SOPHOS

FIREWALL BEST PRACTICES ZUR ABWEHR VON RANSOMWARE

Sophos-Whitepaper August 2020

Firewall Best Practices zur Abwehr von Ransomware

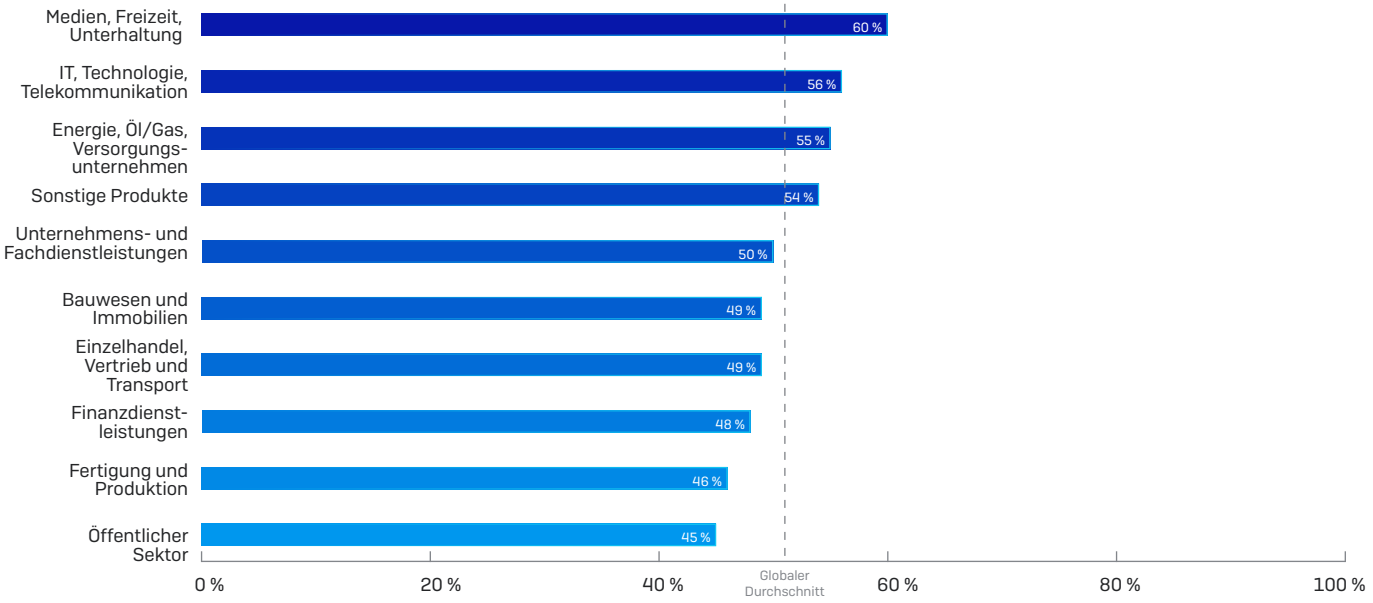
Ransomware hat Unternehmen weiterhin fest im Griff: Die Hälfte der von uns befragten Unternehmen in 26 Ländern gab an, im vergangenen Jahr Opfer von Ransomware geworden zu sein*. Diese Angriffe werden immer raffinierter und effizienter: Sie nutzen Schwachstellen in Netzwerken und Systemen aus – und die Unternehmen bleiben auf dem Schaden sitzen: In Deutschland betragen die Kosten im Durchschnitt ganze 420.000 EUR.

Moderne Firewalls wurden speziell dafür entwickelt, Systeme gegen solche Angriffe zu schützen, allerdings müssen hierfür zunächst die geeigneten Voraussetzungen geschaffen werden. In diesem Whitepaper erfahren Sie, wie Ransomware-Angriffe ablaufen, wie sie abgewehrt werden können und wie Sie sich durch die korrekte Konfiguration Ihres Netzwerks und Ihrer Firewall optimal vor Ransomware schützen.

