WHITEPAPER

Ransomware-Abwehr mit Unified Security von WatchGuard

Inhaltsverzeichnis

EINFÜHRUNG

Das Aufkommen von Ransomware, der vielleicht lukrativsten Methode der Cyberkriminalität, markiert einen deutlichen Wandel in der Art und Weise, wie Internetkriminelle aus den Daten ihrer Opfer Profit schlagen. Mit Ransomware müssen sich die Angreifer nicht länger auf die Daten konzentrieren, die sie leicht weiterverkaufen können. Sie nutzen stattdessen den Wert aus, den die Daten für ihre Opfer darstellen. Selbst wenn es sich nicht um sonderlich sensible Daten handelt, sie sind möglicherweise für die betrieblichen Abläufe dringend notwendig. Indem sie die Daten „gefangen" nehmen und für die Freigabe ein Lösegeld fordern, können Angreifer sogar Daten zu Geld machen, für die sie andernfalls wahrscheinlich keine Verwendung gehabt hätten.

Aufgrund dieses Paradigmenwechsels geraten viele Unternehmen, die sich bisher für zu klein hielten, um ein lohnendes Ziel für Cyberangriffe zu sein, nun doch in das Visier der Cyberkriminellen.

WAS IST RANSOMWARE?

Bei Ransomware handelt es sich um einen hochentwickelten Malware-Angriff, der Computer in befällt und entweder den Benutzer komplett aussperrt oder Dateien so verschlüsselt, dass sie nicht verwendet werden können. Die Angriffe auf Ihre Geräte können auf verschiedene Arten erfolgen: Die Ransomware kann von einer bösartigen oder kompromittierten Website heruntergeladen, als Anhang einer Phishing-E-Mail eingeschleust oder via Exploit-Kits auf unsicheren Systemen abgeladen werden. Sobald sich die Ransomware auf Ihrem Computer befindet und ausgeführt wird, sperrt sie den Zugriff auf wichtige Teile Ihres Computers. Zu Anfang wurden einfach Dokumente auf Ihrem System verschlüsselt, so dass für die Arbeit benötigte Daten nicht mehr verfügbar waren.

Neuere Arten von Ransomware blockierten den Zugriff auf den Computer, indem Sie den Zugang zum Desktop sperrten oder den Computer neu starteten und in einen gesperrten Zustand versetzten. Die neuesten Formen von Ransomware kopieren wichtige Daten von Ihrem Computer. In allen Fällen meldet sich der Angreifer irgendwann mit einer „offiziellen" Lösegeldforderung sowie genauen Anweisungen und Zeitangaben, wie und wann eine Zahlung zu leisten ist, damit der Zugriff auf das Gerät wieder freigegeben bzw. der Code für die Entschlüsselung der gekaperten Dateien mitgeteilt wird.

KOSTENANSTIEG DURCH RANSOMWARE

Es leuchtet ein, dass Ransomware-Angriffe für unsere Gegner äußerst lukrativ sein können, aber bei neuesten Angriffen stiegen die Forderungen ins Astronomische. 2018 betrug die durchschnittliche Lösegeldforderung 41.000 Dollar. 2019 stieg diese Zahl um das Zweifache auf 84.000 Dollar, zum Teil aufgrund des Zusammenschlusses und der Zusammenarbeit vorher konkurrierender Banden von Cyberkriminellen.[1]

Das FBI sagte 2016 voraus, dass Cyberkriminelle mit Ransomware-Angriffen eine Milliarde Umsatz erzielen würden. Heute gehen Schätzungen davon aus, dass der Markt Ende 2021 zwanzigmal mehr Umsatz generieren wird.[2]

Leider erscheint die Lösegeldzahlung im Vergleich zu den insgesamt durch einen Ransomware-Angriff verursachten Kosten häufig das kleinere Übel zu sein. In die Berechnung der tatsächlichen Kosten eines Ransomware-Angriffs müssen sowohl alle Schäden an IT-Ressourcen, Zeit- und Kostenaufwand für die Wiederherstellung der Daten als auch Vertrauensverluste bei Kunden und Mitarbeitern einfließen. Mehr als ein Drittel der Ransomware-Opfer meldet Umsatzverluste, während 20 % unmittelbar nach einem erfolgreichen Ransomware-Angriff den Geschäftsbetrieb komplett einstellen mussten.[3] Untersuchungen zeigen außerdem, dass die durchschnittlichen Kosten für eine Geschäftsunterbrechung bei KMUs 2019 auf 141.000 Dollar stieg, bei einer jährlichen Steigerungsrate von 200 %.[4] Und es gibt nur wenige kleine Betriebe, die für einen derartigen Angriff gewappnet sind.

