Ransomware bleibt draußen

Inhaltsverzeichnis

Inhalt

Was ist Ransomware?

Bei Ransomware handelt es sich um einen hochentwickelten Malware-Angriff, der Computer in Geiselhaft nimmt und entweder den Benutzer komplett aussperrt oder Dateien so verschlüsselt, dass sie nicht verwendet werden können. Derartige Angriffsformen verschaffen sich auf verschiedenen Wegen Zugang zu Ihrem Gerät. 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 sie einmal im System ausgeführt worden ist, sperrt sie entweder den Computer oder verschlüsselt bestimmte Dateien. Der Angreifer meldet sich dann 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 bekannt gegeben wird.

Ransomware-Angriffe machen Schlagzeilen:

- Ende Oktober 2016 waren drei Kliniken der Stiftung Northern Lincolnshire and Goole NHS Foundation Trust gezwungen, geplante Operationen und Termine für ambulante Untersuchungen abzusagen, nachdem das komplette System aufgrund einer Infektion mit Globe2 Ransomware heruntergefahren werden musste.[1]
- Von der St. Louis Public Library forderten Hacker ein Lösegeld in Höhe von 35.000 US-Dollar für die Wiederherstellung von Daten, die bei einem Ransomware-Angriff auf mehr als 700 Computer in den 17 Zweigstellen des Bibliotheksystems gekapert worden waren.[2]
- Im März 2016 musste das Hard Times Café in Rockville, Maryland, für eine Woche die Tore schließen und sein POS-System komplett neu aufbauen, nachdem es – wie insgesamt acht lokale Unternehmen – Opfer eines Ransomware-Angriffs geworden war. [3]
- Die Bigfork Public Schools büßten bei einem Ransomware-Angriff sämtliche Daten ein, darunter die Noten der Schüler und das Bezirksverzeichnis mit den Kontaktdaten für Eltern und Lehrer sowie die Sozialversicherungsnummern. [4]
- Im Januar 2017 konnte das Personal im romantischen Seehotel Jägerwirt in der österreichischen Skiregion Turracher Höhe für neu ankommende Gäste keine Schlüsselkarten mehr ausstellen, weil ein Ransomware-Angriff das elektronische Schlüsselsystem lahm gelegt hatte. [5]

In diesem Whitepaper werden wir beleuchten, welche Bedrohung Ransomware für kleine bis mittlere Unternehmen tatsächlich darstellt, einige eindeutige Merkmale von Ransomware benennen und Möglichkeiten zur Bekämpfung von Ransomware-Angriffen aufzeigen.

Ransomware belauert kleine bis mittelständische Unternehmen

Ransomware gehört zu den Sicherheitsbedrohungen, über die heute am meisten gesprochen und geschrieben wird. Was mit einigen wenigen, Aufsehen erregenden Angriffen einer Handvoll Malware-Varianten begann, hat sich mittlerweile zu einer virulenten Bedrohungslage entwickelt. Selbst unqualifizierte Hacker sind inzwischen in der Lage, Unternehmen unabhängig von Größe oder Komplexität mit hochwirksamen Ransomware-Kampagnen zu attackieren. In der Zeit von Januar bis September 2016 nahmen die Ransomware-Angriffe gegen Unternehmen im Vergleich zum Gesamtjahr 2015 um dreihundert Prozent zu. Im selben Zeitraum stieg die Häufigkeit der Ransomware-Angriffe auf Unternehmen von einem Angriff alle zwei Minuten auf einen Angriff alle 40 Sekunden.

Kleine bis mittlere Unternehmen werden unverhältnismäßig häufig Opfer von Ransomware – oftmals weil ihnen die technischen Kenntnisse und Werkzeuge zur Abwehr solcher Übergriffe fehlen. Studien haben ergeben, dass mehr als 50 Prozent der kleinen und mittelständischen Unternehmen bereits einmal Opfer von Ransomware-Angriffen waren. Von diesen Geschädigten entschieden sich 48 Prozent zur Zahlung des geforderten Lösegelds, um ihre Daten zurückzugewinnen.[7] Zwar wird generell davon abgeraten, Lösegeld zu zahlen, doch zwingt Ransomware Unternehmen häufig zu einer schnellen geschäftsrelevanten Entscheidung – bei der eventuelle Bedenken, ob man der Forderung des Angreifers nachkommen sollte oder nicht, angesichts der dringend benötigen Daten in den Hintergrund treten.

