The bridge to possible

Schutz vor Ransomware

Zero-Trust-Sicherheit für die moderne Belegschaft

Inhalt

The bridge to possible

Ransomware wird es auch in Zukunft geben

Ransomware hat sich als Angriffsstrategie schnell weiterentwickelt. Während es sich dabei einst um die feindliche Übernahme einzelner Computer handelte, steht heute viel mehr auf dem Spiel. Böswillige Akteure nehmen zunehmend geopolitische Ziele, kritische Geschäftssysteme und Infrastrukturen ins Visier (z. B. „Big Game Hunting“), was zu ungeahnten Schäden führen kann. Heute zählt Ransomware zu den größten Bedrohungen im Bereich der Cybersicherheit und nimmt im Jahr 2020 aufgrund der rasanten Verlagerung zur Remote-Arbeit um 150 % zu.

Ransomware wird inzwischen als Cyberterrorismus eingestuft und die jüngste Verfügung von US-Präsident Biden bestätigt, dass jetzt Maßnahmen zum Schutz der Systeme ergriffen werden müssen. Ein Zero-Trust-Ansatz ist der Goldstandard zum Schutz vor Ransomware. Laut dem National Institute of Standards and Technology (NIST) ist die „Implementierung einer Zero-Trust-Architektur zu einem wichtigen Faktor für die Cybersicherheit und zu einer wirtschaftlichen Notwendigkeit geworden“.

Im Merkblatt des Weißen Hauses heißt es: „Die jüngsten Cybersicherheits-Vorfälle wie SolarWinds, Microsoft Exchange und der Vorfall bei Colonial Pipeline sind eine ernüchternde Erinnerung daran, dass öffentliche und private Einrichtungen in den USA es zunehmend mit ausgeklügelten böswilligen Cyberaktivitäten sowohl von nationalstaatlichen Akteuren als auch von Cyberkriminellen zu tun haben.“

„Die jüngsten Cybersicherheits-Vorfälle wie SolarWinds, Microsoft Exchange und der Vorfall bei Colonial Pipeline sind eine ernüchternde Erinnerung daran, dass öffentliche und private Einrichtungen in den USA es zunehmend mit ausgeklügelten böswilligen Cyberaktivitäten sowohl von nationalstaatlichen Akteuren als auch von Cyberkriminellen zu tun haben.“

Merkblatt des Weißen Hauses der Vereinigten Staaten von Amerika

Was ist Ransomware?

Einfach ausgedrückt: Ransomware nutzt eine Vielzahl von Taktiken, um BenutzerInnen vor allem durch Malware-Infektionen anzugreifen, die i. d. R. mit E-Mail-Phishing, einem gestohlenen Kennwort oder einem Brute-Force-Angriff beginnen. Ein Ransomware-Angriff kann durch die Verschlüsselung von Dateien oder Ordnern, die Verhinderung des Systemzugriffs auf die Festplatte und die Manipulation des Master Boot Records zur Unterbrechung des Systemstartvorgangs erfolgen. Sobald die Malware installiert und verteilt wurde, können Hacker Zugriff auf vertrauliche Daten und Sicherungsdaten erhalten, die sie verschlüsseln, um die Informationen in Geiselhaft zu halten. Hacker können schnell vorgehen oder monatelang unbemerkt in der Netzwerkinfrastruktur herumspionieren, bevor sie einen Angriff starten.

Der Datenklau soll bei den Opfern Angst und Dringlichkeit hervorrufen. Die Informationen sind bis zur Zahlung eines Lösegelds (vorwiegend in Bitcoin) unzugänglich. Und sogar dann kann es sein, dass Unternehmen nicht alle ihre Daten zurückbekommen. Es gibt viele verschiedene Varianten von Ransomware, aber in den meisten Fällen wird Crypto-Ransomware eingesetzt. Aufgrund von Polymorphie (Malware, die sich ständig verändert) gibt es viele Varianten, die nicht erkannt werden können.

Die Crypto-Ransomware, durch die Daten gesperrt werden, wird immer besser. Im Jahr 2006 verwendete Ransomware 56 Bit mit eigener Verschlüsselung. Heute verwendet die fortgeschrittene Version von Ransomware symmetrische AES-Algorithmen und eine Verschlüsselung mit öffentlichen Schlüsseln auf Basis von RSA oder EEC, um Daten zu sperren.

Ransomware entwickelt sich zu einem ganzen Geschäftszweig

Während Ransomware weiter an Fahrt gewinnt, hat sich die Taktik zu einem professionellen Geschäft entwickelt. Das Ziel dieser kriminellen Organisationen (meist mit Sitz in China, Russland, Nordkorea und Osteuropa) ist es, hochrangige Ziele anzugreifen und zu stören und im Austausch für Daten Geld zu erpressen. Um die Effektivität ihrer Angriffe zu steigern, gehen diese Organisationen sogar so weit, dass sie Callcenter einrichten, um Zielpersonen beim Kauf von Bitcoin und der Bezahlung des Lösegelds zu unterstützen. Der Kundenservice einiger dieser Organisationen wird von ihren Zielpersonen sogar positiv bewertet.

Um einen Anreiz für die Zahlung zu schaffen, stellen Angreifer manchmal nach Erhalt des Lösegelds einen detaillierten „Sicherheitsbericht“ zur Verfügung, in dem die Durchführung des Angriffs genau beschrieben wird. Es wäre zwar klug, wenn Banden die Dateien gegen Geld entschlüsseln würden, um ihren Ruf für das nächste Ziel zu wahren, aber das ist nicht immer der Fall. In der Sophos-Studie The State of Ransomware 2021 heißt es, dass nur 8 % der Opfer ihre Daten zurückerhalten und 29 % können mehr als die Hälfte wiederherstellen. Manchmal werden die Daten gesammelt und mit anderen Angreifern ausgetauscht oder für eine spätere Lösegeldforderung aufbewahrt.