RANSOMWARE FÜHRT ZU PARADIGMENWECHSEL

Sicherheitsexperten haben lange und ausführlich über die Notwendigkeit diskutiert, sensible Daten zu schützen. Angesichts von Bedrohungen wie Identitätsdiebstahl und Betrug war es unumgänglich, der Sicherheit bestimmter Datentypen Vorrang einzuräumen. Der Schutz sensibler Daten ist alles andere als trivial, aber es hilft eine relativ einfache Formel: sensible Daten identifizieren, Schutzwälle um die Speicher- und Nutzungsorte dieser Daten errichten und die Daten selbst möglichst auch verschlüsseln.

Geschützt werden müssen vor allem die sensiblen Informationen, die für den Angreifer am wertvollsten sind, also in der Regel die Daten, die ein Angreifer am schnellsten und einfachsten verkaufen oder zum Erzielen sonstiger finanzieller Vorteile nutzen kann. Heutzutage sind diese Daten streng reguliert und viele Organisationen sind verpflichtet, sich beim Umgang mit diesen Daten an nationale und internationale Compliance-Richtlinien zu halten.

Mit dem Aufkommen von Ransomware hat sich die Formel zur Bewertung der relevanten Informationen gravierend verändert. Für den Angreifer ist jetzt nicht mehr der Marktwert der gekaperten Daten interessant, es geht vielmehr darum, wie wichtig die Daten für Sie bzw. Ihr Unternehmen sind. Selbst wenn es sich nicht um sonderlich sensible Inhalte handelt, werden diese Daten möglicherweise kurz- oder langfristig dringend für die betrieblichen Abläufe in Ihrer Organisation benötigt. Indem sie Ihre Daten in Geiselhaft nehmen und für die Freigabe ein Lösegeld fordern, können Angreifer sogar Inhalte zu Geld machen, für die sie andernfalls wahrscheinlich keine Verwendung gehabt hätten.

Aufgrund dieses Paradigmenwechsels geraten viele Unternehmen, von denen sich viele bisher für zu klein hielten, um ein lohnendes Ziel für Cyberangriffe zu sein, nun doch in das Visier zunehmend raffinierter Angreifer.

2018 betrug die durchschnittliche Lösegeldforderung 41.000 Dollar.

2019 hatte sich diese Zahl bereits mehr als verdoppelt.

Schätzungen zufolge werden die Einnahmen durch Ransomware 20-mal höher sein als 2016.

Die durchschnittlichen Kosten einer Geschäftsunterbrechung bei KMUs stieg im Jahr 2019 auf 141.000 Dollar, bei einer jährlichen Steigerungsrate von 200 %.

DIE 2. RANSOMWARE-WELLE

Während der ersten Ransomware-Welle (2016-2017) bestand die Strategie der Angreifer darin, so viele Leute wie möglich zu infizieren und kleinere Lösegelder zu verlangen, manchmal nur 100 Dollar. Anfang 2019, mit Beginn der zweiten Welle, wechselte das Angriffsmodell. Statt großflächig zu infizieren, konzentrierten sich die Angriffskampagnen jetzt auf spezifische Unternehmen. Die Angreifer arbeiteten wochen- oder monatelang, um Zugang zu bestimmten Unternehmen zu erlangen und dann möglichst viele Computer des Unternehmens zu infizieren.

Die Lösegeldforderungen bei diesen Angriffen stiegen auf mehrere Tausend Dollar. Der Anstieg der Lösegeldforderungen war möglich, da die Ransomware-Bedrohung den Bedarf an Cyberversicherungen ansteigen ließ. Wenn ein Ransomware-Angriff ein Opfer trifft, das über eine Cyberversicherung verfügt, hilft die Versicherung bei der Zahlung des Lösegelds. Damit steigt die Wahrscheinlichkeit, dass die betroffene Firma das Lösegeld bezahlt.

Ransomware im Angebot! Schwarzmarkt für Ransomware-Werkzeuge senkt Einstiegshürde

Der kontinuierliche Anstieg der Ransomware-Bedrohung ist zum Teil darauf zurückzuführen, dass Ransomware-Werkzeuge und -Dienste in den Weiten des Internet zum Kauf angeboten werden. Mit diesen Werkzeugen können nun auch technisch weniger versierte Angreifer Ransomware-Angriffe starten und sind in der Lage, trotz begrenzter Computerkenntnisse groß angelegte Ransomware-Kampagnen zu führen.