Ransomware führt zu Paradigmenwechsel

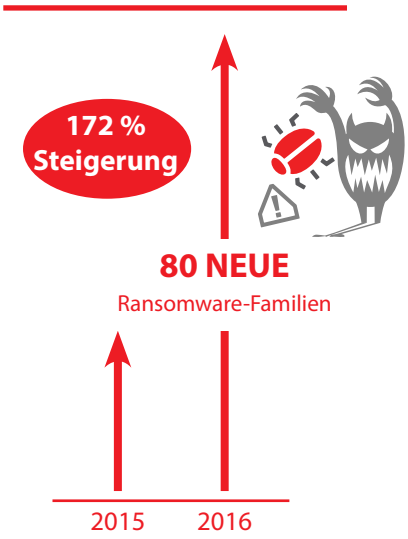
Sicherheitsexperten haben lange und ausführlich über die Notwendigkeit diskutiert, sensible Daten zu schützen. Angesichts von Bedrohungen wie Identitätsdiebstahl und Betrug war es unumgänglich, der Sicherheit bestimmter Datentypen Vorrang einzuräumen. Der Schutz sensibler Daten ist alles andere als nebensächlich, die entsprechende Formel relativ einfach: 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-Initiativen 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 selbst Inhalte zu Geld machen, für die sie andernfalls wahrscheinlich keine Verwendung gehabt hätten.

Aufgrund dieses Paradigmenwechsels gerät eine Fülle von Unternehmen – von denen sich viele bisher für zu klein hielten, um ein lohnendes Ziel für Cyberangriffe zu sein – nun doch in das Visier einer Meute zunehmend dilettantischer Angreifer.



Ransomware im Angebot! Schwarzmarkt für Ransomware-Werkzeuge senkt Einstiegshürde

Ransomware hat mittlerweile das Ausmaß einer Epidemie erreicht. Laut eines Berichts von Trend Micro wurden in der ersten Hälfte des Jahres 2016 80 neue Ransomware-Familien entdeckt, was einem Anstieg von 172 Prozent gegenüber dem Vorjahr entspricht.[8] Dieses Anschwellen der Ransomware-Gefahr ist auf die zunehmende Anzahl von Ransomware-Werkzeugen und -Services zurückzuführen, die im Darknet erhältlich sind. Mit diesen Werkzeugen können auch technisch weniger versierte Personen Ransomware-Angriffe starten. Solche Möchtegern-Angreifer sind nun in der Lage, trotz begrenzter Computerkenntnisse groß angelegte Ransomware-Feldzüge zu führen.

Das Aufkommen von Ransomware-as-a-Service-Angeboten ist ein weiterer, Besorgnis erregender Trend im Kampf gegen Ransomware. Das Leistungsspektrum zweifelhafter „Full-Service-Anbieter" reicht mittlerweile von Malware-Samples und Hosting-Infrastrukturen bis hin zu Call Centern, die Opfern bei der Zahlung des Lösegelds helfen – Angreifer erhalten für einen bestimmten Prozentsatz des gezahlten Lösegelds alles, was sie brauchen.

Da jeder Möchtegern-Angreifer sich diese Hilfsmittel einfach per Klick beschaffen kann, sollte es nicht überraschen, dass immer mehr kleine und mittlere Unternehmen Opfer großer Ransomware-Offensiven werden. Laut Berichten von Kaspersky Labs wurden 42 Prozent der kleinen und mittleren Unternehmen in den vergangenen zwölf Monaten Opfer eines Ransomware-Angriffs. Damit ist Ransomware zu der gefährlichsten Bedrohung avanciert, der kleine und mittlere Unternehmen heutzutage ausgesetzt sind.