In den letzten Jahren haben böswillige Akteure Ransomware-as-a-Service (RaaS) entwickelt. Dabei handelt es sich um eine umfassend integrierte, sofort einsatzbereite Lösung, die es jedem ermöglicht, einen Ransomware-Angriff auszuführen, ohne über Programmierkenntnisse zu verfügen. Wie Software-as-a-Service (SaaS)-Produkte bietet RaaS einen relativ kostengünstigen und einfachen Zugriff auf diese Art von Schadprogrammen gegen eine Gebühr, die geringer ist als die Kosten für die Erstellung eines eigenen Programms. RaaS-Anbieter erhalten i. d. R. einen Anteil von 20 % bis 30 % des erzielten Lösegeldgewinns. Es gibt jetzt Abonnement- und Partnermodelle, um erfolgreiche Angriffe zu unterstützen. Die Hackergruppe REvil betrieb ein Partnermodell, bei dem jeder, der zu einem erfolgreichen Ransomware-Angriff beitrug, eine Gewinnbeteiligung erhielt. Dieses Modell hat zu einem dramatischen Anstieg der Zahl der Ransomware-Angriffe geführt.

Ein weiterer Trend, der ursprünglich der Maze-Bande zugeschrieben wurde, ist die doppelte Erpressung. Dabei drohen die Hacker mit der Veröffentlichung der erbeuteten Informationen im Dark Web und/oder Internet, wenn ihre Forderungen nicht erfüllt werden. Laut dem 2020 Data Breach Investigations Report von Verizon verfügen sie über eine eigene Infrastruktur zur Verarbeitung dieser Datenmengen. Bei den meisten Ransomware-Banden ist die sogenannte „Name and Shame“-Taktik inzwischen sehr beliebt, ebenso wie das „Penalty“-Modell, bei dem die Lösegeldforderung mit der Zeit steigt.

Während Unternehmen ihren Sicherheitsstatus für Computer und Netzwerke gegen Ransomware-Angriffe verbessern, wählen Hacker mittlerweile vermehrt Mobilgeräte als Ziele. Diese Geräte haben einen viel kleineren Bildschirm und zeigen auf den ersten Blick keine umfassenden Informationen an (z. B. E-Mails). Dadurch steigt die Wahrscheinlichkeit, dass Opfer auf schädliche Links klicken. Angriffe auf das Internet of Things (IoT) sind ebenfalls auf dem Vormarsch, da Ransomware und fehlende Sicherheitsvorkehrungen Geräte und Objekte zu Einstiegspunkten für Ransomware-Tools machen können. Im Jahr 2020 nahmen Ransomware-Angriffe auf IoT-Geräte in den USA um 109 % zu.

Diese Umstände sowie bestimmte Länder, die Angreifern als sichere Häfen dienen, haben zu einem Anstieg der Ransomware-Kriminalität geführt. Im Jahr 2020 fand alle 10 Sekunden ein erfolgreicher Ransomware-Angriff statt, und laut der Harris-Umfrage von Anomali ist einer von fünf Amerikanern Opfer von Ransomware-Angriffen. Darüber hinaus berichtet das Infosecurity Magazine, dass die beliebteste Angriffsmethode „mit Abstand Botnet-Traffic (28 %) war, gefolgt von Cryptomining (21 %), Informationsdiebstahl (16 %), mobiler Malware (15 %) und Banking-Malware (14 %)". Entsprechend geben Unternehmen immer mehr Geld für Sicherheit aus (laut Gartner 150 Milliarden Dollar im Jahr 2021).

Die Angriffe auf Einzelpersonen gehen zurück, da sich Hacker auf lukrativere Ziele konzentrieren. Anbieter von Managed Services (MSP) melden einen 85-prozentigen Anstieg der Angriffe auf kleine und mittelständische Unternehmen. Mehr denn je werden Großunternehmen, Firmen aus den Bereichen Infrastruktur, Gesundheitswesen und Fertigung sowie Behörden ins Visier genommen, die für ihre Daten dann einen Preis in Millionenhöhe bezahlen müssen. Die Höhe des Lösegelds hat sich im letzten Jahr verdoppelt, da die Angreifer größere Unternehmen zum Ziel nehmen. Angriffe auf Anbieter, Auftragnehmer und Software von Drittanbietern haben ebenfalls stark zugenommen. Unternehmen mussten sich darauf verlassen, dass die Sicherheit dieser externen Parteien, die Zugriff auf ihre Systeme haben, gewährleistet ist.

Die Zunahme von Ransomware-Banden	Der erste bekannte Fall von Ransomware ging von Disketten aus, die AIDS-Studien und Malware enthielten und 1989 von Dr. Joseph Popp in der ganzen Welt verteilt wurden. Die Disketten verschlüsselten Dateien auf dem System des Opfers und verweigerten den Zugriff, bis eine Zahlung von 189 Dollar an ein Postfach in Panama überwiesen wurde. Die infizierten CDs wurden dann auf der AIDS-Konferenz der Weltgesundheitsorganisation verteilt. Zahlungen und das Versenden von CDs waren schwierig und teuer.
2006	Cyberkriminelle begannen, eine effektivere Form der öffentlichen 660-RSA-Verschlüsselung zu verwenden, um Dateien schneller zu verschlüsseln. Zu den Hauptakteuren in dieser Zeit gehörten der Archiveus-Trojaner und der GPcode, die Phishing-E-Mails als Eintrittspunkte nutzten.
2008-2009	Neue Antivirus-Software, die Ransomware-Malware enthielt, tauchte auf und betrügerische Sicherheitssoftware nutzte FileFix Pro, um Geld für die Entschlüsselung zu erpressen.
2010	Bitcoin hat alles verändert. Zehntausend Ransomware-Varianten wurden entdeckt und zum ersten Mal trat Ransomware mit Bildschirmsperre auf.
2013	Es existierten eine Viertelmillion Ransomware-Samples und Cryptolocker und Bitcoin wurden schnell zur wichtigsten Zahlungsmethode. Die Ransomware nutzte eine 2048-Bit-RSA-Verschlüsselung für erhöhte Forderungen, was sich für Banden als lukrativ erwies.
2015	Der Ransomware-Trojaner Teslacrypt tauchte auf, es gab inzwischen 4 Millionen Ransomware-Varianten und Ransomware-as-a-Service (RaaS) wurde eingeführt.
2016	JavaScript- und Locky-Ransomware waren sehr beliebt, wobei täglich 90.000 Opfer mit Locky infiziert wurden. Angreifer hatten es auf größere Organisationen wie Krankenhäuser und akademische Einrichtungen abgesehen. Mit Ransomware wurden mehr als 1 Milliarde US-Dollar Gewinn erzielt. Die Petya-Malware richtete einen finanziellen Schaden von über 10 Milliarden US-Dollar an.
2017	In diesem Jahr tauchte der Kryptowurm WannaCry auf, von dem täglich neue Varianten auftraten und der sich über einen Microsoft-Exploit schnell auf 300.000 Computern weltweit verbreitete.
2018	Katsuya trat auf den Plan. SamSam legte mehrere öffentliche Dienste in der US-Stadt Atlanta lahm.

