fehler schnell zu finden und zu beheben. Auch Hochleistungsrechner für umfangreiche Rechenoperationen, Anwendungen oder Datenbanken können so aus der Ferne bedient werden.

Auf Unternehmensrechnern, auf die Mitarbeiter remote Zugriff haben sollen, muss RDP aktiviert sein. Idealerweise sollte der Zugang zusätzlich per *Multi-Faktor-Authentifizierung (MFA)* abgesichert werden. Dann können sich Mitarbeiter mithilfe der RDP-Software mit diesen Systemen verbinden, zum Beispiel über ihren Laptop. Wird die Netzwerkadresse des Zielrechners eingegeben, fragt die Client-Software den zugewiesenen Port im Zielrechner an (der Standard-Port für RDP ist 3389 – dieser lässt sich aber ändern). Der Mitarbeiter sieht dann als Nächstes ein Login-Fenster, das nach einem Benutzernamen und Passwort fragt. Wie ein solches Fenster üblicherweise auf einem Windows-Rechner aussieht, zeigt Abbildung 1.

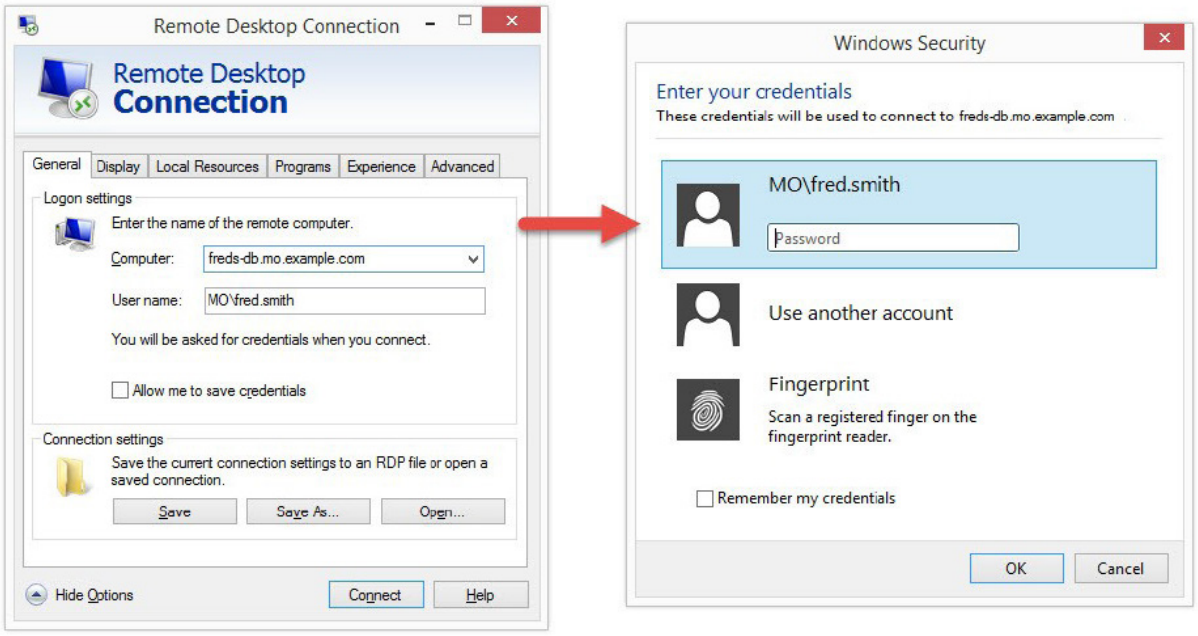

Abbildung 1: RDP-Login-Fenster

Unternehmen nutzen RDP vor allem um:

1. Programme, die auf einem Server laufen, zu verwalten, z.B. eine Website oder eine Backend-Datenbank. Im einfachsten Fall gibt ein Systemadministrator hierfür den Port 3389 frei, um den Zugriff durch Externe zu ermöglichen.
2. Unternehmensrechnern oder VMs den Fernzugriff auf Unternehmensressourcen zu ermöglichen, die sonst nicht von außen erreichbar sind. Die Nutzung von RDP ermöglicht es, sensible interne Server für bestimmte Gruppen erreichbar zu machen, ohne sie dem gesamten Internet gegenüber offenzulegen. Zusätzlich hilft RDP, leistungsstarke oder anderweitig besonders ausgestattete Rechner, die physisch im Büro stehen, für externe Mitarbeitern nutzbar zu machen. Auch hierfür wird meist einfach Port 3389 freigegeben.

Genau diese Vorteile machen RDP jedoch auch zum beliebten Einfallstor für Angriffe. Ist es möglich, von außen auf ein System zuzugreifen, haben Kriminelle oft leichtes Spiel, denn:

- unzureichend abgesicherte RDP-Systeme lassen sich ohne großen Aufwand ausfindig machen
- das Eindringen in solche Systeme ist für Angreifer besonders einfach
- viele RDP-Systeme sind nur unzureichend abgesichert
- Haben Kriminelle einmal Zugang erhalten, können sie auf eine Vielzahl von Tools und Methoden zurückgreifen, um sich selbst mit umfassenden Rechten auszustatten.

RDP-Server lassen sich mit speziellen Suchmaschinen wie *Shodan* ohne Vorkenntnisse ausfindig machen. Sie durchforsten das Internet nach verbundenen Geräten und sammeln Informationen darüber. Eine Suche bei shodan.io am 15. Juni 2021 ergab beispielsweise, dass bei mehr als drei Millionen Rechnern im Internet besagter Port 3389 offen war. Wie in Abbildung 2 zu sehen, standen mehr als 130.000 dieser Systeme in Deutschland. (Für die vollständige Ansicht gefilterter Suchanfragen ist ggf. eine Registrierung notwendig).

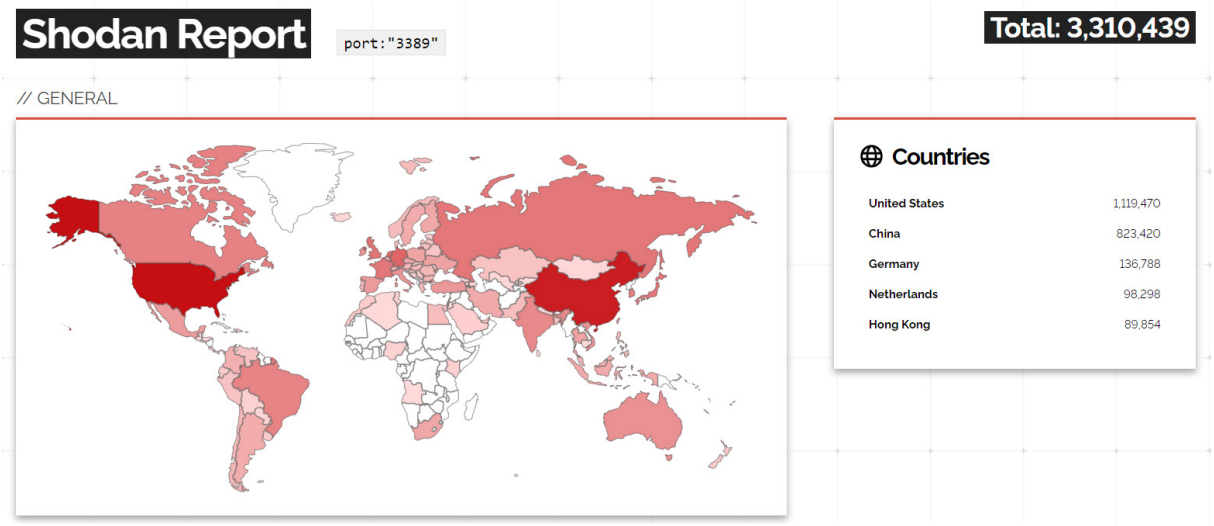

Abbildung 2: Mehr als drei Millionen Rechner im Internet nutzen Port 3389 (Quelle: Shodan)

Wie eine *weitere Suchanfrage* ergab, läuft auf mehr als 2,7 Millionen Rechnern weltweit explizit RDP. Für einen Angreifer sind diese potenzielle und leicht angreifbare Ziele. Zwar erfordert der Login auf ein RDP-System einen Benutzernamen und ein Passwort. Diese Daten sind jedoch in vielen Fällen für die Angreifer erstaunlich einfach zu erraten. Entsprechend leicht ist es für Kriminelle, über RDP/Port 3389 Zugang zu fremden Netzwerken zu erhalten.

Noch einfacher ist es für Kriminelle mit ausreichend großem Budget: Zugangsdaten zu bereits kompromittierten RDP-Systemen können problemlos im Darknet gekauft werden. Dabei gilt die Verbreitung von Ransomware nicht als einziger Grund für Kriminelle, Geld dafür auszugeben. Sie lassen sich ebenso für den Versand von Spam, Malware-Hosting, das Knacken von (besser geschützten) Passwörtern, zum Schürfen von Kryptowährung, für Käuferbetrug oder Geldwäsche sowie eine Vielzahl anderer illegaler Aktivitäten nutzen. Allen gemein ist der Wunsch der Verantwortlichen, anonym zu bleiben und sicherzustellen, dass die Aktivität nicht bis zu ihnen zurückverfolgt werden kann.

Werden nur Benutzername und Passwort für einen externen Zugang benötigt, versuchen die Angreifer meist, diese in vielen Versuchen zu erraten. Geschieht dies besonders schnell und mithilfe einer Datenbank möglicher Zugangsdaten, bezeichnet man diese Form auch als Brute Force-Angriff. Fehlt ein Sicherheitsmechanismus, der das System bei zu vielen fehlgeschlagenen Versuchen (kurzzeitig) abriegelt, sind solche Angriffe höchst effektiv und ermöglichen Cyberkriminellen umfassenden Zugriff auf fremde Netzwerke.

Wie ESET Telemetrie-Daten bestätigen, zählt RDP zu den beliebtesten Angriffsvektoren. Allein zwischen Januar 2020 und Juni 2021 wurden mehr als 71 Milliarden Angriffe über RDP beobachtet. Während in der ersten Hälfte des Jahres 2020 der Anstieg am steilsten verlief, gab es 2021 die insgesamt größte Anzahl entsprechender Attacken. Vergleicht man H1 2020 mit H1 2021, versechsfachte sich die Anzahl von Brute Force-Angriffen auf RDP.