Ausnutzung des schwächsten Glieds: Mitarbeiter

Mitarbeiter bilden die vorderste Front bei der Abwehr von Ransomware-Katastrophen. Leider sind dieselben Mitarbeiter in vielen kleinen bis mittleren Unternehmen auch die größte und wichtigste Sicherheitslücke. 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.

Die häufigste Ursache für Ransomware-Infektionen in Unternehmen sind Mitarbeiter, die dazu verleitet werden, in E-Mails Links anzuklicken oder Dateien zu öffnen. Wenn solche E-Mails breit gestreut an eine Vielzahl von Empfängern gesendet werden, spricht man von Phishing. Ein gezielteres Vorgehen mit einem zur Steigerung der Erfolgsquote sorgsam auf bestimmte Unternehmen oder Mitarbeiter abgestimmten Angriff bezeichnet man als Spear-Phishing. In beiden Fällen sind E-Mails die bei weitem häufigste Methode zum Einschleusen von Ransomware. Dabei erfolgen 31 Prozent der Infektionen durch Anklicken eines Links und 28 Prozent beim Öffnen eines E-Mail-Anhangs.[9]

Kostenanstieg durch Ransomware

Es versteht sich von selbst, dass Ransomware-Angriffe für unsere Gegner äußerst lukrativ sein können. 2016 wurde Lösegeld in Höhe von jeweils durchschnittlich 679 US-Dollar gefordert – mehr als das Doppelte der Forderungen des Vorjahres. Diese lagen bei durchschnittlich 294 US-Dollar.[10] Angesichts von FBI-Angaben, laut derer sich die Einnahmen der Internetkriminellen mit Ransomware 2016 auf eine Milliarde Dollar belaufen,[11] zeichnet die Summe von 679 US-Dollar ein katastrophales Bild des Umfangs und Erfolgs von Ransomware-Angriffen.

Leider erscheint die Lösegeldforderung 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. 2016 meldeten 34 Prozent der Ransomware-Opfer Umsatzverluste, während 20 Prozent unmittelbar nach einem erfolgreichen

Ransomware-Angriff den Geschäftsbetrieb komplett einstellen mussten.[12] Untersuchungen haben gezeigt, dass kleinen Betrieben durch einen erfolgreichen Ransomware-Angriff Kosten in Höhe von bis zu 99.000 US-Dollar entstehen können.[13] Und es gibt nur wenige kleine Betriebe, die für einen derartigen Angriff gewappnet sind.

Ransomware verhindern – eine Herausforderung

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. Antivirenlösungen 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 zur Abwehr erstellt 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 ausgerüstet, dass sie signaturbasierte Virenschutzlösungen umgeht. Es tritt inzwischen Malware auf, 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. Das sind nur einige der mehr als 500 Ausweichtaktiken,[14] die Experten bei den neuesten ausgefeilten Malware-Varianten beobachtet haben.

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-Samples kommen an den Lösungen vorbei. Diese Technik bezeichnet man als Polymorphismus.

Polymorphe Malware ist eine fachsprachliche Bezeichnung für Malware, die ihr Erscheinungsbild ständig verändert, um von Signaturen nicht erkannt zu werden und Abwehrmechanismen 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 und wird von Virenschutzprodukten auch als solche erkannt. Dadurch wird die zuvor identifizierte Malware außer Acht gelassen. Dieser Polymorphismus war der Auslöser für die exponentielle Zunahme der Jahr für Jahr neu freigesetzten Malware-Varianten (Abbildung 1). Da pro Jahr mehr als 140 Millionen neue Malware-Varianten zu bekämpfen sind, ist den signaturbasierten Virenschutzprodukten mittlerweile die Luft ausgegangen.