The bridge to possible

2019	Ab diesem Jahr war REvil, eine RaaS-Hackergruppe aus Russland, aktiv. Ryuk, eine fortschrittliche und kostspielige Ransomware-Variante, die in bösartige Anhänge und Phishing-E-Mails eingebettet war, verlangte im Vergleich zu ähnlichen Angriffen höhere Zahlungen und legte alle großen Zeitungen in den USA lahm.
2020	Darkside, Egregor und Sodinokibi traten als wichtige Akteure in Erscheinung. Bei Ryuk stieg die Zahl von einem Fall pro Tag auf 19,9 Millionen im September, was acht Fällen pro Sekunde entspricht.
2021	Das Gesundheitswesen wurde von Angriffen mit REvil/Sodinokibi, Conti und LockBit hart getroffen. CryptoLocker erpresste in einer der bisher größten Ransomware-Zahlungen 40 Millionen Dollar vom großen Versicherungsanbieter CNA Financial. DarkSide gelang es, die Colonial Pipeline Company anzugreifen, was den größten öffentlich bekannt gewordenen Hackerangriff auf kritische Infrastrukturen in den USA darstellte.

Der Perimeter erweitert sich

Wie konnte sich Ransomware so stark verbreiten? Früher war der Perimeter eine Art Schutzwall, hinter dem zentralisierte Daten und Anwendungen über VPN-Firewalls (Virtual Private Network) und MDM-Lösungen (Mobile Device Management) verwaltet wurden. Man kann sich dies wie einen Wassergraben um eine Burg vorstellen. Heutzutage wird von überall und von jedem Gerät aus gearbeitet (auch von privaten Mobilgeräten) und der Zugriff auf Daten muss über Drittanbieteranwendungen in der Cloud erfolgen. Es gibt keinen Wassergraben, stattdessen finden sich sogar mehrere Eingänge zur Burg. Durch die Zunahme von Remote-Arbeit während der Pandemie verwandelte sich der traditionelle Perimeter in einen „softwaredefinierten Perimeter". Da schnell dafür gesorgt werden musste, dass die Belegschaft weiterarbeiten konnte, wurde das Thema Sicherheit vernachlässigt, was böswilligen Akteuren Gelegenheiten für Ransomware-Angriffe eröffnete.

Remote-Zugriff

Laut dem Gartner-Bericht Top Security and Risk Management Trends for 2021 können 64 % der MitarbeiterInnen jetzt von zu Hause arbeiten und zwei Fünftel der Belegschaft arbeiten von zu Hause. Während des pandemiebedingten Lockdowns mussten die meisten Arbeitnehmer zu 100 % remote arbeiten. Voraussetzung dafür war, dass sie auf ihren eigenen Geräten arbeiten und auf SaaS-Anwendungen in der Cloud und vor Ort zugreifen können. Viele Unternehmen verfügten nicht über die entsprechende Infrastruktur, um diese Veränderung zu unterstützen. Heutzutage ist Remotezugriff für MitarbeiterInnen eine Selbstverständlichkeit. Während sich Unternehmen an diesen Umbruch in der Arbeitskultur anpassen, wird die Zukunft voraussichtlich ein hybrides Modell aus Remote-MitarbeiterInnen und solchen sein, die vom Büro aus arbeiten.

„Um kontinuierliche Sicherheit zu gewährleisten, erfordert die neue Normalität von allen Unternehmen eine stets vernetzte Abwehrbereitschaft und Klarheit darüber, welche Geschäftsrisiken Remote-BenutzerInnen schaffen", so Peter Firstbrook, VP Analyst bei Gartner, in einem Blog-Eintrag.

Unternehmen, die ihren Sicherheitsstatus im Hinblick auf diese Veränderung nicht erhöht oder das interne Sicherheitsbewusstsein nicht gestärkt haben, machen es Angreifern einfach. Laut Gartner sind 57 % der Sicherheitsverletzungen auf Fahrlässigkeit von MitarbeiterInnen oder Dritten zurückzuführen. Laut ZDNet verschaffen sich Bedrohungsakteure am häufigsten über Remote Desktop Protocol (RDP) Zugang zu Windows-Computern und installieren Ransomware und andere Malware. Weitere beliebte Methoden sind E-Mail-Phishing und VPN-Bug-Exploits.

Nachteile von VPNs

Das Hacken von Exploits in VPNs ist die drittbeliebteste Zugriffsmethode für Ransomware-Hacker. Der Hackerangriff, der die Colonial Pipeline Company lahmlegte, war das Resultat eines kompromittierten Kennworts aus einem nicht genutzten VPN. Auch wenn VPNs den Zugriff auf lokale Anwendungen einschränken können, gibt es Inkonsistenzen beim Zugriff auf Cloud-Anwendungen, die zu Sicherheitslücken führen können. Kompromittierte VPNs können einen Zugriff auf das Netzwerk durch die Hintertür ermöglichen, was es Hackern ermöglicht, auf internen Systemen Malware zu installieren.