Wen Hacker ins Visier nehmen

Auf wen haben es die Hacker abgesehen? Die Antwort ist kurz und knapp: jeden. In einer kürzlich durchgeführten Befragung gaben 51 % der Befragten an, im letzten Jahr von Ransomware getroffen worden zu sein, wobei die Unternehmensgröße keine entscheidende Rolle zu spielen scheint. 47 % der Unternehmen hatten weniger als 1.000 Mitarbeiter, 53 % mehr als 1.000. Kein Land, keine Region und kein vertikales Marktsegment scheint immun zu sein.

Prozentsatz der Unternehmen, die im letzten Jahr von Ransomware getroffen wurden



Wurde Ihr Unternehmen im letzten Jahr von Ransomware getroffen? Basis: 5.000 Befragte.

Wenn Sie in den Nachrichten nach dem Thema „Ransomware-Angriffe" suchen, werden Sie jede Woche gleich mehrere Meldungen über neue erfolgreiche Angriffe finden. Die Auswirkungen sind verheerend: horrende Lösegeldforderungen, erhebliche Ausfallzeiten und negative Auswirkungen auf den Geschäftsbetrieb, Reputationsverlust und Datenverlust. Immer öfter versteigern Hacker sogar sensible Unternehmensdaten.

* The State of Ransomware 2020 – unabhängige, von Sophos in Auftrag gegebene und von Vanson Bourne durchgeführte Befragung von 5.000 IT-Managern in 26 Ländern.

Wie Ransomware-Angriffe ins Netzwerk gelangen

Im Jahr 2020 gab es einen wachsenden Trend hin zu serverbasierten Angriffen. Dabei handelt es sich um zielgerichtete, hochkomplexe Angriffe, deren Bereitstellung mehr Aufwand erfordert. Allerdings sind sie in der Regel auch sehr viel verheerender, weil wertvollere Daten verschlüsselt werden, für deren Freigabe Millionenbeträge gefordert werden können. Glücklicherweise sind solche Angriffe mit geeigneten Sicherheits-Best-Practices vermeidbar.