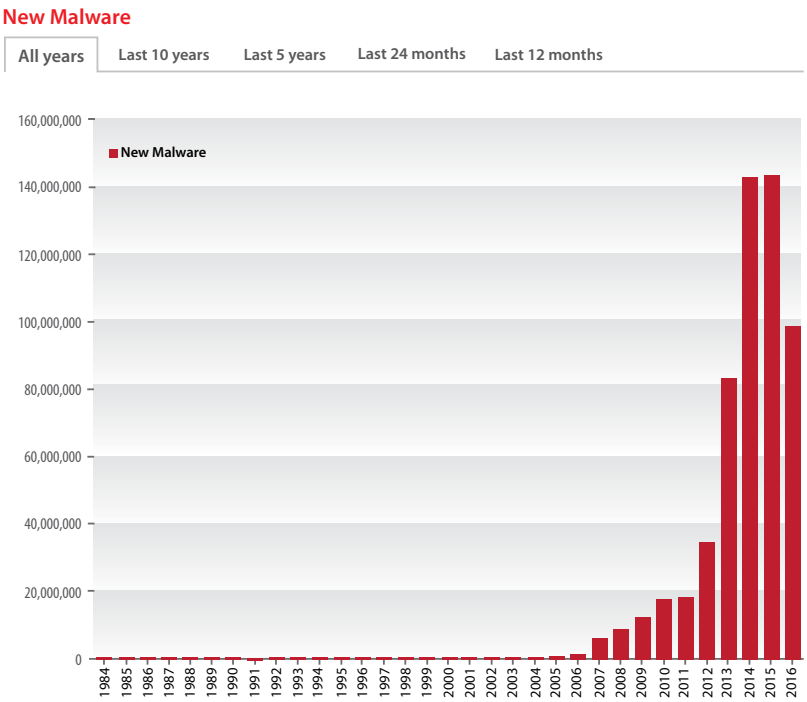


Abbildung 1: Anzahl der neuen Malware-Samples pro Jahr, lt. AV-Test.org[15]

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 waren 97 Prozent der auf Endgeräten gefundenen Malware-Arten einzigartig[16], d. h. sie waren noch niemals zuvor auffällig geworden und wären von signaturbasierten Virenschutzlösungen höchstwahrscheinlich auch nicht abgefangen worden. Bestätigt werden diese Erkenntnisse von anderen Experten, die festgestellt haben, dass fast die Hälfte der Virenschutzprodukte versagt, wenn sie neu entwickelte Malware[17] 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-Samples zu erkennen, zu denen auch die ausgeklügelte Ransomware gehört, die in letzter Zeit so viele Unternehmen drangsaliert.

Erkennen moderner Ransomware

Dass viele Organisationen sich nicht mehr allein auf Virenschutzlösungen verlassen können, heißt nicht, dass sie hilflos den Fängen einer immer perfideren Ransomware-Bedrohung ausgeliefert sind. Ransomware entwickelt sich zwar in einem rasanten Tempo weiter, doch haben viele Ransomware-Samples identische Eigenschaften, die Anzeichen für eine Bedrohung sind.

Einige charakteristische Verhaltensweisen von Ransomware:

- **Lösegeldforderung.** Das Opfer eines Daten-Kidnappings mag zunächst anderer Meinung sein, doch ist die bloße Tatsache, dass Ransomware ihre Anwesenheit gegenüber einem Opfer zu erkennen gibt, eine Schwachstelle des Angriffs. Durch die Bekanntgabe ihrer Existenz liefert die Malware Hinweise, die analysiert und dann verwendet werden können, um identische Infektionen in Zukunft zu verhindern.
- **Änderungen bei Verschlüsselung und Entropie.** Nur wenige Ransomware-Angreifer beherrschen die Kunst der Kryptographie. Viele Hacker arbeiten mit Kryptographie-API (beispielsweise Microsoft CryptoAPI), damit sie sicher sein können, dass ihre Verschlüsselung nicht geknackt werden kann und Best Practices entspricht. Erfreulicherweise macht es gerade die Verwendung dieser Kryptobibliotheken einfacher, Ransomware-Angriffe zu erkennen, bevor größerer Schaden angerichtet werden kann. Andere Verschlüsselungsmethoden helfen ebenfalls bei der Erkennung, da sie unweigerlich zu deutlichen Änderungen der Entropie führen, wodurch wiederum Alarmfunktionen ausgelöst werden können.
- **Verdeckte „Command and Control"-Strukturen.** In vielen Fällen muss Malware, die einen Ransomware-Angriff durchführen will, eine Verbindung zu einem bösartigen Server herstellen und den Verschlüsselungscode zur Chiffrierung der Dateien eines Opfers anfordern.
- **Rechteausweitung.** Ransomware versucht, sich Administratorrechte zu verschaffen, um Sicherheitsfunktionen der kompromittierten Systeme deaktivieren zu können.
- **Löschen von Samples.** Üblicherweise löscht Ransomware das erste Sample, mit dem ein System infiziert wurde, um eine genauere Analyse und Rückentwicklung (Reverse Engineering) zu verhindern.