Laut einer Studie von Google lassen sich 100 % der automatisierten Bots, 99 % der Phishing-Massenangriffe und 90 % der gezielten Angriffe durch einen Zero-Trust-Ansatz mit VPN, Firewall und MFA verhindern.

Ungeschützte Endpunkte

Mit der Zahl der Geräte, die mit Unternehmensnetzwerken verbunden werden, steigt auch die Zahl der Privat- und Schattengeräte. Da diese Geräte möglicherweise nicht überwacht werden oder nicht auf dem neuesten Stand sind, können sie zu Sicherheitsverletzungen an wichtigen Endpunkten führen, die unbemerkt bleiben. Ungeschützte Endpunkte und die Tatsache, dass nicht klar ist, welche BenutzerInnen und Geräte sich mit dem Netzwerk verbinden und wie es um die Integrität der Geräte bestellt ist, können zu einer Sicherheitsverletzung durch Hacker führen, die akribisch nach Einstiegsmöglichkeiten suchen.

The bridge to possible

Phishing, gezielte Angriffe und Schwachstellen

Welche Techniken kommen bei Ransomware-Angriffen zum Einsatz? Es handelt sich um einen mehrstufigen Prozess, bei dem Angreifer eindringen und die Daten verschlüsseln, die am wertvollsten sind und den meisten Schaden verursachen, wenn sie in Geiselhaft genommen werden. Dieser Vorgang kann relativ kurz sein oder sich über mehrere Monate erstrecken. CSOonline.com berichtet, dass 94 % der Malware per E-Mail verbreitet wird und dass über 80 % der Sicherheitsvorfälle auf das Konto von Phishing-Angriffen gehen. Zu weiteren Einstiegspunkten zählen nicht gepatchte Updates und Zero-Day-Schwachstellen. Bei so gut wie allen Angriffen beginnt alles mit dem Diebstahl von Anmeldeinformationen.

Ransomware-Techniken

„Spray-and-Pray"-Ansatz oder breit gefächertes Phishing

Bedrohungsagenten erwerben auf dem Schwarzmarkt E-Mail-Listen, analysieren dann die Anmeldeinformationen und verteilen Phishing-E-Mails. Für einen erfolgreichen Angriff sind nur wenige Anmeldeinformationen erforderlich. Häufig erhalten Angreifer diese über E-Mails mit bösartigen Anhängen, betrügerische Websites, die legitim erscheinen, oder die Verwendung einer gefälschten Identität als hochrangige MitarbeiterInnen.

Spear Phishing

Bei diesem koordinierten, gezielten Angriff auf eine bestimmte Gruppe von BenutzerInnen werden personalisierte, sozial manipulierte Nachrichten von einer legitim wirkenden Quelle verschickt, die Neugierde oder Angst auslösen sollen oder eine Belohnung in Aussicht stellen. Die E-Mails und die Website enthalten Malware, mit der Anmeldeinformationen gestohlen werden können. Malware kann auch über soziale Medien und Instant-Messaging-Anwendungen verbreitet werden.

Brute Force

Bei einer Umfrage von LastPass gaben 91 % der Befragten zu, dass sie ihre Kennwörter wiederverwenden. Hacker sind sich dessen sehr wohl bewusst und sammeln Kennwörter aus Anmeldedaten-Dumps oder im Dark Web. Mithilfe automatisierter Tools testen sie dann Kennwörter auf verschiedenen Websites, was als Credential Stuffing oder Brute Force bezeichnet wird. Sobald sie Zugang erhalten, kann der Angriff beginnen.

Ausnutzung bekannter Sicherheitslücken

Um ein hohes Sicherheitsprofil aufrechtzuerhalten, ist es nicht nur wichtig zu wissen, welche Geräte mit dem Netzwerk verbunden sind, sondern auch, wie es um die Integrität der Geräte bestellt ist und wie aktuell die Patches und Updates sind. Laut Security Boulevard sind „veraltete und 'verwaiste' Open-Source-Komponenten weit verbreitet. 91 % der Programmcodes enthielten Komponenten, die entweder seit mehr als vier Jahren veraltet waren oder in den letzten zwei Jahren nicht weiterentwickelt wurden."

The bridge to possible

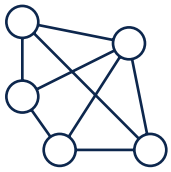
Schritt-für-Schritt-Anleitung für einen Ransomware-Angriff

Verschlüsseln von Ransomware

In den meisten Fällen werden bei Ransomware-Angriffen die Daten auf den Zielsystemen verschlüsselt und somit unzugänglich gemacht, bis ein Lösegeld für die Entschlüsselung gezahlt wird. Die neueste Taktik ist die doppelte Verschlüsselung, bei der die Hacker ein System zweimal verschlüsseln oder zwei verschiedene Gruppen dasselbe Opfer angreifen. Bei diesem Ansatz haben Angreifer die Möglichkeit, zweimal Lösegeld zu kassieren: einmal für die erste Verschlüsselungsebene und dann überraschen sie ihre Opfer nach der Bezahlung für die erste Ebene mit einer weiteren Ebene. Am häufigsten wird die asymmetrische oder symmetrische Verschlüsselung verwendet.

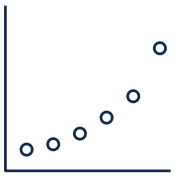
Angriffkoordination

In dieser Phase erledigen Ransomware-Hacker ihre Hausaufgaben und informieren sich über die jeweiligen Unternehmen, auf die sie es abgesehen haben. Es kann sein, dass sie E-Mail-Listen im Dark Web kaufen, wichtige Führungskräfte ausfindig machen, sich über die Finanzen des Unternehmens informieren, Profile in den sozialen Medien recherchieren und eine Liste der wichtigsten Stakeholder wie Auftragnehmer, Lieferanten und Partner zusammenstellen. Welche Taktiken verwenden Hacker zum Einstieg? Die drei beliebtesten Angriffe im Jahr 2020 sind auf nicht ausreichend geschützte RDP-Endpunkte, E-Mail-Phishing-Angriffe und die Ausnutzung von Zero-Day-Schwachstellen von VPNs zurückzuführen. Böswillige Akteure erhalten in erster Linie über kompromittierte Anmeldeinformationen Zugang.