Das Aufkommen von Ransomware-as-a-Service-Angeboten ist ein weiterer, besorgniserregender Trend im Kampf gegen Ransomware. Gegen eine Beteiligung am Lösegeld bieten Full-Service-Shops inzwischen alles für einen Ransomware-Angriff an, von Malware-Samples über die Hosting-Infrastruktur bis hin zu Call-Centern, die den Opfern bei der Bezahlung des Lösegelds assistieren. Da jeder Möchtegern-Angreifer sich diese Tools einfach per Klick beschaffen kann, sollte es nicht überraschen, dass immer mehr kleine und mittlere Unternehmen Opfer großer Ransomware-Offensiven werden.

Ransomware im Rampenlicht - Maze

Im Januar 2020 sorgte die Ransomware-Kampagne von Maze für eine weitere Eskalation der Ransomware-Strategie. Zusätzlich zur Sperrung des Zugriffs auf Computer und Dokumente übertrug die Ransomware einige der Daten der betroffenen Computer zu einer Art Command-and-Control-System. Damit war die Brücke zu einem anderen Geschäftsmodell der Cyberkriminellen geschlagen, dem Verkauf gestohlener Daten. Bis 2016 erzielten Cyberkriminelle den meisten Umsatz mit dem Verkauf gestohlener Daten an beliebige Kunden. Durch die Fusion der beiden Geschäftsmodelle können die Angreifer jetzt mit dem gehackten Zugang zu einem Unternehmen zwei Einkommensströme anzapfen.

Noch besorgniserregender an diesen neuen Ransomware-Angriffen ist, dass die Betroffenen nun davon ausgehen müssen, dass ihre vertraulichen Daten über das Internet übertragen werden. Derartige Datenverluste spielen plötzlich auch im Hinblick auf Datenschutzgesetze in Kalifornien und Europa eine Rolle. Der Druck auf die Opfer von Ransomware-Angriffen ist plötzlich doppelt so hoch, da diese letztlich für die sichere Verarbeitung von personenbezogenen Daten verantwortlich sind.

HAUPTSCHAUPLATZ: ANWENDER

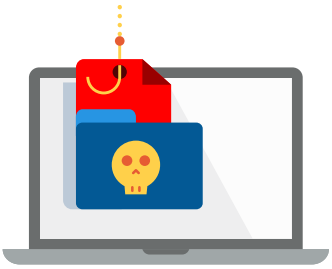
Cyberkriminelle nutzen zunehmend die Naivität der Anwender als hauptsächlichen Angriffsvektor und machen sich die mangelnden Kenntnisse über Cybersicherheit zu Nutzen. Mitarbeiter bilden daher die vorderste Front bei der Abwehr von Ransomware-Katastrophen. Ein falscher Klick auf einen Link oder eine Datei genügt, um das Räderwerk einer Ransomware-Infektion in Gang zu setzen. Hierbei führt unter anderem Panikmache oder Einschüchterung häufig zum Erfolg: Der Absender gibt sich beispielsweise als offizielle Behörde bzw. die Polizei aus oder schleust Malware über sorgsam ausgearbeitete E-Mails an eine vorab als Opfer auserkorene Person ins Unternehmen ein – die Angreifer sind ausgesprochen versiert und wissen, mit welchen Techniken sie die Wahrscheinlichkeit eines Klicks erhöhen können. Tatsächlich beginnen 90 % der heutigen Cyberangriffe mit erfolgreichen Phishing-Versuchen, bei dem Anwender dazu verleitet werden, auf einen Link zu klicken oder eine Datei herunterzuladen, mit der Malware übertragen wird oder mit der sich der Angreifer Zugriff verschafft.