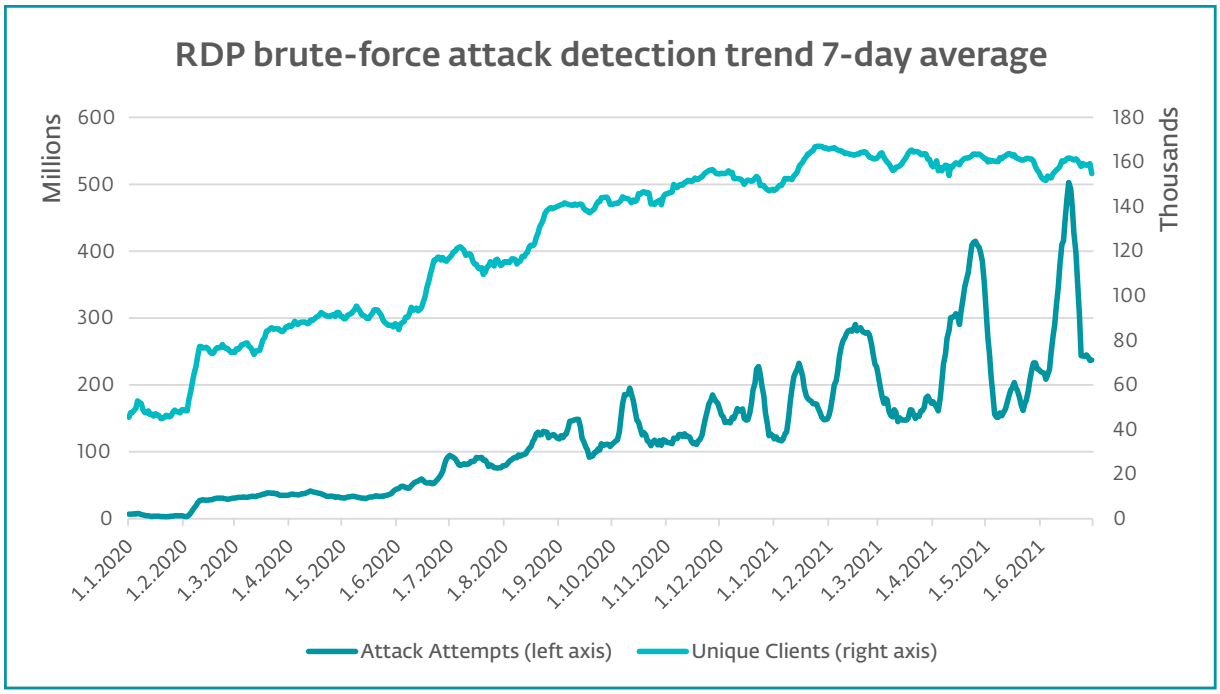

Abbildung 3: Trends der Angriffsversuche auf RDP und Einzel-Clients zwischen Januar 2020 und Juni 2021, gleitendes 7-Tages-Mittel

Grundsätzlich müssen Angreifer einen größeren Aufwand betreiben, um über das Internet auf RDP-Systeme zuzugreifen, als Ransomware schlicht per E-Mail zu versenden. Zugleich bieten Angriffe über diesen Weg einige Vorteile: die Möglichkeit, einen bestehenden, legitimen Zugang zu missbrauchen, Security-Mechanismen zur Absicherung des Endpoints zu umgehen sowie die Chance, gleich mehrere Rechner oder gar das gesamte Netzwerk in einem Unternehmen zu kompromittieren.

> „Im Gegensatz zu verseuchten E-Mails werden Angriffe via RDP von vielen Abwehrmechanismen nicht zuverlässig erkannt. Das führt auch dazu, dass weniger Daten zur Gefahrenlage vorliegen und das allgemeine Bewusstsein über die Gefahr entsprechend geringer ausfällt.“

Im Fall von Ransomware per E-Mail schlagen viele Security-Systeme an und blockieren deren Ausführung. Solche Vorfälle werden intern dokumentiert und durch die Security-Programme gemeldet. Die Hersteller wiederum erstellen aus diesen Daten umfangreiche anonymisierte Statistiken, die Einsicht in die aktuelle Bedrohungslage geben.

Auch Websites, über die sich Ransomware verbreitet, werden in Statistiken erfasst. Hat der Angreifer jedoch mithilfe von Admin-Rechten die Endpoint Security deaktiviert, bevor die Ransomware auf das System des Opfers gelangt, taucht der Angriff nicht in den üblichen Statistiken auf.

Serverparasiten

Für Kriminelle kann ein gekapertes RDP-System noch wesentlich mehr Nutzen bringen als ein bloßes Lösegeld für verschlüsselte Daten. Es kann zum Beispiel Ausgangspunkt einer großflächigeren Attacke sein, mit denen der Angreifer Zugriff auf ein ganzes Netzwerk von Geräten erlangt – die Basis für die Verschlüsselung oder den Diebstahl viel größerer und wertvollerer Datenmengen. Bei den oben zitierten Fällen ging es den Hackern scheinbar um solch groß angelegte Angriffe. Die Methoden, die solche Attacken erfordern, sind dabei weder besonders komplex noch schwer in Erfahrung zu bringen.

Hat er einmal Zugriff auf ein System erhalten, versucht der Angreifer im Allgemeinen, so viel wie möglich darüber herauszufinden, wie es sich für seine Zwecke nutzen lässt. Beispielsweise, welche Verbindungen dieser Rechner oder Server zu anderen Systemen unterhält. Hat er den Zugriff nicht sowieso schon über die Adminrechte erlangt, kann der Kriminelle sich verschiedener Techniken bedienen, um diese nachträglich zu erlangen. Ist eine Endpoint Security-Lösung auf dem System installiert, die der Nutzer mit Adminrechten deaktivieren könnte, wird der Angreifer dies vermutlich auch tun. Damit kann er wiederum zusätzliche Software herunterladen, mit denen er das Potenzial des gekaperten Systems umfassend nutzen kann. (Anm: Reden wir von einem „Angreifer", ist damit nicht unbedingt eine Person gemeint, die vor einem Rechner sitzt und die Aktivitäten ausführt. Große Teile der Angriffe werden automatisiert durch Software ausgeführt.)

Um nicht entdeckt zu werden, versuchen Hacker, möglichst wenig Schadcode direkt auf die infizierten Systeme aufzuspielen. Stattdessen missbrauchen sie oftmals bekannte legitime Software für ihre Zwecke. Besonders beliebt sind Programme, die der eigentliche Administrator des Systems für dessen Verwaltung verwendet. Aber auch Standard-Tools des Betriebssystems können zweckentfremdet werden, um immer größeren Schaden im Netzwerk anzurichten. So werden beispielsweise PsExec und die Windows-Kommandozeile WMIC häufig verwendet, um sich lateral durch das kompromittierte Netzwerk zu bewegen. Da es sich bei diesen Tools um vielfach verwendete, legitime Programme handelt, ist ein Missbrauch nur schwer zu identifizieren. Unmöglich ist es allerdings nicht. (Im Abschnitt zu EDR-Tools werden wir auf dieses Thema noch genauer eingehen.)

Wenn sich Angreifer „lateral" durch ein Netzwerk bewegen, bedeutet das übrigens, dass sie sich zunächst Zugriff auf einen Rechner verschaffen und sich dann auf die Systeme weiterbewegen, die mit diesem verbunden sind. So können sie unzureichend abgesicherte Server übernehmen, die gar nicht im fraglichen Unternehmen stehen, aber mit der übrigen Firmeninfrastruktur verbunden sind. Die Ransomware verbreitet sich dann über diese Vernetzung und kann im schlimmsten Fall alle verbundenen Geräte erreichen.

Eine weitere Strategie von Kriminellen besteht darin, *bisher ungepatchte Schwachstellen in legitimer Software auszunutzen*, um Zugang zu einem Netzwerk zu erhalten. Das wohl beste Beispiel für die Anwendung dieser Strategie ist die Ransomware WannaCryptor, die sich über den *Exploit EternalBlue* verbreitet hatte. Dieser wiederum bediente sich einer Schwachstelle in Microsofts Server Message Block (SMB)-Protokoll. Zwar war die Sicherheitslücke bereits zwei Monate vor der groß angelegten WannaCryptor-Kampagne am 12. Mai 2017 gepatcht worden – dennoch konnte WannaCryptor mehr als 200.000 nicht aktualisierte Rechner infizieren. Dabei können die Folgen solcher Attacken durchaus lange nachhallen: Einmal mit WannaCryptor infizierte (und nicht gesäuberte) Geräte blieben lange gefährlich, weil sie Mitarbeiter (ungewollt) in Netzwerke und Netzwerkteile brachten, die Admins für bereits gesäubert hielten.

Während die oben genannten Strategien eher langfristig und großflächig angelegt sind, steht den Angreifern auch immer die Möglichkeit offen, mit relativ geringem Aufwand schnelles Geld zu machen. Haben sie einmal Zugriff auf einen Server – beispielsweise mit sensiblen Unternehmensdaten – erhalten, können sie diese schlicht stehlen, verschlüsseln und für die Freigabe ein Lösegeld fordern. Langfristige Strategien versprechen jedoch oftmals größeren Profit. Viele Urheber von Ransomware

werfen daher zumindest einen genaueren Blick auf die gestohlenen Daten, bevor sie sie verschlüsseln. Schließlich lässt sich nicht sagen, welche Möglichkeiten für kriminelle Aktivitäten sich daraus vielleicht ergeben.

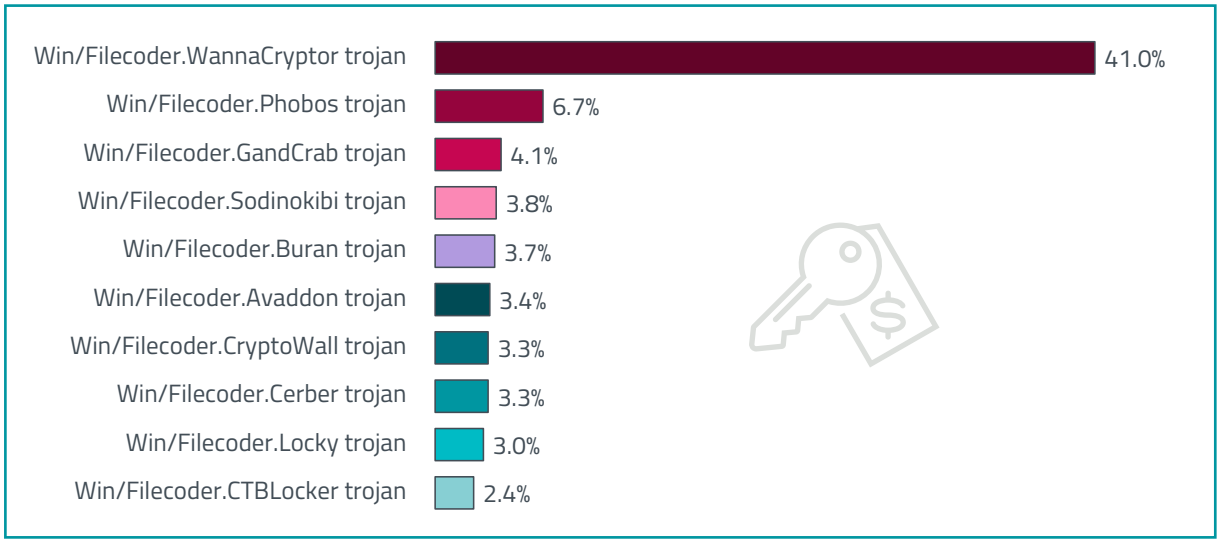

Abbildung 4: Auch vier Jahre nach der ursprünglichen Kampagne im Jahr 2017 ist WannaCryptor eine der am häufigsten beobachteten Ransomware-Familien (Quelle: *ESET Threat Report T1, 2021*)

Abwehr RDP-basierter Ransomware

Glücklicherweise ist es mit nur sehr geringem Aufwand möglich, RDP-Server gegenüber unerlaubtem Zugriff zu schützen: sei es zur proaktiven Abwehr von Ransomware oder anderen Formen des Missbrauchs. Der folgende Abschnitt erläutert, welche Abwehrstrategien sich wie umsetzen lassen. Technische Details zum Vorgehen finden sich im Abschnitt *„Absicherung von RDP gegenüber Ransomware"*.