Vertikale Bewegungen

Unter vertikaler Bewegung versteht man in der Phase der Infiltration und Infektion, wenn Angreifer von einer externen Position zu einer internen Position wechseln. Sobald sie sich Zutritt verschafft haben, scannen sie Dateien und führen schädlichen Code auf Endpunkten und Netzwerkgeräten aus. Die Malware bewegt sich durch das infizierte System und deaktiviert Firewalls und Antivirus-Software. Inzwischen haben die Angreifer die Daten in ihren Besitz gebracht, aber sie sind noch nicht verschlüsselt. Zu den gängigen Einstiegspunkten für vertikale Bewegungen zählen gefälschte E-Mail-Konten, einfache Webserver und unzureichend geschützte Endpunkte.



Seitwärtsbewegungen	Auslesen der Daten	Bezahlung und Entsperrung
Aufgrund von Seitwärtsbewegungen werden Advanced Persistent Threats (APT) immer erfolgreicher. Um im Netzwerk Fuß zu fassen, müssen Kriminelle Computer verschlüsseln und die Ransomware an so viele Systeme wie möglich verteilen. Sobald sie Zugriff erhalten haben, beginnt die Jagd der Hacker. Sie beginnen, sich wochen- oder monatelang unbemerkt seitwärts im Netzwerk zu bewegen, um wichtige Ziele wie das Command and Control Center (C2), asymmetrische Schlüssel und Sicherungsdateien zu identifizieren. Gleichzeitig infizieren sie weitere Systeme und Benutzerkonten, um ihre Zugriffs- und Benutzerrechte zu erhöhen, und bereiten eine dauerhafte bösartige Präsenz vor, um Daten in Besitz zu nehmen. Beispiele für Seitwärtsbewegungen sind etwa das Ausnutzen von Remote-Diensten, internes Spear-Phishing und die Verwendung gestohlener Kennwörter, auch bekannt als „Pass the Hash“.	Sobald die Bestandsaufnahme abgeschlossen ist, beginnt die Verschlüsselung. Systemsicherungen werden gelöscht, lokale Dateien und Ordner werden manipuliert, nicht zugeordnete Netzwerklaufwerke werden mit infizierten Systemen verbunden, und es wird eine Kommunikation mit dem Command and Control Center hergestellt, um die auf dem lokalen System verwendeten kryptografischen Schlüssel zu generieren. Die Netzwerkdaten werden lokal kopiert, verschlüsselt und dann hochgeladen, wobei die Originaldaten ersetzt werden. Ausgelesene Daten können für eine doppelte Erpressung verwendet werden. In diesem Fall wird Lösegeld für die Entschlüsselung der verschlüsselten Daten verlangt, und anschließend wird ein zweites Lösegeld verlangt, damit die gestohlenen Daten nicht weitergegeben werden.	Die Angreifer aktivieren dann die Malware, sperren Daten und verkünden ihre Lösegeldforderung an kompromittierten Orten. Dabei geben sie genaue Anweisungen, wie das Lösegeld zu zahlen ist, normalerweise in Bitcoin. Ein Ransomware-Angriff führt zu sehr kostspieligen Ausfällen, die extrem schwierig zu beheben sind. Drohungen werden ausgesprochen und der Countdown beginnt. Unternehmen müssen sich entscheiden: Möchten sie die Kosten auf sich nehmen und zahlen? Sollen sie versuchen, ihre Dateien selbst wiederherzustellen? Oder nehmen sie ihre Cybersicherheits-Versicherung in Anspruch, die nur einen Teil des Lösegelds erstattet? Damit Unternehmen nicht zwischen diesen Übeln wählen müssen, sollten sie unbedingt eine Zero-Trust-Architektur implementieren und bewährte Sicherheitspraktiken einführen.

Anfällige Branchen

Das Gesundheitswesen, Kommunen und Behörden sowie der Einzelhandel, das Bildungswesen und das Finanzwesen sind die Branchen, die am stärksten von Ransomware-Angriffen betroffen sind. In diesen Branchen werden komplexe Bestandslösungen eingesetzt, die möglicherweise keine zuverlässige Cloud-Sicherheit bieten. Außerdem werden Sicherheitsstandards im Gesundheits- und Bildungswesen sowie in Behörden nur langsam an Neuerungen und neue Technologien angepasst, was sie zu lukrativen und zugleich leichten Zielen macht.

The bridge to possible

Stoppen eines Ransomware-Angriffs, bevor er richtig beginnt

Bei einem Ransomware-Angriff müssen Angreifer zuerst Zugriff erhalten. Dazu können sie sich kompromittierte Anmeldeinformationen beschaffen, wie es beim Angriff auf Colonial Pipeline der Fall war.

Duo Multi-Faktor-Authentifizierung (MFA) kann dazu beitragen, dass Ransomware gar nicht erst ins Netzwerk gelangt. Bei MFA müssen BenutzerInnen eine Kombination aus zwei oder mehr Anmeldedaten vorlegen, um ihre Identität für die Anmeldung zu bestätigen. Zusätzlich zum Benutzernamen und Kennwort fragt Duo MFA z. B. nach einem vertrauenswürdigen Gerät oder einem Software- oder Hardware-Token, bevor der Zugriff auf Ressourcen gewährt wird. Dank dieser zusätzlichen Anforderung durch MFA wird es für Ransomware um einiges schwieriger, Fuß zu fassen.

Ransomware nutzt auch häufig Remote-Services wie RDP und VPNs, um sich Zugang zu einem Netzwerk zu verschaffen. Darkside, der mutmaßliche Verursacher des Colonial Pipeline-Angriffs, soll sich über den firmeninternen VPN-Zugriff Zugang zur Umgebung des Opfers verschafft haben. Die Kombination von Duo MFA, Duo Device Trust, Duo Network Gateway (DNG) und Duo Trust Monitor in einer einzigen Trusted Access-Lösung bietet mehr als nur MFA und kann Ihnen helfen, den Remote-Zugriff auf lokale Infrastruktur zu schützen und das Eindringen von Ransomware zu verhindern.