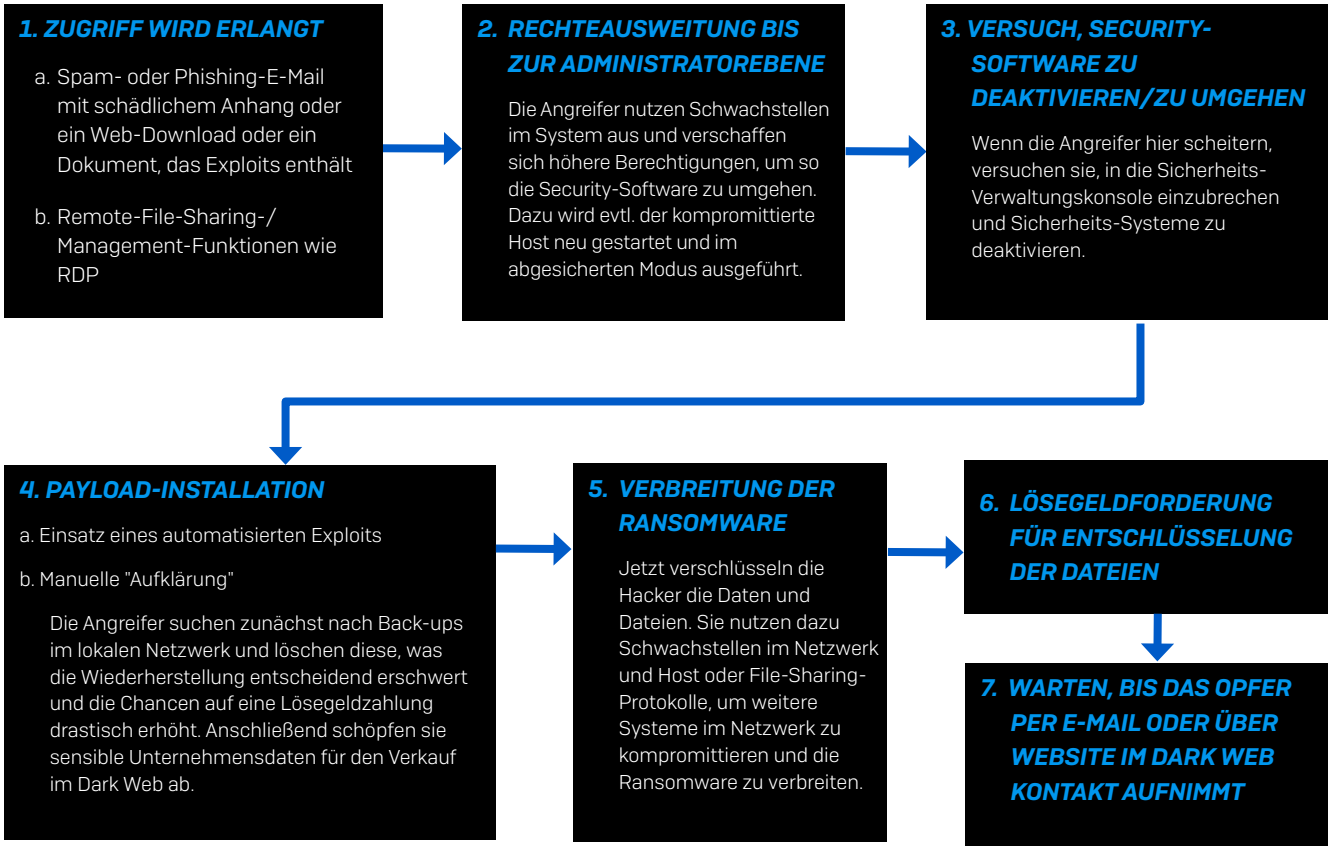
SO IST DIE RANSOMWARE INS UNTERNEHMEN GELANGT	% DER VORFÄLLE
Über einen Datei-Download/eine E-Mail mit schädlichem Link	29 %
Per Remote-Angriff auf den Server	21 %
Per E-Mail mit schädlichem Anhang	16 %
Falsch konfigurierte Public-Cloud-Instanzen	9 %
Über unser Remote Desktop Protocol (RDP)	9 %
Über einen Zulieferer, der mit unserem Unternehmen zusammenarbeitet	9 %
Über einen USB-Stick/Wechseldatenträger	7 %
Sonstige Produkte	0 %
Unsicher	0 %
Gesamt	100 %

Wie ist die Ransomware in Ihr Unternehmen gelangt? Frage an die Befragten, deren Unternehmen im letzten Jahr von Ransomware getroffen wurde.
Basis: 2.538 Befragte.

Wie Sie den Antworten in der Tabelle oben entnehmen können, ist der häufigste Eintrittspunkt für Ransomware ein Datei-Download oder eine mittels Spam- oder Phishing-Angriff versendete Datei. Sie dürfen das Thema Sicherheit also keinesfalls Ihren Benutzern überlassen, sondern benötigen leistungsstarken Firewall-Schutz.

Wie ein Ransomware-Angriff abläuft

Typischer Ablauf eines gezielten Ransomware-Angriffs:



Bereitstellung von Ransomware über RDP

Die meisten Betriebssysteme nutzen harmlose und sehr praktische Desktop-Sharing-Tools wie RDP (Remote Desktop Protocol) und VNC (Virtual Network Computing) für den Remote-Zugriff und die Remote-Verwaltung von Systemen. Ohne ausreichenden Schutz bieten diese Tools allerdings eine willkommene Schwachstelle, die häufig für gezielte Ransomware-Angriffe genutzt wird.