Heutzutage regeln Sicherheitsrichtlinien von Unternehmen Zugriffe auf das Netzwerk von außen genauestens. So gibt es vermutlich auch in Ihrem Unternehmen die Vorgabe, dass alle RDP-Zugriffe nur per VPN möglich sind, dass sie durch eine Multi-Faktor-Authentifizierung abgesichert werden müssen, nur von bestimmten Personen und nur auf besonders geschützten Systemen durchgeführt werden dürfen, laufend gepatcht und überwacht sowie durch eine Firewall geschützt werden müssen. Regelmäßige Backups sind ebenfalls meist verpflichtend.

Diese Regeln, seien sie geplant oder bereits implementiert, bieten allerdings keine Garantie, dass Ihr Remote-Zugang nicht doch gehackt werden kann. Auch hier geht es wieder nicht ohne die Kooperation Ihres Teams: Stellen Sie sicher, dass jeder einzelne Mitarbeiter alle Sicherheitsvorgaben verinnerlicht hat und strikt einhält. Unabhängig von allen Schutzvorkehrungen müssen Sie Verhaltensregeln für den Fall aufstellen, falls ein Angriff erfolgreich sein sollte.

Grundvoraussetzung für eine funktionierende Absicherung Ihrer IT-Infrastruktur ist der vollständige und laufend aktuelle Überblick über alle mit dem Internet verbundenen Systeme. Es mag trivial klingen, aber wenn Sie nicht wissen, dass sich ein Gerät in Ihrem Netzwerk befindet, können Sie es auch nicht absichern. Unsere Erfahrungen zeigen übrigens: Dieser Fall ist gar nicht so selten. Vielfach wussten Sicherheitsverantwortliche vor einer Attacke über bestimmte Rechner nicht, dass diese überhaupt Teil des Unternehmensnetzwerks waren.

Damit Ihnen das nicht passiert, können Sie verschiedene Vorkehrungen treffen. Entscheidend ist, dass es zum Beispiel für externe Dienstleister oder Mitarbeiter nicht möglich sein sollte, einen physischen oder virtuellen Server mit dem Unternehmensnetzwerk bzw. dem Internet zu verbinden. Einzige Ausnahme:

Dieser ist vernünftig konfiguriert. Und zwar, bevor der Server online geht. Das gilt umso mehr für diejenigen, die RDP über einen Domain Admin-Account verwenden.

Haben Sie nun einen Überblick über alle mit dem Internet verbundenen Geräte in Ihrem Netzwerk, müssen Sie herausfinden, welche per Remote Access erreichbar sind und ob dies in jedem einzelnen Fall überhaupt notwendig ist. Ist dem so, sollten diese Nutzerzugänge mit besonders starken und möglichst langen Passwörtern geschützt werden. 15 Zeichen sind das Minimum. Diese lassen sich übrigens am besten über *Passphrasen* merken. Passwörter mit ausreichender Länge müssen nicht allzu komplex sein. Die Verpflichtung zu Sonderzeichen und ähnliche Vorgaben verleiten Nutzer im Zweifelsfall nur zu unzureichender Passworthygiene. Haben Sie die betroffenen Zugänge entsprechend abgesichert, sollten Sie zusätzlich prüfen, ob das Gerät nicht alternativ im internen Netzwerk platziert oder per VPN erreicht werden kann.

Muss ein Gerät über einen öffentlichen Internetzugang via RDP zugänglich sein und kann kein VPN verwendet werden, sollten Sie zumindest eine Multi-Faktor-Authentifizierung einrichten. Dann beruht der Schutz nicht allein auf einem einzigen Passwort. Die verwendete MFA sollte auf keinen Fall SMS-basiert sein, denn diese Art der Authentifizierung lässt sich auf verschiedenste Arten missbrauchen. Dies zeigte sich unter anderem bei Angriffen auf europäische Banken, bei denen dieses System über viele Jahre im Einsatz war.

Kann – zum Beispiel aus Budgetgründen – keine MFA implementiert werden, sollten Sie zumindest vermeiden, dass Hacker Zugangsdaten durch schlichtes Raten in Erfahrung bringen können. Setzen Sie eine Maximalanzahl für erfolglose Login-Versuche. Wird sie überschritten, sind für eine begrenzte Zeit (z.B. drei Minuten) keine weiteren Versuche möglich. Abbildung 5 zeigt, wie sich dies in der Praxis auf einem Windows-Rechner einstellen lässt.

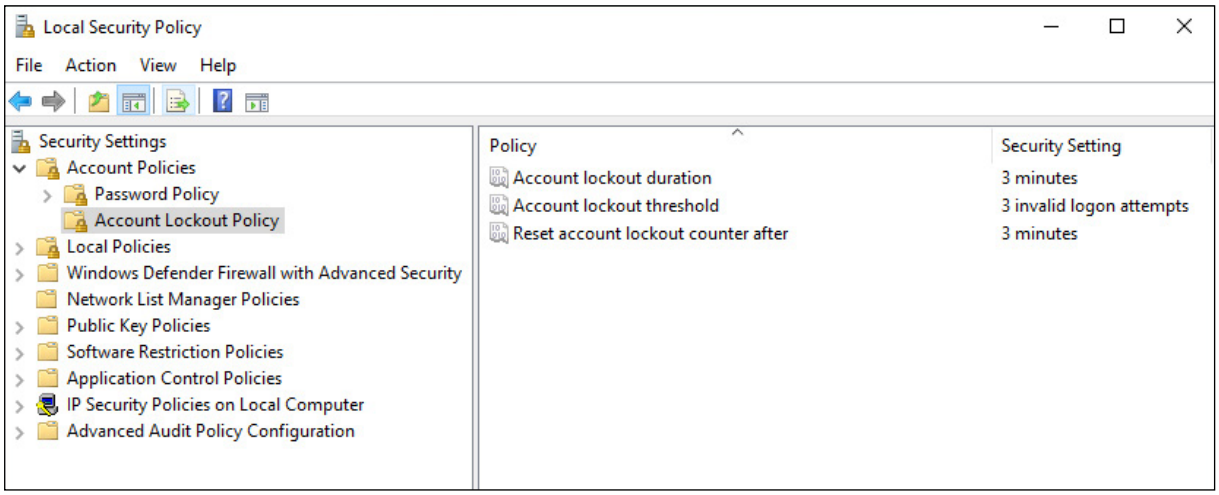

Abbildung 5: Regeln für Kontensperrung

Eine weitere, besonders einfache Maßnahme ist es, statt des üblichen Port 3389 einen anderen für die Verbindung des Servers mit dem World Wide Web zu verwenden. So erschweren Sie es potenziellen Angreifern, diesen als mögliches Ziel ausfindig zu machen. Die Änderung geschieht über die Systemeinstellungen. Zusätzlich müssen Sie auch die Firewall-Einstellungen neu konfigurieren, um sie den Änderungen anzupassen. Vergessen Sie auch nicht, dass diese „Tarnung" keinen wirklich effektiven Schutz bietet und immer nur in Verbindung mit anderen Methoden zur RDP-Absicherung sinnvoll ist. (Der Abschnitt „Absicherung von RDP gegenüber Ransomware" erläutert das Vorgehen im Detail.)

Grundsätzlich gilt: Alle von außen erreichbaren Systeme sollten regelmäßig gepatcht, ihr Schutz geprüft und gegebenenfalls erweitert werden. Sorgen Sie zudem dafür, dass alle nicht benötigten Dienste

und Komponenten entfernt oder deaktiviert werden und alle Einstellungen der Maßgabe maximaler Absicherung entsprechen.

Auf Windows-Systemen lassen sich beispielsweise Einschränkungen für Software so setzen, dass Dateien nicht aus den Ordnern AppData und LocalAppData ausgeführt werden können. Dieses typische Verhalten von Malware wird dadurch gestoppt. Zusätzliche Sicherheit schafft die Windows-Anwendung AppLocker, die festlegt, welche Apps und Dateien Mitarbeiter auf ihren Rechnern ausführen können.

Nicht zuletzt schützt ein umfassendes und ausreichend getestetes Backup- und Wiederherstellungssystem Ihre Unternehmenssysteme vor RDP-Ransomware. Da es sich hierbei um einen zentralen Aspekt bei der Absicherung von Unternehmensnetzen handelt, werden wir später noch einmal genauer darauf eingehen.

Zunächst jedoch wenden wir uns den drei Angriffsvektoren E-Mail, Lieferkette (Supply Chain) und ungepatchte Schwachstellen zu.

Ein weiteres Einfallstor: Das SMB-Protokoll

Das Server Message Block (SMB)-Protokoll wird vor allem dazu verwendet, um Dateien in Unternehmensnetzwerken zu teilen oder Drucker in das Netzwerk einzubinden. Gleichzeitig stellt es ein beliebtes Einfallstor für Malware dar, insbesondere Ransomware. Im ersten Drittel des Jahres 2021 *verhinderten ESET Security-Lösungen* allein 335 Millionen Brute Force-Angriffe gegen öffentlich zugängliche SMB-Dienste. Dies bedeutet einen Rückgang der Attacken um 50% im Vergleich zu den letzten vier Monaten des Vorjahres – auf die leichte Schulter sollten Sie die Gefahr durch SMB-Angriffe aber dennoch nicht nehmen. Schließlich verbreitet sich die bekannte Ransomware WannaCrypto (aka WannaCry), die allein für 41 Prozent aller beobachteten Ransomware-Angriffe in besagtem ersten Drittel 2021 verantwortlich war, häufig über Verbindungen auf Basis des unsicheren SMBv1-Protokolls.

Die folgenden Hinweise helfen Ihnen, sich gegen Angriffe per SMB zu schützen:

- Deaktivieren Sie die veralteten Protokolle *SMBv1 und SMBv2*. Bedenken Sie, dass einige Netzwerkgeräte eventuell mit diesem Protokoll arbeiten und entsprechend neu konfiguriert werden müssen.
- Arbeiten Sie nur mit der neuesten Version des SMB-Protokolls (aktuell SMBv3).
- Konfigurieren Sie die Einstellungen für Gruppenrichtlinien so, dass die Kommunikation über SMB von beiden Seiten digital signiert wird, damit sich kein potenzieller Angreifer in die Kommunikation einklinken kann.
- Schließen Sie die TCP-Ports 445 und 139 sowie die UDP-Ports 137 und 138. So kann nicht von außen auf die in Ihrem Netzwerk verwendeten SMB-Protokolle (egal welche Version) zugegriffen werden.

Absicherung von RDP gegenüber Ransomware

Folgende Strategien und Techniken können helfen, RDP in Ihrem Netzwerk sicherer zu machen:

1. **Gerätedokumentation**
   Listen Sie alle im Unternehmen mit dem Internet verbundenen Geräte auf und sorgen Sie dafür, dass diese den Security-Verantwortlichen bekannt sind. Stellen Sie sicher (z.B. durch Standardprozesse), dass alle neuen Geräte in diese Liste aufgenommen werden.
2. **Risikominimierung**
   Denken Sie daran, dass nur diejenigen Geräte direkt mit dem Internet verbunden sind, die entsprechend konfiguriert und abgesichert sind. Hinterfragen Sie, ob für das jeweilige Gerät auch eine indirekte Verbindung via VPN möglich wäre. Deaktivieren Sie RDP immer dann, wenn es nicht zwingend gebraucht wird. (Details, wie dies in den verschiedenen Windows-Versionen zu bewerkstelligen ist, finden Sie hier: *Server 2019*; *Server 2016*; *Server 2008/R2*; *Windows 10*; *Windows 8*; *Windows 7*).