Mit Duo MFA wird für die Authentifizierung mehr als ein Benutzername und ein Kennwort benötigt. Mit DNG können BenutzerInnen auf lokale Websites, Webanwendungen, SSH-Server und RDP zugreifen, ohne VPN-Anmeldeinformationen zu benötigen. Duo Device Trust gewährleistet, dass es sich bei dem Gerät, das aus der Ferne auf Ressourcen zugreift, um einen vertrauenswürdigen Computer und nicht um ein Gerät eines Angreifers handelt. Duo Trust Monitor macht auf Authentifizierungsanfragen aufmerksam, die verdächtig erscheinen, z. B. solche aus Ländern, in denen Ransomware-Akteure bekanntermaßen aktiv sind oder in denen ein Unternehmen keine MitarbeiterInnen hat.

Eine weitere beliebte Methode zur Infektion mit Ransomware ist die Verwendung von Malware. Cisco bietet zusätzliche ergänzende Lösungen wie Secure Endpoint und Email Gateway, die Malware-basierte Ransomware untersuchen, erkennen und blockieren können, bevor sie Endgeräte infiziert.

The bridge to possible

So schützt Duo vor Ransomware

Laut Gartner sind 90 % der Ransomware-Fälle vermeidbar. Duo kann Unternehmen in dreierlei Hinsicht unterstützen:

1. Verhindern, dass Ransomware in einer Umgebung Fuß fassen kann
2. Verhindern oder Verlangsamen der Ausbreitung von Ransomware, wenn sie in ein Unternehmen eingedrungen ist
3. Schutz wichtiger Ressourcen und Teile des Unternehmens, während ein Angreifer noch in der Umgebung anwesend ist und bis zur vollständigen Beseitigung des Schadens

Die Verbreitung verhindern

Ransomware, die nur eine kleine Anzahl von Systemen befällt, hat geringere Auswirkungen und dürfte kaum dazu führen, dass der Betrieb lahmgelegt wird und Lösegeld gezahlt werden muss. Aus diesem Grund ist die Verbreitung von Ransomware so wichtig, um wesentliche Teile eines Unternehmens zum Erliegen zu bringen und sie zur Zahlung des Lösegelds zu zwingen, damit der Betrieb schnell wieder aufgenommen werden kann. Im Jahr 2017 nutzten WannaCry und NotPetya den Exploit External Blue, um eine Microsoft-Schwachstelle auszunutzen und sich ohne Zutun der BenutzerInnen zu verbreiten.

Device Health Application von Duo sorgt dafür, dass Geräte alle Patches und Updates erhalten, was eine automatische Verbreitung von Ransomware erschwert. Darüber hinaus bietet die Anwendung Sichtbarkeit und sie prüft bei jedem Anmeldeversuch den Status der Device Health, wozu auch der Update-Status des Geräts zählt. Mit der Duo-Funktion zur eigenständigen Behebung können BenutzerInnen auf einfache Weise sämtliche Patches auf ihre Geräte anwenden, ohne Unterstützung durch die IT-Abteilung zu benötigen.

Sichere Korrekturmaßnahmen

Wenn ein Ransomware-Angriff überstanden ist und Systeme wieder betriebsbereit sind, bedeutet das nicht unbedingt, dass der Angreifer nicht mehr in der Umgebung ist. Möglicherweise hat er versucht, sich für einen späteren Angriff einzunisten. Häufig werden dazu bestehende Konten kompromittiert oder neue Konten erstellt, oft über Active Directory oder andere Verzeichnisse mit Benutzerkonten. Duo MFA kann die Seitwärtsbewegung von Angreifern, die über kompromittierte Anmeldedaten verfügen und sich noch im Netzwerk befinden, unterbinden und so Sorgenfreiheit bieten. So kann außerdem Zeit gewonnen und verhindert werden, dass ein Angreifer weiteren Schaden anrichtet, während der Angriff vollständig behoben wird und alle Spuren einer Einnistung beseitigt werden.

Implementierung eines Zero-Trust-Sicherheitsmodells

Zero Trust ist ein Sicherheitsmodell, das auf dem Prinzip „niemals vertrauen, immer überprüfen“ basiert und Unternehmen bei der proaktiven Implementierung von Best Practices unterstützen kann, die bekanntermaßen Schutz vor Cyberangriffen, einschließlich Ransomware, bieten.

Zero Trust hat eine so enorme Bedeutung, dass das Weiße Haus den Einsatz von Zero Trust und MFA per Dekret verlangt.

Duo bietet eine MFA, die benutzerfreundlich und einfach zu implementieren ist. Außerdem können Unternehmen nur dann Zugriff gewähren, wenn BenutzerInnen und ihre jeweiligen Geräte verifiziert werden können und vertrauenswürdig sind. Diese Möglichkeit zur Kontrolle und Verwaltung des Zugriffs ist eine der grundlegenden Säulen von Zero Trust und Duo MFA ist einer der ersten Schritte zur Implementierung eines Zero-Trust-Frameworks.

Fazit

Ransomware-Angriffe werden zunehmen und Unternehmen müssen wachsamer sein. Social Engineering und Spear Phishing sind erfolgreich, weil sie die menschliche Komponente der Sicherheit eines Unternehmens ausnutzen. Um Ransomware-Angriffen einen Schritt voraus zu sein, ist es wichtig, einen Zero-Trust-Sicherheitsansatz einzuführen und umzusetzen, der mit einer starken MFA und einer vertrauenswürdigen Zugangsplattform beginnt.

The bridge to possible

Erweitern Sie die Bedrohungsabwehr mit Duo über MFA hinaus

Unternehmen können sich vor den Auswirkungen von Ransomware durch gezielte Phishing-Angriffe schützen, indem sie Richtlinien für den bedingten Zugriff implementieren, die anhand kontextbezogener Faktoren wie dem Standort und dem Status des Geräts das Vertrauen in die BenutzerInnen und ihre Geräte herstellen.