Sorgen Sie deshalb dafür, dass RDP und ähnliche Remote-Management-Protokolle hinter einem VPN (Virtual Private Network) ausreichend geschützt sind, oder legen Sie zumindest fest, welche IP-Adressen über Remote-Tools zugreifen können – sonst stehen Angreifern alle Türen offen. Denn viele Angreifer nutzen Brute-Force-Hacking-Tools, die Hunderttausende Kombinationen aus Benutzername und Passwort ausprobieren, bis sie sich erfolgreich Zugriff verschaffen.

Die besten Tipps zum Schutz vor Ransomware

Um Ihr Unternehmen erfolgreich vor Ransomware zu schützen, sollten Sie drei wichtige Maßnahmen ergreifen:

1. Upgraden Sie Ihre IT-Security

Ihre Firewall- und Endpoint-Security können dafür sorgen, dass Angriffe gar nicht erst in Ihr Netzwerk gelangen. Und sollte es einem Angreifer doch einmal gelingen, sich Zugriff zu Ihrem Netzwerk zu verschaffen, können Firewall- und Endpoint-Security die Ausbreitung der Bedrohung und deren Übergreifen auf weitere Systeme verhindern. Aber nicht alle Firewalls und Endpoint-Security-Lösungen erfüllen diese Aufgabe effektiv. Stellen Sie daher sicher, dass Sie über ein IT-Sicherheitssystem verfügen, das dieser Aufgabe auch wirklich gerecht wird.

Achten Sie auf folgende Funktionen:

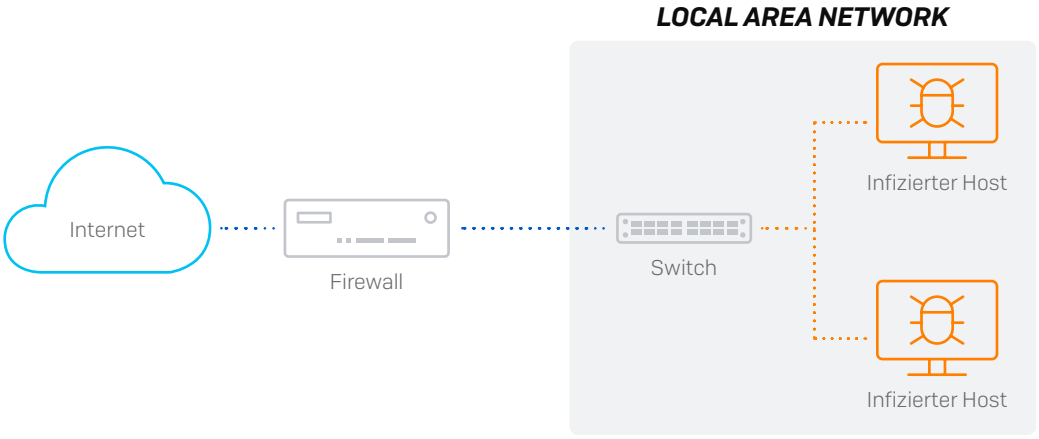
- Erschwingliche Sandboxing-Technologie zur Analyse des Dateiverhaltens während der Ausführung und vor Eintritt ins Netzwerk
- Neueste Machine-Learning-Technologie, die neue Zero-Day-Varianten in allen Dateien identifizieren kann, die die Firewall passieren
- Firewall IPS mit Live-Signatur-Aktualisierung zum Blockieren von Netzwerk-Exploits
- Kostenloses und einfaches Remote Access VPN zur Remote-Verwaltung Ihres Netzwerks ohne Sicherheitseinbußen
- Endpoint-Schutz mit Anti-Ransomware-Funktionen