3. Schutz gefährdeter Geräte

In den Fällen, in denen es auf keinen Fall ohne RDP geht und in denen kein Zugang über VPN möglich ist, sollten Sie möglichst viele der folgenden Maßnahmen implementieren:

a. Ändern Sie in regelmäßigen Abständen das Passwort des Benutzeraccounts, mit dem Sie auf dem Remote-Rechner arbeiten. Selbstverständlich sollte auch das Standard-Passwort, das häufig für Cloud-Instanzen vergeben wird, umgehend geändert werden.

b. Verwenden Sie nur starke Passwörter. (Am sichersten sind Passphrasen mit mindestens 15 Zeichen und ohne Begriffe, die in irgendeiner Weise mit Ihrer Branche, Ihrem Unternehmen, Produktnamen oder dem Nutzer zu tun haben.)

c. Legen Sie fest, nach wie vielen fehlgeschlagenen Login-Versuchen der Account automatisch für eine bestimmte Zeit gesperrt wird. So verhindern Sie, dass potenzielle Angreifer Ihr Passwort mithilfe von Brute Force erraten. In Windows legen Sie die maximale Anzahl an Fehlversuchen folgendermaßen fest: Sie gehen auf Start-->Programme-->Verwaltungstools--> Lokale Sicherheitsrichtlinie (Windows 10: Windows-Suche „Lokale Sicherheitsrichtlinie). Unter „Kontorichtlinien-->Kontosperrungsrichtlinien" sollten Sie für alle drei Unterpunkte Werte festlegen. Eine Kontosperre von drei Minuten bei drei gescheiterten Versuchen ist generell eine gute Wahl.

d. Testen Sie Patches für alle bekannten Schwachstellen und wenden Sie sie auch an. Achten Sie darauf, dass diese bekannte Ransomware-Familien wie *BlueKeep* und *EternalBlue* einbeziehen. Kann ein einzelner Rechner nicht länger gepatcht werden, planen Sie ein, ihn zeitnah zu ersetzen.

e. Arbeiten Sie mit einer Authentifizierung auf Netzwerkebene (NLA), um die Sicherheit des RDP Host-Servers zu erhöhen. Hierbei wird der Nutzer aufgefordert, sich noch vor Start der Session gegenüber dem Host-Server zu authentifizieren.

f. Ändern Sie den Standardport 3389 für RDP. Bedenken Sie aber, dass diese „Tarnung" keinen wirklich effektiven Schutz bietet und immer nur in Verbindung mit anderen Methoden zur RDP-Absicherung sinnvoll ist. Um den Port zu wechseln, ändern Sie den folgenden Registry-Eintrag: (ACHTUNG: Dies sollte nur von Nutzern mit Erfahrung mit der Windows Registry und TCP/IP durchgeführt werden): HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\PortNumber.

g. Legen Sie fest, welche öffentlichen IP-Adressen sich via RDP mit Ihrem Netzwerk verbinden können. Dies kann allerdings eine etwas mühselige Aufgabe sein, wenn Ihre Nutzer keine statischen IP-Adressen haben – zum Beispiel, weil Sie von zuhause oder unterwegs aus arbeiten.

h. Fordern Sie für die Authentifizierung von Nutzern mehr als einen Faktor. Die Faustregel lautet hier: „Etwas, das man weiß" (z.B. Nutzernamen und Passwörter), „Etwas, das man ist" (z.B. Fingerabdrücke oder die Stimme des Nutzers) und schließlich „Etwas, das man hat" (z.B. das Smartphone des Nutzers, dass einen Einmalcode empfangen oder eine Authentifizierungs-App ausführen kann). Vermeiden Sie aber unbedingt, SMS für die Authentifizierung zu verwenden. SMS-basierte Authentifizierung kann auf verschiedenste Arten missbraucht werden – und wurde es bereits mehrfach. (Wie genau, erläutert zum Beispiel *dieser Artikel*). Auf dem Markt gibt es viele gute Multi-Faktor-Authentifizierungen (darunter *ESET Secure Authentication*), die Smartphones nutzen – aber eben nicht auf Basis von SMS.

i. Verschärfen Sie Zugriffs- und Rechtebeschränkungen. Dateien sollten nicht aus den Ordnern AppData oder LocalAppData oder aus Temp (standardmäßig ein Unterordner von AppData) heraus gestartet werden können. Ebenso sollten ausführbare Dateien (.exe) nicht aus den Arbeitsverzeichnissen der verschiedenen Entpack-Programme (z.B. WinZip oder 7-zip) heraus ausgeführt werden können. Mithilfe eines guten Endpoint Security-Produkts können Sie zudem sogenannte HIPS (Host Intrustion Prevention System)-Regeln festlegen, die es nur bestimmten Anwendungen erlaubt, überhaupt auf dem fraglichen Rechner ausgeführt zu werden. Alle anderen werden automatisch blockiert.

j. Vergeben Sie starke und einmalige Passwörter für Nutzeraccounts mit Adminrechten, z.B. mithilfe des Windows-eigenen LAPS (Local Administrator Password Solution) oder einem anderen vertrauenswürdigen Passwortmanager. Zusätzlich sollte nur eine begrenzte Gruppe Nutzer überhaupt auf den Server zugreifen können, um die potenzielle Angriffsfläche so klein wie möglich zu halten.

k. Setzen Sie das Verschlüsselungslevel für Remote Desktop-Sessions für alle Verbindungen auf „hoch". Ist dies nicht möglich, setzen Sie das Verschlüsselungslevel auf den höchstmöglichen Wert.
l. Installieren Sie ein VPN-Gateway, um alle RDP-Verbindungen von außen mit Ihrem lokalen Netzwerk überwachen zu können.
m. Sichern Sie Ihre Endpoint Security mit einem Passwort, um unerlaubte Änderungen in den Einstellungen oder gar eine Deaktivierung/Deinstallation durch Unbefugte zu verhindern. (Natürlich sollte dieses Passwort ein anderes sein als das, welches Sie für Ihren RDP-Login verwenden.)
n. Aktivieren Sie Features in Ihrer Endpoint Security-Software, die *Exploits abwehren* – die also unabhängig von Signaturen erkennen und melden, wenn sich besonders häufig im Visier stehende Anwendungen *auffällig verhalten*.
o. Gibt es in Ihrem Netzwerk unsichere Rechner, die aber dennoch per RDP von außen angesprochen werden müssen, isolieren Sie sie vom Rest des Netzwerks.
p. Arbeiten alle Mitarbeiter und Zulieferer im selben Land (oder einigen wenigen Ländern), sollten Sie in Erwägung ziehen, IP-Adressen aus allen anderen Ländern (oder bestimmten) den Zugriff am VPN-Gateway zu verbieten. So schränken Sie die Liste möglicher Angreifer von vornherein ein.

RANSOMWARE VIA EMAIL

Jeder Security-Experte weiß: Cyberkriminelle tun ihren Opfern selten den Gefallen, nur den jeweils neuesten Malware-Trends nachzulaufen und dem Rest keinerlei Beachtung mehr zu schenken. Nur weil aktuell Ransomware-Angriffe vor allem über extern zugängliche Server erfolgen, heißt das nicht, dass Sie andere potenzielle Einfallstore nicht trotzdem im Auge behalten sollten. Noch immer werden E-Mails mit Malware-verseuchten Anhängen versendet, die dann den Weg für spätere Ransomware-Attacken ebnen.

Eine beliebte Strategie von Kriminellen ist es, Downloader in E-Mail-Anhängen zu verbergen, die dann Malware auf dem Rechner des Empfängers installieren. Zusätzlich dienen verseuchte E-Mails als Sprungbrett für größer angelegte Angriffe auf Unternehmensnetzwerke. Haben die Kriminellen einen Zugang zum Unternehmensnetzwerk erhalten, können sie jederzeit wertvolle Daten stehlen oder verschlüsseln und – wie bei Ransomware-Angriffen per RDP – hohe Summen an Lösegeld fordern.

Gleichzeitig gilt die E-Mail-Kommunikation von Unternehmen als ein beliebter Angriffsvektor für Botnetze wie beispielsweise Trickbot, Qbot oder Dridex. Sie bedienen sich Microsoft Office-Dokumenten mit kompromittierten Makros, um Zugang zu Unternehmensnetzwerken zu erhalten. Das Ziel ist auch hier, zu einem späteren Zeitpunkt mithilfe von Ransomware Lösegeld zu erpressen. Viele der bisher damit in Zusammenhang stehenden Kampagnen standen in enger Verbindung zu Botnetzen wie *Emotet* und Qbot, *Trickbot*, *Ryuk* und Conti, *Dridex* und FriedEx (aka BitPaymer), *Nemucod* mit *Avaddon*, Dridex, Ursnif und Trickbot sowie *SmokeLoader und Zloader* mit LockBit und Crysis.

Im Jahr 2021 gelang es den Behörden, *Emotet* aus dem Verkehr zu ziehen. Infolge dessen sank die Zahl der per Mail versendeten Downloader beträchtlich. In den ESET Threat Reports beschreiben wir die Auswirkungen von Emotet vor und nach der erfolgreichen Bekämpfung: *ESET Threat Report erstes Drittel 2021*, *ESET Threat Report viertes Quartal 2020* und *ESET Threat Report drittes Quartal 2020*.

Nichtsdestotrotz blieben und bleiben im Jahr 2021 infizierte Makros eine der häufigsten Angriffsvarianten für Attacken per Mail. Im Januar – vor der Unschädlichmachung Emotets – hatte die Anzahl der E-Mails mit verseuchten Office-Anhängen, die zu Dridex- und Emotet-Downloadern führten, sogar noch einmal einen Boom erlebt.

Ein weiteres verbreitetes Botnetz, *Trickbot*, konnte im Oktober 2020 entscheidend gestört werden. Dies scheint den Betrieb allerdings nur für gewisse Zeit verlangsamt zu haben. Schon im Januar 2021 starteten die Urheber eine *weitere Phishing-Kampagne*. Das Ziel: vor allem Großkanzleien und Versicherungsunternehmen in den USA. Hier scheint also noch viel Arbeit nötig zu sein, um Trickbot wirklich dauerhaft unschädlich zu machen.

Doch was können nun Sie als Entscheider tun, Ihr Unternehmen gegen Ransomware via E-Mail zu schützen? Bereits ein einzelner, gut konfigurierter Spam- und Phishingfilter bildet die erste wichtige Verteidigungslinie gegenüber Ransomware. Viele Unternehmen haben einen solchen bereits im Einsatz. Es war schon vor den aktuellen, groß angelegten Ransomware-Kampagnen sinnvoll, Mitarbeiter vor Spam und Phishing zu schützen.

Eine weitere einfache und wirkungsvolle Maßnahme ist, grundsätzlich solche Anhänge zu blockieren, die in Ihrem Unternehmen im Allgemeinen nicht verwendet werden. Wie praktikabel diese Herangehensweise ist, hängt natürlich von Ihrem Unternehmen ab und erfordert möglicherweise umfassendere Prozessänderungen. Beispielsweise sind es Ihre Mitarbeiter möglicherweise gewohnt, einander Excel- und Word-Dateien per E-Mail zu schicken. Die Umstellung auf File-Sharing-Lösungen oder weitere sichere Kollaborationstools kann sinnvoll sein, stößt aber eventuell auf Widerstände. Bevor Sie also grundsätzlich „althergebrachte" Arbeitsweisen verbieten, unterstützen Sie Ihre Mitarbeiter zunächst beim Übergang zu anderen, für sie eventuell neuartigen Methoden.