Ransomware-Bedrohung mit WatchGuard abwehren

WatchGuard ist der Überzeugung, dass ein wirksamer Schutz gegen Ransomware eine Lösung auf Enterprise-Niveau erfordert, die Ransomware-Angriffe verhindert, erkennt und abwehrt. Ausschlaggebend ist hier die Fähigkeit, Sicherheitsereignisse im Netzwerk und am Endpunkt mit detaillierten Analysen der Bedrohungslage in Verbindung setzen zu können. Dadurch lassen sich potenzielle Angriffe noch früher erkennen und bewerten. Sofortmaßnahmen zur Abwehr erfolgen ohne Verzögerung.

Mit der WatchGuard Total Security Suite können sich Organisationen jeder Größenordnung gegenüber raffinierten Malware-Bedrohungen schützen, d. h. auch gegen Ransomware-Angriffe. Die Total Security Suite ist das erste UTM-Serviceangebot, mit dem Organisationen – unabhängig von ihrer Größe –Ransomware nicht nur erkennen und abwehren, sondern auch von vornherein verhindern können.

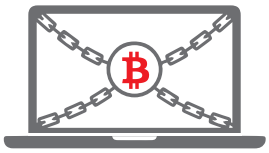
Mit der WatchGuard Total Security Suite erhalten Organisationen:

Transparenz bis zum Endpunkt dank Threat Detection and Response

Ransomware infiziert vorzugsweise Endgeräte. Durch Visualisierung der Ereignisaktivitäten auf diesen Geräten können Bedrohungen erkannt und abgewehrt werden, bevor überhaupt ein Schaden entsteht. Threat Detection and Response, der neue Sicherheits-Service von WatchGuard, vereint über den WatchGuard Host Sensor mehrere Erkennungsformen zum Aufspüren selbst raffiniertester Malware-Bedrohungen. Unser innovatives Host Ransomware Prevention-Modul bietet zudem die Möglichkeit, Ransomware-Vorfälle zu erkennen und die zugehörigen Prozesse abzubrechen, bevor sie Schaden anrichten können.

Hauptkomponenten von WatchGuard Threat Detection and Response

Verhaltensanalyse und Honeypots – Da Malware-Bedrohungen bestimmten Verhaltensmustern folgen, trägt die Beobachtung dieser Aktivitäten zuverlässig zur Erkennung unbemerkter Malware-Varianten bei. Mithilfe von Verhaltensanalysen sowie aktuellen Verzeichnissen der jeweils im Umlauf befindlichen Gefahren überprüft HRP (Host Ransomware Prevention) eine Vielzahl von Merkmalen und ist somit in der Lage zu erkennen, ob ein Ereignis 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 Endpunkt eine Dateiverschlüsselung stattfindet.



- Hochentwickelte Heuristik – Statt sich auf Signaturen zu verlassen, sucht TDR anhand von Regeln oder Algorithmen nach Hinweisen, die auf bösartige Absichten hindeuten könnten. Diese Erkennungsmethode kann eine Bedrohung im Nu identifizieren – selbst wenn die Infektion noch gar nicht stattgefunden hat. TDR setzt mit dem WatchGuard Host Sensor über 175 Heuristiken ein.
- Threat Intelligence auf Enterprise-Niveau – WatchGuard Threat Detection and Response nutzt Bedrohungsanalysen auf Enterprise-Niveau um zu beurteilen, ob es sich bei einem verdächtigen Ereignis um eine bekannte Bedrohung handelt.