Häufige Angriffsvektoren von Ransomware

Angreifer benutzen bei Ransomware-Kampagnen drei hauptsächliche Vektoren, um sich Zugang zu verschaffen:

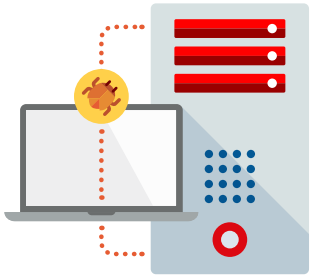
- Phishing eines Anwenders
- RDP-Missbrauch
- Scan-&-Exploit-Techniken

Phishing



Gartner zufolge werden im Jahr 2025 85 % der erfolgreichen Angriffe auf menschliches Fehlverhalten und nicht auf fortgeschrittene Malware zurückzuführen sein. Im Vergleich zur Technologie wird sich der menschliche Einflussfaktor viel langsamer entwickeln und am stabilsten bleiben. 83 % der Unternehmen sind bereits einem Phishing-Angriff zum Opfer gefallen, und da immer mehr Mitarbeiter im Home-Office arbeiten, steigt die Zahl der Phishing-Angriffe. E-Mails sind die bevorzugte Methode für diese Angriffe, obwohl auch Textnachrichten und Chat-Anwendungen dafür verwendet werden. Das Spear-Phishing und das so genannte Whaling, d. h. gezielte Angriffe auf CIOs oder andere Führungskräfte unter Nutzung firmeninterner E-Mail-Adressen (Business Email Compromise, BEC), findet ebenfalls immer häufiger statt. Dem FBI zufolge rührten von 2016 bis 2019 mehr als 26 Milliarden Dollar Verlust von dieser Art von BEC-Angriffen her.

RDP-Missbrauch



Als Folge der COVID-19-Pandemie wurden mehr als 1,5 Millionen RDP-Serververbindungen (Remote Desktop Protocol) über das Internet eingerichtet, um Mitarbeitern schnell den Remote-Zugriff zu ermöglichen, ohne allzu sehr auf die Sicherheit zu achten. Angriffe mit Credential-Stuffing- oder Brute-Force-Methoden gegen internetexponierte RDP-Dienste, VPN-Dienste und Benutzerkonten sind sehr häufig. Durch systematisches Erraten oder die Verwendung von Kennwortlisten und zuvor erbeuteten Anmeldedaten versuchen die Angreifer, die Authentifizierung für den Zugriff auf Geräte oder Dienste zu erzwingen.

Scan-and-Exploit-Techniken

Diese Angriffstechniken nutzen die Tatsache, dass viele Organisationen das Schwachstellen- und Patch-Management noch nicht adäquat handhaben. Für die Angreifer sind derartige Schwachstellen eine leichte Beute.

Tatsächlich sind es nur einige wenige Schwachstellen, von denen manche seit Jahren existieren, über die ein großer Anteil von Shareware-Angriffen ausgeführt wird. In wirksame Maßnahmen zu investieren, um Remote-Systeme zu analysieren und zu aktualisieren, ist also enorm wichtig, selbst wenn diese nicht an ein VPN angeschlossen sind. Einer Studie des Cybersicherheitsunternehmens SenseCy aus dem Jahr 2020 zufolge wurden bei den 180 untersuchten Sicherheitsvorfällen nur vier Schwachstellen ausgenutzt.

RANSOMWARE-PAYLOADS ENTDECKEN

Bis vor kurzem noch nutzte man in erster Linie Virenschutzprodukte, um Angriffe von Malware – beispielsweise Ransomware – abzufangen, bevor sie ein Netzwerk oder einen Computer infizieren konnten. Antiviruslösungen setzen dabei auf Experten, die neue Malware-Varianten suchen und in den bösartigen Dateien die charakteristischen Muster entdecken, die diese eindeutig identifizieren. Anhand dieser Muster – Signaturen, wenn man so will – können die Lösungen dann zuvor entdeckte Malware erkennen und blockieren, bevor sie in Ihr Netzwerk eindringen oder Ihre Computer infizieren kann.

Lange Zeit schienen solche Ansätze auf Basis von Signaturen vollkommen ausreichend zu sein, um der Mehrzahl der Malware-Anwendungen einen Riegel vorzuschieben. Diese älteren Virenschutzlösungen haben allerdings eine Achillesferse: Die auf der Erkennung von Mustern basierenden Lösungen sind immer reaktiv und niemals proaktiv. Ein Mensch oder ein automatisiertes System muss eine neue Malware-Form bereits gefunden und analysiert haben, bevor die Signaturen erstellt und geblockt werden können. Kurz gesagt: Ältere Lösungen sind nicht in der Lage, Malware zu identifizieren, die erstmalig auftritt.

Dieses Manko haben sich Angreifer zunutze gemacht und ihre Malware so entwickelt, dass sie signaturbasierte Virenschutzlösungen umgeht. Es gibt inzwischen Malware, die mithilfe von Dropper-Dateien in mehreren Phasen geladen wird. Des Weiteren wird versucht, Sicherheitsprogramme (auch Virenschutzsoftware) zu deaktivieren. Hinzu kommen Schadprogramme, die auf so unterschiedliche Weise codiert sind, dass es ihnen gelingt, sich unbemerkt an den neusten Signaturen vorbei zu schleichen.