2. Sperren Sie Remote-Zugriff und -Verwaltung

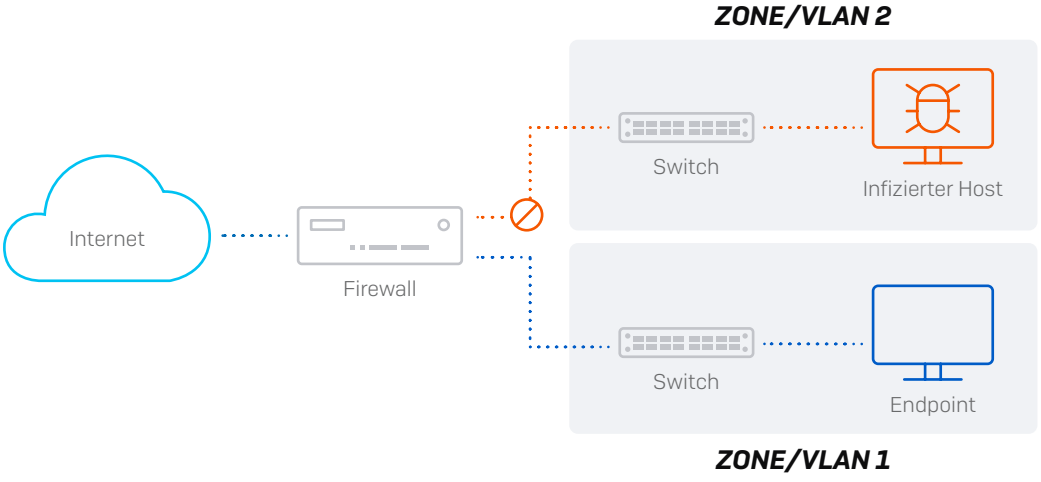
In Netzwerken ist jede Öffnung zur Außenwelt eine potenzielle Schwachstelle, die nur darauf wartet, von einem Ransomware-Angriff ausgenutzt zu werden. Den Zugriff auf das Remote Desktop Protocol, offene Ports und andere Verwaltungsprotokolle Ihres Unternehmens zu sperren, zählt daher zu den wirksamsten Mitteln gegen gezielte Ransomware-Angriffe. Es gibt zahlreiche Möglichkeiten, diese Sperrung zu realisieren. Eine gängige Methode ist, dass alle Benutzer sich bei einem VPN anmelden müssen, bevor sie auf Ressourcen wie RDP zugreifen dürfen, und den VPN-Zugriff auf bekannte IP-Adressen zu beschränken. Sichern und härten Sie Ihre Server außerdem ordnungsgemäß, verwenden Sie komplexe Passwörter, die häufig geändert werden, und nutzen Sie eine mehrstufige Authentifizierung.

3. Segmentieren Sie Ihr Netzwerk

Leider operieren viele Unternehmen mit einer flachen Netzwerk-Topologie – sie verbinden alle Endpoints mit einem zentralen Switch. Eine solche Topologie schwächt Ihren Schutz: Ihre Firewall hat keine Transparenz oder Kontrolle über den Datenverkehr, der den Switch durchläuft – dies ermöglicht laterale Bewegungen und die Ausbreitung von Angriffen innerhalb des lokalen Netzwerks.



Eine Best Practice ist es, das LAN unter Verwendung von Zonen und VLANs in kleinere Subnetze zu segmentieren und diese dann durch die Firewall miteinander zu verbinden. So wird eine Anwendung von Anti-Malware- und IPS-Schutz zwischen Segmenten ermöglicht. Auf diese Weise können Bedrohungen effektiv identifiziert und blockiert werden, die versuchen, sich lateral im Netzwerk zu bewegen.



Ob Sie Zonen oder VLANs verwenden, hängt von Ihrer Segmentierungs-Strategie für das Netzwerk und dem Umfang der Segmentierung ab. Beide Varianten bieten die Möglichkeit, auf Datenbewegungen zwischen Segmenten geeignete Sicherheits- und Kontrollmaßnahmen anzuwenden. Zonen sind die ideale Lösung für kleinere Segmentierungs-Strategien oder Netzwerke mit nicht verwalteten Switches. VLANs sind in den meisten Fällen die bevorzugte Methode zur Segmentierung interner Netzwerke und bieten maximale Flexibilität und Skalierbarkeit. Allerdings erfordern sie den Einsatz (und die Konfiguration) verwalteter Layer-3-Switches.