Best-in-Class-Lösungen im Rahmen der Netzwerksicherheit mit Firebox UTM

Das Netzwerk spielt als Abwehrschicht eine wichtige Rolle beim Schutz Ihres Unternehmens vor Ransomware. Einblicke in ungewöhnliche oder gesperrte Datenbewegungsmuster, Besuche bösartiger oder riskanter Websites sowie das Erkennen von Botnets und anderen Bedrohungen sind entscheidende Punkte jeder Strategie zur Abwehr von Ransomware.

Hauptkomponenten der WatchGuard UTM-Lösung:

- Leistungsstarke Webfilter. WebBlocker verwehrt Benutzern automatisch den Zugriff auf bekannte bösartige Websites, aktiviert allerdings auch URL-Filter, um riskante und unangemessene Websites zu sperren, auf denen sich möglicherweise Malware eingenistet hat.
- Schutz vor Bedrohungen durch E-Mails. Ausgestattet mit der branchenführenden RPD-Technologie (Recurrent Pattern Detection) bietet der WatchGuard spamBlocker dauerhaften und sofortigen Schutz gegenüber verseuchten E-Mails – nahezu 100 Prozent der unerwünschten und gefährlichen E-Mails werden abgefangen.
- Schutz gegen bekannte Bedrohungen – Mithilfe eines branchenführenden, leistungsstarken Scanning-Moduls prüft WatchGuard Gateway Antivirus den Datenverkehr in allen gängigen Protokollen und bietet auf diese Weise Echtzeitschutz vor bekannten Viren, Trojanern, Würmern, Spyware und Rogueware.

Schutz vor Zero-Day-Gefahren mit WatchGuard APT Blocker

WatchGuard APT Blocker macht sowohl den sich schnell verändernden als auch permanenten Bedrohungen den Garaus: Eine moderne Cloud-Sandbox, in der physische Hardware simuliert wird, spürt Malware auf, die darauf ausgelegt ist, die Abwehr traditioneller Netzwerkstrukturen auszuhebeln.

Hauptkomponenten der WatchGuard ATP Blocker-Lösung:

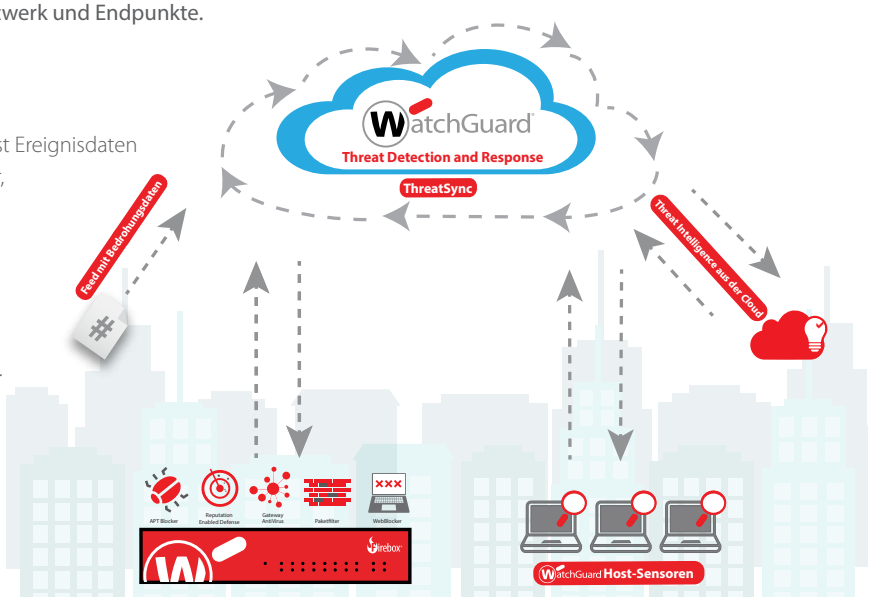
- **Verhaltensanalyse**. WatchGuard APT Blocker nutzt das Prinzip der Verhaltensanalyse, um festzustellen, ob eine Datei bösartig ist. Verdächtige Dateien werden identifiziert und an eine Cloud-basierte Sandbox weitergegeben, in der Code emuliert, ausgeführt und analysiert wird, um sein Bedrohungspotenzial zu bestimmen.
- **Vollständige Systememulation.** Moderne Malware-Formen – insbesondere APT (Advanced Persistent Threats), Ransomware und Zero-Day-Angriffe – sind so konzipiert, dass sie herkömmliche Verteidigungsmechanismen erkennen und umgehen. Die vollständige Systememulation von APT Blocker, bei der sowohl die physische Hardware als auch CPU und Speicher simuliert werden, bietet umfassenden Schutz gegen fortschrittliche Malware.