Um dieser Gefahr zu begegnen, sind auch Virenschutzprodukte weiterentwickelt worden. Mit komplexeren Signaturregeln fangen sie nun eine breitere Palette von Samples (sogenannte Malware-Familien) ab. Einfache heuristische Lösungen versuchen, neue Malware anhand ihrer Dateiattribute zu identifizieren. Leider bedienen sich Kriminelle mittlerweile einer weiteren, äußerst effektiven Ausweichtechnik. Die Spielregeln haben sich dadurch radikal geändert und immer mehr neue Malware-Arten umgehen die Schutzlösungen. Diese Technik bezeichnet man als *Polymorphismus*.

Polymorphe Malware ist eine fachsprachliche Bezeichnung für Malware, die ihr Erscheinungsbild ständig verändert, um der signaturbasierten Erkennung zu entkommen. Mit Methoden, die Kriminelle als „Packen und Verschlüsseln" bezeichnen, können Angreifer eine Malware-Datei auf binärer Ebene wiederholt verändern, sodass sie gegenüber Virenschutzsoftware immer wieder anders dargestellt wird. Die bösartige, ausführbare Datei verhält sich zwar genauso wie zuvor, sieht jedoch aus wie eine komplett neue Datei. Dadurch erkennen Virenschutzprodukte Malware nicht mehr, die sie zuvor aufgespürt hätten. Dieser Polymorphismus war der Auslöser für die exponentielle Zunahme der Jahr für Jahr neu freigesetzten Malware-Varianten (Abbildung 1).

Wie verbreitet sind „Zero-Day-Schadprogramme" bzw. neue und einzigartige Malware-Formen? Leider hat sich dieses Problem aufgrund des Polymorphismus bereits massiv ausgebreitet. Webroot zufolge war 97 % der auf Endpoints gefundenen Malware unbekannt[5] und wäre daher von signaturbasierten Antivirusprogrammen wahrscheinlich nicht erkannt worden. Bestätigt werden diese Erkenntnisse von anderen Experten, die festgestellt haben, dass fast die Hälfte der Virenschutzprodukte versagt, wenn sie neu entwickelte Malware[6] am ersten Tag ihres Auftretens (Tag 0) abfangen sollen.

Die Quintessenz daraus ist: Signaturbasierte Virenschutzlösungen bewähren sich immer noch, wenn es um die Abwehr einfacher Malware in begrenztem Umfang geht. Sie versagen allerdings, wenn es gilt, die mittlerweile weit verbreiteten, auf Ausweichmanöver programmierten, hochentwickelten Malware-Arten zu erkennen, zu denen auch die ausgeklügelte Ransomware gehört, die in letzter Zeit so viele Unternehmen drangsaliert.