Stellen Sie in jedem Fall sicher, dass auf den Rechnern jedes Mitarbeiters eine leistungsfähige Endpoint Security-Lösung installiert ist. Diese hindert den Einzelnen zum Beispiel daran, bestimmte Webseiten zu besuchen, von denen bekannt ist, dass sie Malware verbreiten. Auch ein Filter für bestimmte Web-Inhalte kann hier gute Dienste leisten, indem er Webseiten mit bestimmten Inhalten von vornherein blockiert, z.B. solche, die keinen Bezug zur Arbeit des Mitarbeiters haben.

Die verwendete Security-Lösung sollte dabei grundsätzlich zentral verwaltet werden, um Sicherheitsrichtlinien erfolgreich um- und durchzusetzen. So lässt sich verhindern, dass Mitarbeiter die Security-Lösung eigenständig deaktivieren oder nicht autorisierte Wechselmedien benutzen. Sorgen Sie dafür, dass Sie immer die neueste Version der Endpoint Security verwenden und alle verfügbaren Updates einspielen. Kann die Lösung mit der Cloud verbunden werden, sollten Sie diese Verbindung aktivieren. Auf Basis von Daten aus der Cloud kann die Lösung viel schneller selbst auf neuartige Bedrohungen reagieren. Viele ESET Produkte interagieren mit der Cloud – die Komponente nennt sich *LiveGrid® oder in einigen Fällen ESET Dynamic Threat Defense*.

Managed Service Provider (MSPs) sollten die ESET Produkte Ihrer Kunden so konfigurieren, dass Ransomware möglichst nicht eindringen kann. Einige Tipps für die Konfiguration finden sich *hier*.

Denken Sie daran, Betriebssysteme und Anwendungen regelmäßig und umfassend zu patchen, um Ransomware-Attacken per Mail oder Drive-by-Downloads zu verhindern. Auch durchdachte Sicherheitseinstellungen spielen eine wichtige Rolle. So kann es sinnvoll sein, Microsoft Office-Makros für bestimmte Nutzergruppen komplett zu deaktivieren, um die Angriffsfläche für Ransomware weiter zu minimieren. Das macht allerdings nur dann Sinn, wenn Ihre Unternehmensabläufe nicht auf Makros angewiesen sind.

Eines steht außer Frage: Die IT-Sicherheit eines Unternehmens ist nur so gut wie jedes einzelne Element – und dazu gehört auch das Bewusstsein jedes einzelnen Mitarbeiters. Entsprechend wichtig sind regelmäßige, aktuelle und praxisnahe Cybersecurity-Trainings. Oder wie wir es in unserem kostenfreien Cybersecurity *Awareness Training* formulieren: „Probleme mit Malware in Unternehmen lassen merklich nach, wenn die Mitarbeiter wissen, worauf sie bei Mails achten müssen und woran sie Phishing und potenzielle Malware erkennen."

Jedem einzelnen Mitarbeiter muss bewusst sein, dass bei verdächtigen Mails oder Anhängen sofort der IT-Helpdesk oder das Security-Team zu informieren sind. So wird nicht nur verhindert, dass Malware tatsächlich ins Unternehmensnetzwerk gelangt. Die Informationen aus solchen Meldungen helfen auch, Spamfilter besser zu kalibrieren, Content-Filter zu schärfen und Firewalls sowie andere Sicherheitsmechanismen zu verbessern.

RANSOMWARE-ATTACKEN ÜBER DIE SUPPLY CHAIN

Ein weiterer Angriffsvektor, der nähere Betrachtung verdient, ist die Lieferkette von Softwareprodukten, die sogenannte Supply Chain. In den Anfangsjahren von Software und Malware verbreiteten sich Computerviren vor allem über Disketten, den Hauptverkehrsweg legitimer Software. Entsprechend kam es vor, dass sich Malware bereits auf neu gekauften Datenträgern befand oder auf Disketten mit Probeversionen, wie sie häufig Computermagazinen beigelegt waren.

Der heutige Infektionsweg kann sehr ähnlich sein: Wie *ESET Forscher 2017* feststellten, nutzte die *NotPetya/DiskCoder.C-Malware* eine legitime Buchhaltungssoftware, um in Systeme einzudringen. Die Angreifer kaperten den Update-Server des Herstellers und fügten dem korrekten Update-Code ihren schädlichen hinzu. Nutzer, die das Update installierten, brachten gleichzeitig eine Backdoor auf ihren Rechner, mit deren Hilfe wiederum Ransomware auf das System gelangen konnte. Um sich vor diesen und ähnlichen Angriffen zu schützen, tun Unternehmen gut daran, eine zuverlässige Endpoint Security-Lösung und zusätzlich EDR-Tools einzusetzen.

In Anbetracht der komplexen Folgen und der umfangreichen nötigen Gegenmaßnahmen sind Supply Chain-Angriffe immer wieder Thema sowohl bei Forschern als auch Security-Verantwortlichen. Am 02. Juli 2021 zum Beispiel war die *IT-Management-Software Kaseya*, die häufig von Managed Service Providern eingesetzt wird, von einer Ransomware-Attacke betroffen. Dabei drang der Trojaner Win32/Filecoder. Sodinokibi.N über eine bislang unbekannte Schwachstelle in die Systeme ein. Glücklicherweise reagierte Kaseya umgehend. Um andere Unternehmen in der Lieferkette zu schützen, wurden sofort weitere Analysen eingeleitet und insbesondere potenziell betroffene Unternehmen benachrichtigt. Kaysea riet ihnen, möglicherweise betroffene lokale VSA-Server sofort herunterzufahren.

Auch die ESET Forschung zeigt: Supply Chain-Attacken nehmen immer mehr zu, die Ausmaße werden teils immer dramatischer. Gleich *mehrere ESET Paper* berichten von Fällen, bei denen dieser Angriffsvektor genutzt wurde. Zwischen November 2020 und Februar 2021 konnten ESET Forscher allein vier Fälle von Supply Chain-Angriffen beobachten – im Vergleich zu den Vorjahren eine immense Zahl.

Die effektivste Abwehr gegenüber solchen Attacken ist es, Software stets aktuell zu halten, eine zuverlässige Endpoint Security-Lösung zu installieren und *EDR-Produkte* einzusetzen. Nicht zuletzt sollten Sie aber auch dringend alle Mitarbeiter anhalten, keine unbekannten Webseiten zu besuchen – egal, welche E-Mail sie dazu auffordert.

RANSOMWARE-ANGRIFFE ÜBER UNGEPATCHTE SCHWACHSTELLEN

Cyberkriminelle bedienen sich aller Arten von Schwachstellen, bekannten wie unbekannten. Bisher unentdeckte sind vor allem für Kriminelle mit großen finanziellen und personellen Ressourcen interessant. Dazu zählen APT-Gruppen und von Regierungen beauftragte oder unterstützte Akteure. Dabei wären schon bekannte Schwachstellen Aufgabe genug für Security-Admins, Forscher und Unternehmen.

Zur Verdeutlichung: Der EternalBlue-Exploit ist bereits seit 2017 bekannt und seine Varianten spielen noch immer eine wichtige Rolle in der Bedrohungslandschaft. Und auch Exploits des – wenn auch veralteten, aber trotzdem offensichtlich vielfach verwendeten – SMBv1-Protokolls von Microsoft sind erstaunlich präsent. (Siehe auch Abschnitt „Serverparasiten".)

Auch die Tatsache, dass WannaCryptor (aka WannaCry) und ähnliche Malware nicht von der Bildfläche zu verschwinden scheinen, deutet vor allem auf eines hin: Viele Unternehmen und Organisationen sind noch immer nicht an dem Punkt, an dem ihr Update- und Patchmanagement wirklich verlässlich und auf die aktuelle Bedrohungslage ausgerichtet ist.

Gleichzeitig wird besagte Bedrohungslage jeden Tag komplexer – mit ihr aber auch die Auswahl an Tools, Unternehmen abzusichern. Diese bringen gleichzeitig neue Ansprüche mit sich, darunter das Auffinden von Schwachstellen in eben diesen Produkten und die Implementierung eines nachhaltigen Patch-Managements.

Insbesondere die immer verbreitetere Nutzung – und teilweise Abhängigkeit – von VPN stellt Entscheider und Administratoren vor neue Aufgaben. Zwei Beispiele zeigen dies besonders deutlich: Sowohl im VPN-Dienst von *Pulse Secure* als auch in dem von *Fortinet* wurden Schwachstellen nachgewiesen, über die Ransomware in die Systeme von Kunden eindringen konnte. So wichtig und effektiv die Nutzung von VPN gerade für große Organisationen ist: Ohne laufende Updates und Patches werden die Dienste schnell zum Sicherheitsrisiko für das gesamte Unternehmen. Zudem sollten VPN-Dienste nur über eine Multi-Faktor-Authentifizierung zugänglich sein, um den Zugriff durch Dritte zu verhindern. Treten Unregelmäßigkeiten auf – zum Beispiel der Verdacht, dass Zugangsdaten gestohlen worden sind – müssen entsprechende Maßnahmen folgen. So aufwendig dies auch ist: In solchen Fällen hilft nur das Zurücksetzen von Accounts (gegebenenfalls allen), um die Sicherheit zuverlässig wiederherzustellen.

Aber auch andere Kollaborationstools und weitere Werkzeuge zur Steigerung der Produktivität von Organisationen stellen ganz eigene Ansprüche an Security-Verantwortliche. Im März 2021 konnte ein Anstieg an Malware-Aktivitäten beobachtet werden, die zu entsprechenden Reaktionen bei Herstellern von IT-Security und der Cybersecurity-Branche allgemein führten. Der Grund: Microsoft hatte mehrere „Notfall-Updates" veröffentlicht, nachdem bisher unbekannte Schwachstellen in Microsoft Exchange Servern von 2013, 2016 und 2019 entdeckt worden waren. Diese wurden von Cyberkriminellen umgehend ausgenutzt, um Zugriff auf Exchange-Server zu erhalten und so E-Mails und Daten zu stehlen sowie Malware auf fremde Systeme aufzuspielen. Letztere sollte dabei als Einfallstor für spätere, groß angelegte Angriffe dienen.

Letztlich folgten auf die Veröffentlichung der Patches Angriffe *von mindestens 10 APT-Gruppen* auf Exchange-Server. ESET Forscher versuchten herauszufinden, wie viele Organisationen von den Angriffen betroffen gewesen sein könnten. Die wichtige Frage war: Auf wie viele Server hatten die Angreifer nun möglicherweise für spätere Attacken Zugriff erhalten und hatten sie sich womöglich sogar Admin-Rechte verschafft?

Wie schon im Abschnitt zu Supply Chain-Angriffen berichtet, waren vom Ransomware-Angriff auf Kaseya mehr als 50 MSPs mit insgesamt mehr als 1.000 Endkunden *betroffen*. Die Angreifer bedienten sich dabei mehrerer bisher unbekannter Schwachstellen – darunter CVE-2021-30116 –, um die verbreitete IT-Management Software Kaseya VSA zu kompromittieren. Nach eigener, eventuell übertriebener Aussage konnten die Kriminellen so in mehr als eine Million Systeme eindringen. Die ESET Telemetrie-Daten für diesen Vorfall sprechen von Opfern in 17 Ländern, darunter Großbritannien, Südafrika, Kanada, Deutschland und die USA.