Verwertbare Einblicke mit dem Korrelationsmodul ThreatSync

Korrelation ist die einzige Möglichkeit, einen vollständigen Überblick über die Sicherheit in Ihrem Unternehmen zu erhalten. ThreatSync ist die neue Cloud-basierte Engine von WatchGuard zur Korrelation und Bewertung von Bedrohungen. Sie liefert verwertbare Einblicke zu Angriffen auf Netzwerk und Endpunkte.

Hauptkomponenten der WatchGuard ThreatSync-Lösung:

- Vollständige Transparenz von Anfang bis Ende ThreatSync erfasst Ereignisdaten von der WatchGuard Firebox und dem WatchGuard Host Sensor, setzt diese mit aktuellen Cloud-basierten Informationen zur Bedrohungslage in Verbindung und analysiert sie.
- Umfassende Bewertung von Bedrohungen. Durch die gezielte Bewertung können die Sicherheitsverantwortlichen im Handumdrehen erkennen, welche Bedrohungen am gefährlichsten sind und umgehende Aufmerksamkeit erfordern.



1. http://www.bbc.com/news/uk-england-humber-37822084
2. https://threatpost.com/st-louis-public-library-recovers-from-ransomware-attack/123297/
3. http://wtop.com/money/2016/03/hard-times-cafe-in-rockville-hit-with-ransomware/
4. http://flatheadbeacon.com/2016/11/23/malicious-software-hits-bigfork-school-district-computer-system/
5. http://www.thelocal.at/20170128/hotel-ransomed-by-hackers-as-guests-locked-in-rooms
6. https://securelist.com/analysis/kaspersky-security-bulletin/76757/kaspersky-security-bulletin-2016-story-of-the-year/
7. https://www.carbonite.com/en/news/ponemon-institute-ransomware-release/
8. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-ransomware-operators-find-ways-to-bring-in-business
9. https://blog.barkly.com/ransomware-statistics-2016
10. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf
11. http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/
12. https://www.scribd.com/document/320027570/Malwarebytes
13. https://business.kaspersky.com/cryptomalware-report-2016/5971/
14. http://labs.lastline.com/evasive-malware-gone-mainstream
15. https://www.av-test.org/en/statistics/malware/
16. http://webroot-cms-cdn.s3.amazonaws.com/7814/5617/2382/Webroot-2016-Threat-Brief.pdf
17. http://labs.lastline.com/lastline-labs-av-isnt-dead-it-just-cant-keep-up

Über WatchGuard

WatchGuard Technologies gehört zu den führenden Anbietern im Bereich Netzwerksicherheit. Mehr als 75.000 Unternehmen weltweit vertrauen auf die ausgeklügelten Schutzmechanismen auf Enterprise-Niveau, wobei dank der einfachen Handhabung insbesondere kleine bis mittlere sowie dezentral aufgestellte Unternehmen vom Einsatz profitieren. Neben der Zentrale in Seattle im US-Bundesstaat Washington verfügt WatchGuard über Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum. Weitere Informationen finden Sie unter WatchGuard.com.

Wenn Sie mehr über WatchGuard, unsere Werbeaktionen und Updates erfahren möchten, folgen Sie uns auf Twitter @WatchGuard, auf Facebook oder 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.de

Teilenr. WGCE66990_021217