Ein Netzwerk zu segmentieren, ist eine klare Best Practice. Dafür, wie das Netzwerk segmentiert werden sollte, gibt es jedoch nicht „die eine" beste Methode. Sie können Ihr Netzwerk nach Benutzertyp (intern, extern, Gäste), nach Abteilung (Vertrieb, Marketing, Engineering), nach Service, Gerät oder Rollentyp (VoIP, Wi-Fi, IoT, Computer, Server) oder nach jeder beliebigen Kombination segmentieren, die für Ihre Netzwerk-Architektur sinnvoll ist. Im Allgemeinen sollten Sie weniger vertrauenswürdige sowie stark gefährdete Bereiche Ihres Netzwerks vom übrigen Netzwerk separieren und auch größere Netzwerke in kleinere Segmente unterteilen. So senken Sie die Gefahr, dass Bedrohungen in weite Teile Ihres Netzwerks vordringen und sich dort ausbreiten können.

Best Practices zur Firewall- und Netzwerk-Konfiguration

- **Sorgen Sie für den besten Schutz:** Implementieren Sie eine moderne, leistungsstarke Next-Gen Firewall mit IPS, TLS Inspection, Zero-Day Sandboxing und Machine-Learning-Ransomware-Schutz.
- **Sperren Sie RDP und andere Dienste** mit Ihrer Firewall. Ihre Firewall sollte in der Lage sein, den Zugriff auf VPN-Nutzer zu beschränken und erlaubte IP-Adressen auf die Whitelist zu setzen.
- **Reduzieren Sie die Angriffsfläche** so weit wie möglich, indem Sie alle Regeln zur Port-Weiterleitung erneut prüfen und alle nicht unbedingt notwendigen offenen Ports entfernen. Jeder offene Port stellt eine potenzielle Schwachstelle für Ihr Netzwerk dar. Nutzen Sie für den externen Zugriff auf das interne Netzwerk nach Möglichkeit VPN und keine Port-Weiterleitung.
- **Sichern Sie offene Ports ordnungsgemäß**, indem Sie auf Regeln zur Steuerung dieses Datenverkehrs einen geeigneten IPS-Schutz anwenden.
- **Aktivieren Sie TLS Inspection** mit Unterstützung der neuesten TLS-1.3-Standards für den Internet-Traffic. So verhindern Sie, dass Bedrohungen über verschlüsselte Datenströme in Ihr Netzwerk gelangen.
- **Minimieren Sie das Risiko lateraler Bewegungen** innerhalb des Netzwerks, indem Sie LANs in kleinere isolierte Zonen oder VLANs unterteilen, die von der Firewall geschützt und miteinander verbunden sind. Wenden Sie unbedingt geeignete IPS-Richtlinien auf Regeln an, über die der Datenverkehr gesteuert wird, der diese LAN-Segmente passiert. So verhindern Sie, dass Exploits, Würmer und Bots sich unter den LAN-Segmenten ausbreiten.
- **Isolieren Sie infizierte Systeme automatisch:** Kommt es zu einer Infektion, ist es unerlässlich, dass Ihre IT-Sicherheitslösung kompromittierte Systeme schnell erkennt und bis zu ihrer Bereinigung automatisch isoliert (z. B. mit Sophos Synchronized Security).
- **Verwenden Sie starke Passwörter und eine mehrstufige Authentifizierung** für Ihre Remote-Management- und File-Sharing-Tools, die sich nicht leicht durch Brute-Force-Hacking-Tools kompromittieren lassen.

Wie Sophos helfen kann

Sophos bietet die ultimative IT-Security-Lösung zur Abwehr neuester Ransomware. Sie erhalten nicht nur an jedem Punkt den besten Schutz, sondern profitieren auch von jahrelanger Integration zwischen Firewall und Endpoint. Dies bietet enorme Vorteile hinsichtlich der Transparenz über den Integritätsstatus des Netzwerks und ermöglicht eine automatische Reaktion auf Sicherheitsvorfälle.