Zwar hielten sich die Folgen dieses Angriffs aufgrund der schnellen Reaktion Kaseyas trotz allem in Grenzen. Dennoch ist eine solche Attacke grundsätzlich fatal und verursachte in diesem Fall schwerwiegende Folgen für die nachfolgenden Teile der Lieferkette. Selbst Unternehmen, die nur entfernte Verbindungen zu Kaseyas VSA-Plattform hatten, waren hiervon betroffen. Am 02. Juli 2021 musste der schwedische Lebensmitteleinzelhändler Coop etwa 500 Filialen vorübergehend schließen. Der *Dienstleister für die Abwicklung von Zahlungen* und den Betrieb der Kassensysteme hatte mit Kaseya gearbeitet. Damit wurde Coop eines der größten, indirekt vom Angriff auf Kaseya betroffenen Unternehmen. Deren Unternehmensvorgänge hingen von einem Dienstleister ab, welcher wiederum aufgrund der Attacke seine Server hatte herunterfahren müssen.

In Anbetracht der Tragweite solcher Angriffe scheint es höchste Zeit, dass sich nicht nur IT-Entscheider eingehender als bisher mit der Bedrohungslandschaft und den möglichen Folgen auf Unternehmensabläufe auseinandersetzen.

Weitere Informationen zu einigen der bekanntesten Schwachstellen finden sich hier:

- *Kaseya VSA*
- *Pulse Connect Secure*
- *Citrix Hypervisor*
- *Fortinet VPN*
- Microsoft Exchange Server — Siehe Beispiel in ESETs aktuellem *Threat Report*.
- *Citrix Application Delivery Controller and Gateway*
- *Microsoft Office Common Controls*
- *Windows Win32k*
- *Accellion File Transfer Appliance*

SEGMENTIERUNG UND AUSLAGERUNG IN DIE CLOUD

Unabhängig davon, welches Einfallstor eine Ransomware ausnutzt: Hat sie es einmal in das Unternehmensnetzwerk geschafft, wird sie sehr wahrscheinlich versuchen, so viele Rechner wie möglich zu infizieren. Um dem proaktiv entgegenzuwirken, bietet es sich an, die Anzahl der Rechner in einem Verbund möglichst klein zu halten. Hierfür gibt es verschiedene Ansätze, einer davon ist die Aufteilung des Netzwerks in kleinere Segmente.

Wir können hier nicht im Detail über Netzwerkarchitekturen sprechen, zumal die Segmentierung eines Netzwerks sich nicht ohne größeren finanziellen und personellen Aufwand durchführen lässt. (Dieser *KPMG-Report* bietet ausführlichere Informationen zum Thema.)

Festzuhalten ist, dass Unternehmen um die Vor- und Nachteile ihrer aktuellen Netzwerkarchitektur wissen sollten, um sie gegebenenfalls optimieren zu können. Schon ein einfaches, interviewbasiertes Audit kann wichtige Einblicke geben. Entscheidende Fragen sind beispielsweise „Wie komme ich von hier nach dort?“ und „Wie wird verhindert, dass jemand von dort hierherkommt?“

In den letzten Jahren hat die Beliebtheit cloudbasierter Systeme auch in der EU stark zugenommen. Die Architektur von Netzwerken wird hierdurch dezentralisiert, wichtige Daten extern gelagert. Dies allein bietet in sich keinen Schutz gegenüber Ransomware, auch wenn weniger seriöse Anbieter dies teilweise behaupten. Aufgrund der geringen Kosten, die das Aufsetzen eines Cloud-Servers verursacht, drängen viele Anbieter in den Markt – und vernachlässigen vielfach die Sicherheit. Entsprechend sind auch Cloud-Server für Kriminelle zu äußerst attraktiven Zielen geworden. Eines ist klar: Die Auslagerung von Unternehmens-IT in die Cloud entbindet Unternehmen nicht von der Verantwortung, hieb- und stichfeste Sicherheitskonfigurationen zu implementieren. Gleichzeitig muss die Cloud in umfassende Backup- und Wiederherstellungsframeworks eingebunden werden.

PATCHING UND BACKUPS: GRUNDLEGENDER SCHUTZ VOR RANSOMWARE

Regelmäßige Updates und Backups sind und bleiben zentral für die Abwehr von Ransomware aller Art. Updates und Patches stellen sicher, dass bekannte Sicherheitslücken geschlossen sind und dass – sollte Ransomware es doch einmal schaffen einzudringen – sie zumindest nur geringen Schaden anrichten kann.

Zugleich ist wohl jedem Systemadministrator schmerzlich bewusst, dass die Verwaltung von Patches eine komplexere Aufgabe darstellt, als es auf den ersten Blick scheint. Updates und Patches für Anwendungen und Betriebssysteme müssen vor dem Ausrollen getestet werden, weil bestehende Abhängigkeiten durch die Aktualisierung gestört werden könnten. Der Aufwand erscheint jedoch gerechtfertigt, bedenkt man die Unsummen, die erfolgreiche Ransomware-Angriffe ein Unternehmen kosten können.

Ein durchdachtes und sorgfältig verwaltetes Backup- und Wiederherstellungssystem ist elementar wichtig. Es bildet die Grundlage aller Wiederherstellungsmaßnahmen, falls es Ransomware – auf welchem Weg auch immer – doch einmal ins Unternehmensnetzwerk schafft. Und das System sorgt dafür, dass wichtige Geschäftsabläufe weiterlaufen können. Zugleich sollten Sie aber nicht vergessen, dass sich Ransomware-Angriffe nicht selten über einen längeren Zeitraum erstrecken und die Malware in dieser Zeit ebenfalls Backups von sich erstellt. Diese erschweren wiederum die Wiederherstellung. Backups sind keineswegs eine statische Verteidigungslinie, sondern müssen fortlaufend überwacht und verwaltet werden. Stellen Sie zudem sicher, dass der Wiederherstellungsprozess regelmäßig getestet wird.

Glücklicherweise sind die Möglichkeiten für umfassende Backups und Wiederherstellungsmethoden aktuell vielfältiger denn je. Dies gilt vor allem dank der Möglichkeit, Daten in die Cloud zu verlagern. Im Gegenzug gibt es so viele Daten wie nie zuvor, die längst nicht mehr nur von Unternehmensrechnern vor Ort aus gesichert werden müssen. Entsprechend groß ist die potenzielle Angriffsfläche, die durch Backups abgesichert werden muss. Und das, ohne ein einziges Gerät zu vergessen.

Den Experten von Xopero, Mitglied der *ESET Technology Alliance*, zufolge umfasst eine gute Backup-Strategie alle Daten und Systemzustände auf allen Endpoints, Servern, E-Mail-Postfächern, Netzlaufwerken, Mobilgeräten und VMs.

Hier ausführlich auf die einzelnen Elemente einer unternehmensweiten Backup- und Wiederherstellungsstrategie einzugehen, würde den Rahmen dieses Papers sprengen. Behalten Sie jedoch in jedem Fall im Hinterkopf, dass eine solche Strategie heute wichtiger ist denn je. Der Schutz vor Ransomware markiert dabei nur einen Punkt in einer langen Liste von Gründen, warum Unternehmen dieses Element ihrer IT-Infrastruktur keineswegs vernachlässigen sollten.

Nichtsdestotrotz gibt es Ransomware-spezifische Punkte, die Sie beim Planen Ihrer Backup-Strategie bedenken sollten: Sind Datenspeicher „always on", sind darauf abgelegte Inhalte leichter angreifbar. Ebenso wie auf lokalen und anderen mit dem Netzwerk verbundenen Datenspeichern kann Ransomware dort leicht Zugriff erlangen und wichtige Daten verschlüsseln.

Offsite-Speicher sollten daher:

- nicht dauerhaft und unhinterfragt online sein
- (wenn sie online sind) Daten sicher und umfassend davor schützen, unbemerkt verändert oder gelöscht zu werden
- auch ältere Backup-Versionen speichern und vor nicht autorisiertem Zugriff schützen, sodass selbst bei Zerstörung jüngerer Backups zumindest einige Daten wiederhergestellt werden können
- Anwender schützen, indem genau dargelegt wird, welche Pflichten der Server-Provider innehat, was mit den Daten passiert, wenn der Provider in Insolvenz geht etc.

Auch wenn sie etwas aus der Mode gekommen sind: Unterschätzen Sie nicht, wie nützlich und einfach nicht wiederbeschreibbare Medien (CD-ROMs, DVDs …) als Mittel zur Archivierung von Daten sein können. Nicht zuletzt sind diese schwer zugänglich für Ransomware.

Zusätzlich gibt es unzählige weitere Gründe wie Naturkatastrophen, Hardwaredefekte oder Anwenderfehler, warum Ihr Unternehmen ein umfassendes Sicherungs- und Wiederherstellungssystem implementieren sollte.

UND WIE REAGIERT MAN NUN AUF RANSOMWARE?

Sich nur vor dem Eindringen von Ransomware zu schützen, reicht natürlich nicht aus. Jedes Unternehmen muss auch in der Lage sein, auf Schadsoftware zu reagieren, die es allen Abwehrstrategien zum Trotz in das Netzwerk geschafft hat. Sicherheitsvorgaben bilden eine robuste Basis, die für das gesamte Unternehmen auf allen Ebenen gelten und regelmäßig entsprechend der neuesten Bedrohungen aktualisiert werden. Die Richtlinien sollten folgende Fragen beantworten:

- Wer ist zu benachrichtigen, wenn Mitarbeiter verdächtige Dateien oder Vorgänge beobachten?
- Wie wird mit Lösegeldforderungen umgegangen?
- Wer ist verantwortlich für eventuelle Zahlungen/Zahlungsverhandlungen in Bezug auf Lösegelder? Ziel ist dabei, grundsätzlich folgende Probleme zu vermeiden:
  - Mitarbeiter melden Vorfälle nicht aus Angst vor negativen persönlichen Konsequenzen,
  - IT-Verantwortliche zahlen Lösegelder, um langwierige Wiederherstellungsprozesse zu umgehen,
  - Informationen über tatsächliche oder vermeintliche Ransomware-Angriffe gelangen unkontrolliert an die Öffentlichkeit.
- Welche nächsten Schritte müssen im Fall von Datenlecks eingeleitet werden?
- Welche Vorgaben sind einzuhalten, wenn betroffene Geräte vom Netz genommen werden sollen? Wer entscheidet darüber? Bedenken Sie, dass auf betroffenen Geräten wichtige Informationen zur nachträglichen Untersuchung des Vorfalls vorhanden sein könnten. Ein Herunterfahren der betroffenen Rechner oder Server könnte diese unwiederbringlich zerstören – was wiederum mögliche rechtliche Konsequenzen nach sich ziehen kann.

Nachdem Sie die Sicherheitsrichtlinien in Bezug auf Ransomware aktualisiert haben, sollten Sie dafür sorgen, dass auch Security Awareness-Prozesse und Trainingsprogramme Ransomware thematisieren.