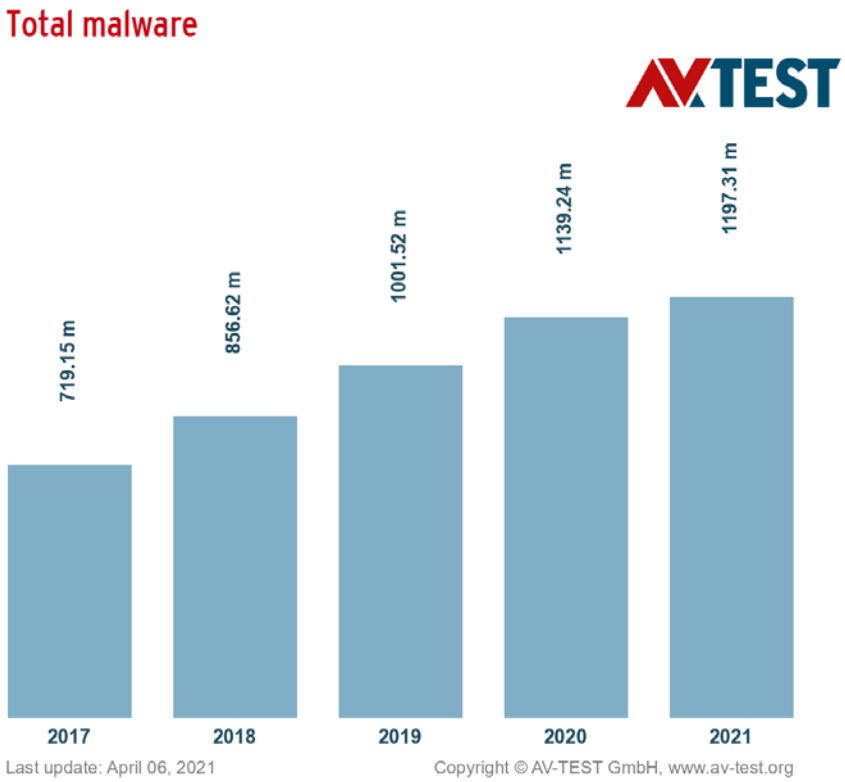
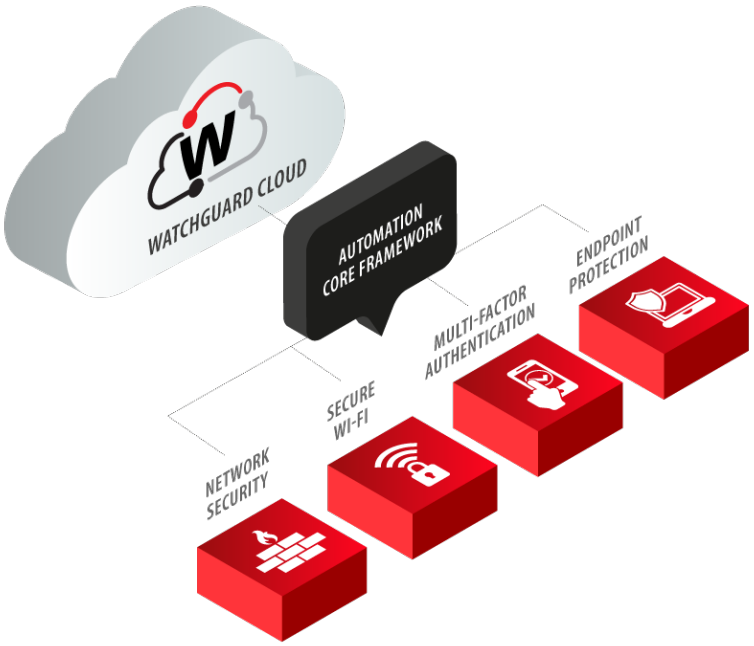


Abbildung 1: Anstieg der Malware im Zeitverlauf nach AV-Test.org [7]

RANSOMWARE MIT UNIFIED SECURITY VON WATCHGUARD BEKÄMPFEN

Ursprünglich von Lockheed Martin im Rahmen seines Modells „Intelligence Driven Defense“ zur Ermittlung und Prävention von Cyberangriffen veröffentlicht, identifiziert die sogenannte „Cyber Kill Chain“, was Angreifer tun müssen, um ihr Ziel zu erreichen, indem sie ein Netzwerk ins Visier nehmen, Daten exfiltrieren und den Fortbestand der Malware in der Organisation sicherstellen.

Durch den Einsatz einer homogenen Sicherheitsplattform ist es möglich, an verschiedenen Punkten der Kill Chain zu intervenieren, um so zu verhindern, dass der Angriff seinem Ziel näherkommt. Ausschlaggebend ist hier die Fähigkeit, Sicherheitsereignisse im Netzwerk und am Endpoint mit Bedrohungsdaten in Verbindung setzen zu können, um Malware-Angriffe zu entdecken, zu priorisieren und sie unverzüglich zu stoppen. Mit der mehrschichtigen Plattform von WatchGuard können sich Organisationen jeder Größenordnung vor raffinierten Malware-Bedrohungen schützen, d. h. auch vor Ransomware-Angriffen.



Um Ransomware-Angriffe zu stoppen, bevor sie überhaupt beginnen, müssen die drei üblichen Vektoren blockiert werden: Phishing, RDP-Missbrauch und Scan-&-Exploit-Techniken. WatchGuard bietet zahlreiche Lösungen an, die Ihre Anwender davor schützen, als Eintrittspforte für Ransomware-Angriff zu dienen. Dazu gehören DNS-Filter, Spam-Schutz, Patch-Management und Multifaktor-Authentifizierung. Eine einheitliche Sicherheitsplattform erleichtert die Arbeit Ihres IT-Teams durch die Integration fortgeschrittener Technologien, mit denen ein umfassendes, mehrschichtiges Sicherheitskonzept über Netzwerke, Anwender, Endpoints, Daten und Anwendungen hinweg (in der Cloud oder vor Ort im Unternehmen) ermöglicht wird. Die Sicherheit in einer einzigen Plattform zu vereinigen führt zu einer Effizienz, die mit isolierten Einzelsystemen schlicht nicht möglich ist. Häufige manuelle Aufgaben, welche die Zeit Ihres IT-Teams beanspruchen, können automatisiert werden.