Die Cloud-basierte Sicherheitsplattform von Duo schützt den Zugriff auf alle Anwendungen, für alle BenutzerInnen und jedes Gerät, von jedem Standort aus. Anhand von sechs wichtigen Funktionen haben wir den sicheren Zugriff vereinfacht, um Identitäts- und Geräterisiken zu vermeiden:

1. Benutzeridentitäten mit sicheren und flexiblen Multi-Faktor-Authentifizierungsmethoden überprüfen
2. Ein einheitliches Anmeldeerlebnis mit Single Sign-On von Duo bereitstellen, das zentralisierten Zugriff auf lokale Anwendungen und Cloud-Anwendungen bietet
3. Gerätetransparenz erhalten und ein detailliertes Verzeichnis aller Geräte pflegen, die auf Unternehmensanwendungen zugreifen
4. Über Integritäts- und Statusprüfungen für verwaltete und nicht verwaltete Geräte Gerätevertrauen herstellen, bevor Anwendungszugriff gewährt wird
5. Granulare Zugriffsrichtlinien durchsetzen, um den Zugriff auf diejenigen BenutzerInnen und Geräte einzuschränken, welche die Risikotoleranzlevels des Unternehmens erfüllen
6. Riskantes Anmeldeverwalten mit Duo Trust Monitor überwachen und erkennen oder Protokolle in Ihr SIEM exportieren, um verdächtige Ereignisse wie die Anmeldung eines neuen Geräts zur Authentifizierung oder die Anmeldung von einem unerwarteten Standort aus zu erkennen

Gründe, die für Duo sprechen

Beschleunigte Sicherheit

Duo liefert die Bausteine für Zero Trust in einer Lösung, die schnell und einfach für BenutzerInnen bereitgestellt werden kann. Je nach konkretem Anwendungsfall können einige Clients innerhalb weniger Minuten einsatzbereit sein.

Benutzerfreundlichkeit

BenutzerInnen können sich selbst registrieren, indem sie einfach eine App aus dem App Store herunterladen und sich anmelden. Wartungs- und Richtlinienkontrollen sind für AdministratorInnen einfach zu handhaben und bieten umfassende Transparenz.

Mit allen Anwendungen integrierbar

Unser Produkt ist so konzipiert, dass es unabhängig ist und mit bestehenden Systemen zusammenarbeiten kann. Mit Duo können Sie den Zugriff auf alle Arbeitsanwendungen für alle BenutzerInnen von überall aus schützen, unabhängig davon, welche IT- und Sicherheitsanbieter Sie nutzen.

Geringere Gesamtbetriebskosten

Da Duo einfach zu implementieren ist und keine Systeme ersetzt werden müssen, erfordert es weit weniger Zeit- und Kostenaufwand. So sind Sie schnell startklar und können mit der Einführung eines Zero-Trust-Sicherheitsmodells beginnen.

Referenzen

The Pandemic-hit World Witnessed a 150% Growth of Ransomware, https://cisomag.eccouncil.org/growth-of-ransomware-2020/, CISO Magazine, 5. März 2021

Exclusive: U.S. to give ransomware hacks similar priority as terrorism, https://www.reuters.com/technology/exclusive-us-give-ransomware-hacks-similar-priority-terrorism-official-says-2021-06-03/, Reuters, 3. Juni 2021

NIST Announces Tech Collaborators on NCCoE Zero Trust Project, https://www.hstoday.us/industry/emerging-innovation/nist-announces-tech-collaborators-on-nccoe-zero-trust-project/, Homeland Security Today, 24. Sept. 2021

FACT SHEET: Ongoing Public U.S. Efforts to Counter Ransomware, https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware, The White House, 13. Okt. 2021

Types of Encryption: Symmetric or Asymmetric? RSA or AES?, https://preyproject.com/blog/en/types-of-encryption-symmetric-or-asymmetric-rsa-or-aes/, Prey Project, 15. Juni 2021

What We Know About DarkSide, the Russian Hacker Group That Just Wreaked Havoc on the East Coast, https://www.heritage.org/cybersecurity/commentary/what-we-know-about-darkside-the-russian-hackergroup-just-wreaked-havoc, The Heritage Foundation, 20. Mai 2021

What We Can Learn From Ransomware Actor "Security Reports", https://www.coveware.com/blog/2021/6/24/what-we-can-learn-from-ransomware-actor-security-reports, Coveware, 24. Juni 2021

The State of Ransomware 2021, https://secure2.sophos.com/en-us/content/state-of-ransomware.aspx, Sophos, 2021

Data Mining Process: The Difference Between Data Mining & Data Harvesting, https://www.import.io/post/the-difference-between-data-mining-data-harvesting, Import.io, 23. April 2019

Ransomware: Enemy at The Gate, https://ussignal.com/blog/ransomware-enemy-at-the-gate, US Signal, 3. September 2021

2020 Data Breach Investigations Report, https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2020-data-breach-investigations-report.pdf, Verizon, 2020

Malware is down, but IoT and ransomware attacks are up, https://www.techrepublic.com/article/malwareis-down-but-iot-and-ransomware-attacks-are-up/, Tech Republic, 23. Juni 2020

One Ransomware Victim Every 10 Seconds in 2020, https://www.infosecurity-magazine.com/news/oneransomware-victim-every-10/, Infosecurity Magazine, 25. Februar 2021

Terrifying Statistics: 1 in 5 Americans Victim of Ransomware, https://sensorstechforum.com/1-5-americansvictim-ransomware/, Sensors Tech Forum, 19. August 2019

Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed $150 Billion in 2021, https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwidesecurity-and-risk-managem, Gartner, 17. Mai 2021

1 in 5 SMBs have fallen victim to a ransomware attack, https://www.helpnetsecurity.com/2019/10/17/smbsransomware-attack/, Help Net Security, 17. Oktober 2019