Ebenso sollten Sie sicherstellen, dass Ihr Krisenreaktionsplan Ransomware-Attacken mit einbezieht. Mindestens folgende Punkte sollten enthalten sein:

- Bei ersten Hinweisen auf einen Angriff sind die entsprechenden Verantwortlichen zu informieren.
- Betroffene Geräte sind zu isolieren und genauestens zu untersuchen.
- Können betroffene Geräte nicht isoliert werden, muss zunächst ein Abbild des betroffenen Systems und des Arbeitsspeichers erstellt werden. Im Anschluss sollten betroffene Geräte vollständig heruntergefahren werden, um eine weitere Ausbreitung der Ransomware zu verhindern.
- Kann bestätigt werden, dass es sich um einen Angriff handelt, muss das Incident/Crisis Response-Team aktiviert werden.
- Die Rechtsabteilung ist zu informieren.
- Zulieferer sollten kontaktiert werden, da sie ggf. Unterstützung bieten können.
- Alle Mitarbeiter sind an ihre Geheimhaltungspflichten gegenüber der Presse und sozialen Medien zu erinnern.
- Der Umfang des Angriffs und die Eigenschaften der Ransomware müssen identifiziert werden.
- Die Polizei/Sicherheitsbehörden sind zu informieren.
- Eine Pressemitteilung muss erstellt werden.
- Wurden Daten verschlüsselt, ist zu klären, ob sich diese aus dem Backup wiederherstellen lassen.
- Mitarbeiter sind auf den neuesten Stand bezüglich der Entwicklungen zu bringen.
- Wenn nötig, muss der Business Continuity-Plan zum Einsatz kommen.
- Relevante Logs und möglichst viele IoCs (Indicators of Compromise), also beispielsweise Binärdateien, Lösegeldforderungen, IP-Adressen, Registry-Einträge und andere Dateien sind zu sammeln und zu archivieren.
- Eine umfassende Dokumentation zu den ersten Untersuchungsschritten und Gegenmaßnahmen muss erstellt werden.

Kein Ransomware-Angriff gleicht dem anderen. Dennoch kann es hilfreich sein, zumindest ein Ransomware-Szenario im Krisenplan unterzubringen und es mit den entsprechenden Mitarbeitern durchzuspielen. Dazu gehören auch Personen aus der Management-Ebene. Dies hilft, eventuelle Lücken im Plan bereits vorab zu identifizieren. Gleichzeitig wird für alle deutlich, was genau passiert, wenn selbst grundlegende Arbeitsmittel nicht nutzbar sind (E-Mail, Internetzugang, VoIP-Telefonie).

ENDPOINT DETECTION AND RESPONSE

Mithilfe von speziellen Tools lässt sich die Abwehr von Ransomware und ihren Folgen wesentlich vereinfachen. Sogenannte Endpoint Detection and Response (EDR)-Tools automatisieren einige Mechanismen der Ransomware-Abwehr und unterstützen so Sicherheitsverantwortliche umfassend. Diese Sammlung an Werkzeugen kann entweder selbst intern entwickelt oder als integriertes Security-Produkt eingekauft werden.

Abbildung 6 zeigt einige EDR-Regeln, mit deren Hilfe verdächtige Aktivitäten, die auf einen Ransomware-Angriff hindeuten, frühzeitig erkannt werden können. (Bei der hier dargestellten EDR-Lösung handelt es sich um den *ESET Enterprise Inspector*).

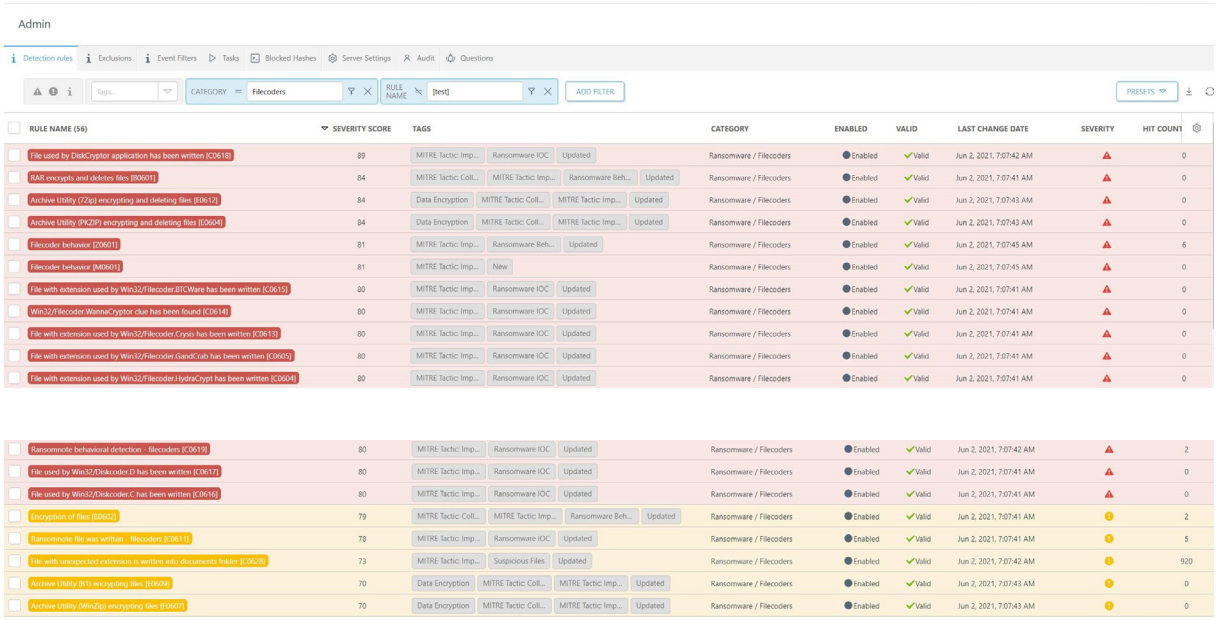

Abbildung 6: Dashboard des ESET Enterprise Inspector mit Regeln für die Erkennung/Abwehr von Ransomware

Mithilfe eines EDR-Tools lassen sich alle Endpoints in Ihrem Unternehmensnetzwerk auf verdächtige Aktivitäten untersuchen, z.B. die Änderung von Dateiendungen. Dieses Verhalten ist typisch für Mimikatz, welches Zugangsdaten aus dem Arbeitsspeicher zieht, oder die Software Cobalt Strike, mit der sich Angreifer in einem Netzwerk einnisten, um von dort aus weitere Befehle auszuführen.

Ein EDR-System ermöglicht, Anzeichen schädlicher Aktivitäten im Netzwerk mithilfe von Regeln und Alarmen frühzeitig zu erkennen. Diese Regeln können dann laufend mit neuen Informationen, z.B. IoCs verfeinert und weiterentwickelt werden. Mithilfe eines guten EDR-Tools können Admins betroffene Geräte schnell identifizieren, isolieren und das Problem diagnostizieren. Dazu gehört auch, die Befehle nachzuvollziehen, die das infizierte System bis dahin ausgeführt hat. So unterstützt ein EDR-Tool Sicherheitsteams umfassend bei der Abwehr von Attacken sowie bei Gegenmaßnahmen und der nachträglichen Analyse von Angriffen.

EIN WORT ZUM THEMA LÖSEGELD

Sollen Unternehmen im Fall der Fälle *das geforderte Lösegeld* bezahlen? Die Antwort darauf lautet: Nein. Denn:

- Mit der Zahlung finanzieren Sie das „Geschäftsmodell" der Angreifer und sorgen für dessen Fortsetzung.
- Das gezahlte Geld hilft, weitere kriminelle Aktivitäten zu finanzieren.
- Sie helfen Ransomware-Gruppen, immer neue Schwachstellen zu finden und auszunutzen.
- Sie geben den Angreifern das Signal, dass Sie ein lohnendes Ziel sind – und fordern Sie so förmlich zu weiteren Angriffen auf Ihr Netzwerk auf.

So verlockend die „einfache Lösung", also die Zahlung des Lösegelds zunächst erscheinen mag: Sie können nicht einmal mit Sicherheit sagen, dass die Kriminellen Ihre Daten auch tatsächlich entschlüsseln werden. Sie haben schließlich keinerlei Handhabe, die Erfüllung des „Vertrags" zwischen Ihnen und den Erpressern vor Gericht oder einer anderen Behörde einzuklagen.

- Es ist nicht einmal sicher, dass die Angreifer Ihre Daten überhaupt wiederherstellen können. Der Verschlüsselungsprozess kann nämlich Informationen kompromittiert haben, sodass sie nicht vollständig wiederhergestellt werden können.
- Das Entschlüsselungstool, welches Ihnen die Kriminellen bereitstellen, kann selbst Malware enthalten, fehlerhaft programmiert sein oder für die Entschlüsselung schlicht länger brauchen als die Wiederherstellung der Daten aus einem Backup.
- Der Bereitstellungsprozess des Entschlüsselungstools kann aus unterschiedlichen Gründen scheitern.
- Die Angreifer *hatten nie vor, Ihre Daten jemals wieder freizugeben*.

Auch das FBI *unterstreicht* die oben genannten Punkte: „Die Zahlung des Lösegelds garantiert in keinem Fall, dass die betroffene Organisation ihre Daten zurückerhält. Wir haben bereits mehrfach Fälle beobachtet, in denen Organisationen auch nach der Zahlung schlicht keinen Entschlüsselungs-Key erhalten haben. Die Zahlung des Lösegelds unterstützt nicht nur die Angreifer dabei, ihre Aktivitäten fortzusetzen und weitere Organisationen ins Visier zu nehmen. Es setzt auch für weitere Kriminelle ein deutliches Zeichen, dass sich diese Form der illegalen Aktivität lohnt."

Unternehmen fühlen sich vor allem dann verpflichtet, Lösegelder zu zahlen, wenn sie sich nicht in der Lage sehen, die Daten aus Backups wiederherzustellen, z.B. weil es keine Backups gibt oder weil diese in irgendeiner Weise kompromittiert sind. Auch in diesem Fall gibt es aber Alternativen zum Zahlen des Lösegeldes: Bevor Sie auf die Forderung eingehen, sollten Sie Security-Anbieter kontaktieren und um Hilfe bei der Wiederherstellung der Daten bitten. Selbst wenn dies nicht möglich ist, können sie Ihnen sagen, ob es sich bei der vorliegenden Ransomware womöglich um eine Variante handelt, bei der die Täter üblicherweise auch nach Zahlung des Lösegeldes die Daten nicht entschlüsseln.

Manche Organisationen gehen irrtümlich davon aus, dass eine Lösegeldzahlung weniger Kosten verursachen würde, als die Daten wiederherzustellen. Dass es sich dabei um eine Milchmädchenrechnung handelt, dürfte nach den oben genannten Argumenten klar sein. Vor allem nach der Erkenntnis, dass Sie es hier nicht mit Akteuren zu tun haben, auf deren grundsätzliche Rechtschaffenheit Sie vertrauen können und dass Sie letztlich mit Ihrem Lösegeld weitere Angriffe auf sich oder andere unterstützen.