WatchGuard hilft Ihrem IT-Team auf 10 Arten, sich gegen Ransomware zu verteidigen.

1. **Phishing-Versuche mit DNS-Filterung automatisch abwehren.** Das Phishing via E-Mail ist die gebräuchlichste Methode zum Starten eines Ransomware-Angriffs. Durch das Blockieren bösartiger E-Mails mit spamBlocker auf der Firebox und Spam-Schutz an Endpoints schützen Sie die Posteingänge Ihrer Anwender. Was, wenn eine E-Mail durchsickert und ein Anwender auf einen Link klickt, auf den er nicht hätte klicken sollen? DNSWatch kann Command-and-Control-Kanäle kappen und die Verbindungen zu den Cyberkriminellen blockieren. Müssen Sie Anwender im Home-Office schützen? DNSWatchGO bietet den gleichen Schutz auf Anwenderbasis, ohne ein VPN zu erfordern.

2. **Starke Anwenderidentitäten implementieren.** AuthPoint bietet eine effektive Multifaktor-Authentifizierung für Ihre Anwender und schützt Ihre Ressourcen, Konten und Daten vor dem Diebstahl von Anmeldedaten, Betrug und Phishing-Angriffen. Darüber hinaus macht die mobile App AuthPoint jeden Anmeldeversuch sichtbar, und die eindeutige Mobile-DNA stellt sicher, dass nur das Originalgerät eine Authentifizierung durchführen kann, wenn raffinierte Bedrohungen versuchen, mobile Geräte zu klonen.

3. **Sicherheitslücken einfach schließen.** Dem Ponemon Institute zufolge geben 57 Prozent der Opfer von Cyberangriffen an, dass die Anwendung eines Patches den Angriff verhindert hätte, und 34 % der Betroffenen sagen, sie hätten die Schwachstelle sogar gekannt, bevor der Angriff erfolgte. WatchGuards Patch Management-Lösung zur Verwaltung von Schwachstellen von Betriebssystemen und Drittanbieteranwendungen auf Windows-Workstations und -Servern hilft dabei, die Angriffsfläche für Ransomware-Angriffe zu verkleinern.

4. Ausführung unbekannter Anwendungen verhindern. Unser exklusiver Zero-Trust Application Service ermöglicht die kontinuierliche Überwachung von Endpoints und die Klassifizierung aller Aktivitäten, um anomales Verhalten von Anwendern, Geräten und Prozessen aufzudecken und zu blockieren. Adaptive Defense 360 entschärft Angriffe automatisch, indem es die Ausführung jeder unbekannten Anwendung blockiert, bis diese von unserem Machine-Learning-System und unserem Cybersicherheitsteam als vertrauenswürdig eingestuft wird.

5 **Malware am Gateway eliminieren.** Firewalls wie die WatchGuard Firebox sind sehr gut dazu geeignet, Malware-Dateien der ersten Angriffsphase zu blockieren, z. B. Dropper, die versuchen, noch schädlicheren Code einzuschleusen. Die Firebox bietet drei Schutzmechanismen: Gateway AV (Signaturen und Heuristiken), IntelligentAV (signaturlose, KI-gestützte Vorbeugung), und APT Blocker (fortgeschrittene Cloud Sandbox).

6 **Aktive Angriffe in Echtzeit sehen und überwachen.** Ransomware infiziert vorzugsweise Endpoints. Durch Visualisierung der Aktivitäten auf diesen Geräten können Bedrohungen erkannt und abgewehrt werden, bevor ein Schaden entsteht. Adaptive Defense 360 bietet eine klare und unmittelbare Sicht auf schadhafte Aktivitäten in der gesamten Organisation. Dank dieser Transparenz können Sicherheitsteams schnell das Ausmaß eines Angriffs beurteilen und entsprechende Maßnahmen ergreifen.