Ransomware – how to stop this growing, major cause of downtime, https://polyverse.com/blog/ransomware-how-to-stop-this-growing-major-cause-of-downtime, Polyverse.com

The strange history of ransomware, https://theworld.org/stories/2017-05-17/strange-history-ransomware, PRI The World, 17. Mai 2017

Ransomware Timeline, https://www.tcdi.com/ransomware-timeline, tcdi.com, 27. Dezember 2017

A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time, https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time, Digital Guardian, 2. Dezember 2020

One of the biggest US insurance companies reportedly paid hackers $40 million ransom after a cyberattack, https://www.businessinsider.com/cna-financial-hackers-40-million-ransom-cyberattack-2021-5, Business Insider, 22. Mai 2021

Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare, https://www.wired.com/story/atlantaspent-26m-recover-from-ransomware-scare, Wired.com, 23. April 2018

Cyber-attack: US and UK blame North Korea for WannaCry, https://www.bbc.com/news/world-uscanada-42407488, BBC.com, 19. September 2017

Ransomware: Now a Billion Dollar a Year Crime and Growing, https://www.nbcnews.com/tech/security/ransomware-now-billion-dollar-year-crime-growing-n704646, NBCNews.com, 9. Januar 2017

The Untold Story of NotPetya, the Most Devastating Cyber Attack in History, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world, Wired.com, 22. August 2018

Ransomware in Healthcare Facilities: The Future is Now, https://mds.marshall.edu/cgi/viewcontent.cgi?article=1185&context=mgmt_faculty, Marshall University Digital Scholar, Herbst 2017

New ransomware holds Windows files hostage, demands $50, https://www.networkworld.com/article/2265963/new-ransomware-holds-windows-files-hostage--demands--50.html, NetworkWorld.com, 26. März 2009

Preventing Digital Extortion, https://subscription.packtpub.com/book/networking_and_servers/9781787120365/4/ch04lvl1sec24/the-advancement-of-locker-ransomware-winlock, PackIt, Mai 2017

The Irreversible Effects of Ransomware Attack, https://www.crowdstrike.com/blog/irreversible-effectsransomware-attack, CrowdStrike, 20. Juli 2016

New Era of Remote Working Calls for Modern Security Mindset, Finds Thales Global Survey of IT Leaders, https://www.businesswire.com/news/home/20210914005014/en/New-Era-of-Remote-Working-Calls-for-Modern-Security-Mindset-Finds-Thales-Global-Survey-of-IT-Leaders, Business Wire, 14. Sept. 2021

FBI sees spike in cyber crime reports during coronavirus pandemic, https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic, The Hill, 16. April 2020

Symantec Security Summary - September 2021, https://symantec-enterprise-blogs.security.com/blogs/featurestories/symantec-security-summary-september-2021, Symantec Security, 27. Sept. 2021

INTERPOL report shows alarming rate of cyberattacks during COVID-19, https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19, Interpol, 4. August 2020

Gartner Top Security and Risk Trends for 2021, https://www.gartner.com/smarterwithgartner/gartner-topsecurity-and-risk-trends-for-2021, Gartner, 5. April 2021

Gartner Survey Reveals 82% of Company Leaders Plan to Allow Employees to Work Remotely Some of the Time, https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time, Gartner, 14. Juli 2020

Gartner Highlights Identity-First Security as a Top Security Trend for 2021, https://www.attivonetworks.com/blogs/gartner-identity-first-security-in-2021, Attivo, 27. April 2021

2021 SonicWall Cyber threat Report, https://www.sonicwall.com/medialibrary/en/white-paper/2021-cyberthreat-report.pdf, SonicWall, 2021

Top exploits used by ransomware gangs are VPN bugs, but RDP still reigns supreme, https://www.zdnet.com/article/top-exploits-used-by-ransomware-gangs-are-vpn-bugs-but-rdp-still-reigns-supreme, ZDNet.com, 23. August 2020

VPN exploitation rose in 2020, organizations slow to patch critical flaws, https://www.cybersecuritydive.com/news/trustwave-network-security-remote-access/602044/, Cybersecurity Dive, 18. Juni 2021

New research: How effective is basic account hygiene at preventing hijacking, https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html, Google Blog, 17. Mai 2019

Top cybersecurity statistics, trends, and facts, https://www.csoonline.com/article/3634869/top-cybersecuritystatistics-trends-and-facts.html, CSOonline.com, 7. Oktober 2021

Protecting Companies From Cyberattacks, https://www.inc.com/knowbe4/protecting-companies-fromcyberattacks.html, Inc.com, 20. September 2021

ThreatList: People Know Reusing Passwords Is Dumb, But Still Do It, https://threatpost.com/threatlistpeople-know-reusing-passwords-is-dumb-but-still-do-it/155996/, Threatpost, 25. Mai 2020

Synopsys Study Shows 91% of Commercial Applications Contain Outdated or Abandoned Open Source Components, https://www.securitymagazine.com/articles/92368-synopsys-study-shows-91-ofcommercial-applications-contain-outdated-or-abandoned-open-source-components, Security Magazine, 12. Mai 2020

Ransomware's Dangerous New Trick Is Double-Encrypting Your Data, https://www.wired.com/story/ransomware-double-encryption/, Wired.com, 17. Mai 2021

Combating Lateral Movement and the Rise of Ransomware, https://www.msspalert.com/cybersecurityguests/combating-lateral-movement-and-the-rise-of-ransomware, MSSP Alert, 24. Juni 2021

Lateral Movement, https://attack.mitre.org/tactics/TA0008/, MITRE| ATT&CK, 17. Oktober 2019

Industries Impacted by Ransomware, https://airgap.io/blog/industries-impacted-by-ransomware, AirGap.com

Defend Against and Respond to Ransomware Attacks, https://www.gartner.com/en/documents/3978727/defend-against-and-respond-to-ransomware-attacks, Gartner Research, 26. Dezember 2019

Executive Order on Improving the Nation's Cybersecurity, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, The White House, 12. Mai 2021

C11-3233828-00 10/22