Vielleicht haben Sie von Ransomware gehört, die ihren Opfern „netterweise" beweisen möchte, dass die Entschlüsselung auch funktioniert. Zu diesem Zweck muss das betroffene Unternehmen lediglich eine verschlüsselte Datei an die Angreifer zurücksenden. Und tatsächlich: Das Opfer enthält eine vollständig entschlüsselte Datei zurück. Dies zieht aber wiederum ganz andere Probleme nach sich. Senden Sie eine verschlüsselte Datei an den Angreifer, zeigen Sie ihm womöglich, dass es sich hierbei um in irgendeiner

Weise wertvolle Informationen handelt. Oder noch schlimmer: Enthält die zu entschlüsselnde Datei personenbezogene oder andere vom Gesetzgeber geschützte Informationen, machen Sie sich selbst aktiv der Preisgabe dieser Daten an Dritte schuldig – mit den entsprechenden Folgen.

Ein weiterer wichtiger Punkt: Sobald Sie die eigentliche Ransomware mithilfe von Security-Software von Ihren Systemen entfernen, kann es sein, dass die Daten gar nicht mehr entschlüsselt werden können. Häufig ist der Entschlüsselungsmechanismus nämlich selbst Teil der Malware.

Kurzum: Die Zahlung eines Lösegelds löst keine Probleme – und erzeugt im Zweifel sogar zusätzliche.

DIE ZUKUNFT VON RANSOMWARE

Jeder, der mit dem Schutz von Systemen und Daten zu tun hat, kennt die berühmte „CIA"-Formel der Informationssicherheit: Confidentiality (Vertraulichkeit), Integrity (Integrität) und Availability (Verfügbarkeit). Ziel von Ransomware ist es, das „A", also die Verfügbarkeit der Daten, zu kompromittieren. Mit zunehmender Abhängigkeit der Unternehmen von Technologie und Daten für den reibungslosen Ablauf der Geschäftsprozesse wächst auch die Angriffsfläche für Ransomware. Entsprechend können wir – vorausgesetzt, es ergeben sich keine größeren weltpolitischen oder ökonomischen Veränderungen – davon ausgehen, dass Ransomware weiterhin bestehen und sich stetig weiterentwickeln wird.

Mit mehr als 30 Jahre Erfahrung in Sachen IT-Security können wir festhalten, dass neuartige Malware meist folgende Evolutionsschritte durchläuft:

- Sicherheitslücken in einer neuen Technologie werden entdeckt und ihr Potenzial für den Missbrauch durch Kriminelle analysiert.
- Hersteller, Security-Experten und Anwender entwickeln erste Maßnahmen zur Schließung der Lücke.
- Tatsächliche Angriffsversuche über die Sicherheitslücke bleiben zunächst die Ausnahme, da es sich für Kriminelle (noch) nicht lohnt und sie genug mit „althergebrachten" Strategien verdienen.
- Ohne tatsächliche Angriffe „in freier Wildbahn" schwindet die Motivation, Gegenmaßnahmen aufrechtzuerhalten.
- Kriminelle entdecken die „neue" Schwachstelle schließlich doch für sich und beginnen, sie großflächig auszunutzen.
- Ein neuer Malware-Trend entsteht.

Entsprechend verlief beispielsweise die Entwicklung von DDoS-Attacken, z.B. gegen IoT-Überwachungsgeräte (Mirai) und die Entwicklung von Router-Malware (VPNFilter). Apropos Internet of Things: Ransomware profitiert derzeit stark vom Trend hin zu (oft schlecht gesicherten) IoT-Geräten, industriellen Steuerungssystemen mit Internetzugang sowie „smarten" Gebäuden und Fahrzeugen (darunter autonome Fahrzeuge, siehe auch den Artikel *„RoT: Was ist Ransomware of Things"* sowie das Webinar *„Ransomware from the Dark Side"*.)

Für die Zukunft lassen sich eine Vielzahl an Szenarios entwerfen, sollten die Gewinne nachlassen, die Kriminelle mit den aktuell verfügbaren Methoden erreichen. Denken Sie nur an Router-Malware, die den Netzwerktraffic drosseln oder komplett sperren könnte, bis ein Lösegeld bezahlt wurde. Sie könnte zudem drohen, den Router komplett unbrauchbar zu machen oder ankündigen, Traffic-Inhalte zu veröffentlichen, sollte versucht werden, die Malware zu entfernen.

Weiterhin wäre es denkbar, dass Fahrzeuge, Wohnungen und Gebäude aus der Ferne gesperrt werden, um Lösegeld zu erpressen. Steuerungssysteme von Heizungen, Klimaanlagen usw. sind quasi prädestiniert dafür, ein lohnenswertes Ziel für Erpressungsversuche zu werden (und *sind es in Ansätzen auch schon*). Auch dass Industrie-Roboter ein Ziel für Malware-Angriffe sein können, wurde bereits gezeigt.

Für Unternehmen ergeben sich aus diesen Entwicklungen verschiedene Implikationen. Wir empfehlen, generell folgendermaßen vorzugehen:

- Nehmen Sie die Gefahren, die von Ransomware ausgehen, in Ihr Risikomanagement auf und planen Sie damit.
- Identifizieren Sie mögliche Ransomware-Ziele im Unternehmen, also IoT-Geräte, SOHO-Router, Roboter, Steuerungssysteme und autonome Systeme und dokumentieren Sie jedes einzelne.
- Dokumentieren Sie Schwachstellen und Sicherheitslücken in diesen Geräten.
- Gibt es bereits Patches für diese Sicherheitslücken, führen Sie sie durch und erstellen Sie Updatepläne, damit die Geräte immer auf dem aktuellen Stand sind.
- Isolieren Sie IoT- und vergleichbare Geräte von Produktivnetzen.

FAZIT

Die Daten, Methoden und Fallbeispiele in diesem Paper zeigen vor allem eines: Ransomware ist und bleibt eine der größten Gefahren für die IT-Security, insbesondere von Unternehmen. Nicht zuletzt die Entwicklung des Doxings im Jahr 2019 hatte großen Anteil daran, dass Ransomware zu einem einträglichen Geschäft für Cyberkriminelle wurde.

Diesem Trend schlossen sich schnell weitere Akteure an und entwickelten ihn weiter. Auf Basis des Doxing entstanden immer neue Methoden, die nicht nur die Daten, sondern auch die Webseiten, Mitarbeiter, Geschäftspartner und Kunden in Erpressungsversuche mit einbezogen – und so den Druck auf ihre Opfer immer weiter erhöhten.

Die weltweite COVID 19-Pandemie und die damit einhergehenden Ängste und Unsicherheiten spielten den Urhebern und Verbreitern von Ransomware erneut in die Hände. Ransomware-Gruppen begannen, in großem Stil Brute Force-Angriffe auf RDP zu fahren – aktuell einer der am häufigsten missbrauchten Angriffsvektoren.

Neben solchen technischen Möglichkeiten setzen Cyberkriminelle weiterhin auf den „menschlichen Gefahrenfaktor“: *Spam* mit verseuchten Makros, Fake-Links und Botnetze sind keineswegs von der Bildfläche verschwunden.

Die Erpressungsmethoden werden immer raffinierter, die Verbreitungswege immer ausgefeilter. Entsprechend steigen die Gewinne, die Kriminelle aus ihren Kampagnen ziehen können. Das Geld hilft dann wiederum, umfassende Geschäftsmodelle auf Ransomware aufzubauen und weitere fragwürdige Akteure anzuziehen. Diese sparen sich nicht selten den Umweg, eigene Ransomware zu entwickeln oder zu verbreiten, sondern kaufen fertige Exploit-Kits für bekannte Sicherheitslücken oder gestohlene Zugangsdaten.

Doch nicht nur Ransomware as a Service (RaaS) ist ein besorgniserregender Trend in der Bedrohungslandschaft. Auch die zunehmende Anzahl an Ransomware-Vorfällen über die Supply Chain deutet an, in welche Richtung sich die Lage entwickeln könnte.

Ransomware-Gruppen sind mittlerweile sowohl mit finanziellen als auch personellen Mitteln so gut ausgestattet, dass kein IT- und Security-Verantwortlicher mehr die Augen vor den Entwicklungen verschließen kann. Dabei hat sich seit dem Beginn dieses Jahrzehnts immer wieder deutlich gezeigt, welchen starken Schutz durchdachte und rigoros umgesetzte Security-Richtlinien, Soft- und Hardwareeinstellungen sowie starke Passwörter in Kombination mit Multi-Faktor-Authentifizierungen bieten. Viele der hier genannten Fallbeispiele unterstreichen zudem die Wichtigkeit regelmäßiger Updates, um bekannte Schwachstellen zu schließen und so zumindest eines der wichtigsten Einfallstore zu schließen.

Für die Bekämpfung von Zero Day-Exploits, Botnetzen, Malware-Spam sowie anderen, technisch komplexeren Methoden braucht es jedoch eine stärkere Abwehr. Eine zuverlässige mehrschichtige Endpoint Security erkennt auch potenzielle Bedrohungen in E-Mails, Fake-Links sowie mögliche Angriffe

auf RDP und andere Netzwerkprotokolle. Mit einer umfassenden EDR-Lösung behalten Security-Verantwortliche zudem den Überblick über alle Vorgänge im Netzwerk, können Unregelmäßigkeiten und potenzielle Malware frühzeitig identifizieren und die betroffenen Geräte isolieren.

Jede technische Neu- und Weiterentwicklung birgt immenses Potenzial, die Gesellschaft ein Stück voranzubringen. Gleichzeitig bietet jede neue Technologie Cyberkriminellen die Möglichkeit, auf immer neuen Wegen aktiv zu werden. Wir hoffen, dass unsere Erklärungen zu den Gefahren, die von Ransomware ausgehen und den Möglichkeiten, sich effektiv davor zu schützen, helfen, das positive Potenzial von Technologie vollends auszuschöpfen und gleichzeitig die Gefahren zu minimieren.

ÜBER ESET

Als europäischer Hersteller mit mehr als 30 Jahren Erfahrung bietet ESET ein breites Portfolio an Sicherheitslösungen für jede Unternehmensgröße.
Wir schützen betriebssystemübergreifend sämtliche Endpoints und Server mit einer vielfach ausgezeichneten mehrschichtigen Technologie, unterstützen Ihren Datenschutz mit Hilfe von Multi-Faktor-Authentifizierung und zertifizierten Verschlüsselungsprodukten oder halten Ihr Netzwerk mit Hilfe von Cloud-Sandboxing frei von Zero-Day-Bedrohungen.

Unsere Endpoint Detection and Response Lösungen und Frühwarnsysteme wie Threat Intelligence Services ergänzen das Angebot im Hinblick auf Forensik sowie gezieltem Schutz vor Cyberkriminalität und APTs. Dabei setzt ESET nicht nur allein auf Next-Gen-Technologien, sondern kombiniert Erkenntnisse aus der cloudbasierten Repudationsdatenbank ESET LiveGrid® mit Machine Learning und menschlicher Expertise, um Ihnen den besten Schutz zu gewährleisten.

BEWÄHRT

Trust Seal www.teletrust.de/itsmie

ESET wurde das Vertrauenssiegel „IT Security made in EU" verliehen

Unsere Lösungen sind nach Qualitätsstandards zertifiziert

ESET IN ZAHLEN

110+ Mio.
Nutzer weltweit

400k+
Business-Kunden

200+
Länder & Regionen

13
Forschungs- und Entwicklungs-zentren weltweit

welivesecurity by ESET

ESET Deutschland GmbH | Spitzweidenweg 32 | 07743 Jena | Tel.:+49 3641 3114 200

ESET.DE | ESET.AT | ESET.CH

ENJOY SAFER TECHNOLOGY™