7 **Telemetriedaten korrelieren, um den Kontext zu sehen.** Cyberkriminelle sind Profis, wenn es darum geht, traditionelle Sicherheitssysteme zu umgehen. Sie führen getarnte, zielgerichtete Angriffe aus, um ihren Fußabdruck zu verkleinern und im Schatten zu bleiben, so dass manche Angriffe leicht unbemerkt bleiben. Als Teil der WatchGuard Firebox verwendet unsere ThreatSync-Lösung einen ressourcenschonenden Host-Sensor und die Cloud, um Telemetriedaten verschiedener Geräte in Ihrer Sicherheitsumgebung zu korrelieren und so blitzschnell Bedrohungen ausmachen und eliminieren zu können, die sonst unerkannt blieben.

8 **Dateiverschlüsselungen aufhalten, ohne einen Finger zu rühren.** Host Ransomware Prevention (HRP) verwendet eine Verhaltensanalyse-Engine und Köderverzeichnisse, um eine Vielzahl von Aktivitäten zu überwachen und zu erkennen, ob eine Aktion mit einem Ransomware-Angriff in Verbindung steht oder nicht. Auf diese Weise kann HRP bei ernsthaften Gefahren automatisch einen Ransomware-Angriff verhindern – noch bevor am Endpoint eine Dateiverschlüsselung stattfindet.

9 **Endpoints einfach wiederherstellen.** Wenn Malware ausgeführt wird, erstellt, modifiziert oder löscht sie häufig Systemdateien und Registry-Einstellungen und ändert Konfigurationseinstellungen. Diese Veränderungen oder Überreste, die zurückbleiben, können Systemfehler und Instabilitäten verursachen oder sogar neuen Angriffen Tür und Tor öffnen. In den wenigen Fällen, in denen Malware ausgeführt wird, stellt Adaptive Defense 360 den Zustand wieder her, den die Endpoints vor der Malware-Infektion hatten.

10 **Schnellere Gefahrenerkennung.** WatchGuards Threat Hunting and Investigation Service hilft beim Aufdecken von Hacking-Versuchen und LotL-Angriffen (Living off the Land). Unsere Sicherheitsexperten analysieren verdächtige Fälle, um neue und einmalige Umgehungstechniken (TTPS) im Ereignisstrom auszumachen. Auf dieser Grundlage erstellen wir neue Regeln zu Angriffsindikatoren (Indicators of Attack, IoA), die auf den Endpoints implementiert werden können, um sie vor neuen Angriffen zu schützen.

1. https://www.darkreading.com/risk/average-ransomware-payments-more-than-doubled-in-q4-2019/d/d-id/1336893
2. https://www.natlawreview.com/article/ransomware-attacks-predicted-to-occur-every-11-seconds-2021-cost-20-billion
3. https://www.scribd.com/document/320027570/Malwarebytes
4. https://www.businesswire.com/news/home/20191016005043/en/Cost-Ransomware-Related-Downtime-Increased-200-Percent
5. http://webroot-cms-cdn.s3.amazonaws.com/7814/5617/2382/Webroot-2016-Threat-Brief.pdf
6. http://labs.lastline.com/lastline-labs-av-isnt-dead-it-just-cant-keep-up
7. https://www.av-test.org/en/statistics/malware/

ÜBER WATCHGUARD

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Netzwerksicherheit, Endpoint-Sicherheit, sicheres WLAN, Multifaktor-Authentifizierung und Network Intelligence. Über 18.000 Vertriebspartner und Dienstleister im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Services des Unternehmens und sorgen somit für den Schutz von 250.000 Kunden. Die Philosophie von WatchGuard ist es, hochprofessionelle Sicherheitslösungen für Unternehmen jeder Größenordnung und Art zu realisieren. Das macht WatchGuard insbesondere für mittelständische und dezentral aufgestellte Unternehmen zum idealen Anbieter. Neben der Zentrale in Seattle im US-Bundesstaat Washington unterhält das Unternehmen Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum. Weitere Informationen finden Sie unter WatchGuard.com/de.

Wenn Sie mehr über WatchGuard, unsere Werbeaktionen und Updates erfahren möchten, folgen Sie uns auf Twitter @WatchGuard, auf Facebook oder auf unserer Seite auf LinkedIn. Lesen Sie auch unseren InfoSec-Blog Secplicity. Darin wird einfach und nachvollziehbar beschrieben, wie Sie den neuesten Bedrohungen am besten begegnen. Hier geht's zum Blog: www.secplicity.org

DEUTSCHLAND, ÖSTERREICH, SCHWEIZ +49 700 92229333 INTERNATIONALER VERTRIEB +1.206.613.0895 www.watchguard.com/de