Der Fokus unserer preisgekrönten XG Firewall liegt in erster Linie darauf, Angriffe auf das Netzwerk zu verhindern. Sollte es Ransomware dennoch gelingen, in Ihr Netzwerk zu gelangen, sind Sie doppelt geschützt. Dank Integration mit unserer branchenführenden Endpoint-Schutz-Plattform Sophos Intercept X kann die XG Firewall Ransomware automatisch stoppen. Sie stellen Ihr Netzwerk quasi auf Autopilot und multiplizieren damit die Arbeitsleistung Ihres Teams.

Wir nennen diese Technologie Sophos Synchronized Security. Synchronized Security vereint unsere Endpoint- und Netzwerk-Schutzfunktionen in einem leistungsstarken, vollständig integrierten Cybersecurity-System. Und das Beste: Die Verwaltung ist kinderleicht und erfolgt gemeinsam mit Ihren anderen Sophos-Produkten über unsere Cloud-Management-Konsole Sophos Central.

Leistungsstarke Technologien von Sophos und der XG Firewall, die speziell für die Abwehr von Ransomware entwickelt wurden

- Mit **Sandstorm-Sandboxing-Technologie** und **Machine-Learning-Analyse** von Dateien, die ins Netzwerk gelangen, verhindert die XG Firewall, dass bekannte und unbekannte Ransomware-Varianten, Exploits, und Malware sich über Spam, Phishing oder Web-Downloads verbreiten.
- Das **Intrusion Prevention System der XG Firewall** fängt die neuesten Netzwerk-Exploits und Angriffe ab, mit denen Hacker versuchen, Schwachstellen in Ihrer Abwehr zu finden.
- Mit den umfangreichen, aber einfachen **VPN-Optionen der XG Firewall** können Sie alle Sicherheitslücken in Ihrem Netzwerk schließen und sich unabhängig von anfälligen RDP-Verbindungen machen, ohne den Netzwerkzugriff für autorisierte Benutzer einzuschränken.
- Die XG Firewall bietet eine leistungsstarke **Xstream TLS 1.3 Inspection** mit flexiblen Richtlinienkontrollen, die sicherstellen, dass Sie die perfekte Balance zwischen Datenschutz, Schutz und Performance schaffen. Außerdem verhindern sie, dass Bedrohungen über verschlüsselte Datenströme unerkannt in Ihr Netzwerk gelangen.
- **Sophos Synchronized Security** vernetzt die XG Firewall mit unserer Intercept X Endpoint Protection. So kann Ransomware automatisch abgewehrt werden: Die ersten Anzeichen einer Kompromittierung werden sofort erkannt, die Angriffe werden gestoppt und Sie werden direkt benachrichtigt.
- **Sophos Intercept X Endpoint Protection mit CryptoGuard** kann laufende Ransomware-Angriffe erkennen, stoppen und automatisch rückgängig machen. Die XG Firewall verfügt über CryptoGuard-Technologie in der Sandbox-Umgebung, die Ransomware auf frischer Tat ertappt, bevor sie in Ihr Netzwerk gelangt.

Fazit

Obwohl Ransomware inzwischen in die Jahre gekommen ist, werden wir wohl auch in Zukunft nicht von neuen Varianten verschont bleiben. Vielleicht werden wir Ransomware nie vollständig eliminieren können. Wenn Ihr Unternehmen jedoch die in diesem Dokument beschriebenen Firewall Best Practices einhält, stehen Ihre Chancen gut, dass Sie vor neuester Ransomware und weiteren Bedrohungen geschützt bleiben.

Zusammenfassung:

- Sorgen Sie für den besten Schutz
- Sperren Sie RDP und andere Dienste mit Ihrer Firewall
- Reduzieren Sie die Angriffsfläche so weit wie möglich
- Sichern Sie alle offenen Ports mit einem geeigneten IPS-Schutz
- Wenden Sie Sandboxing- und Machine-Learning-Analysen auf Downloads und Anhänge an
- Minimieren Sie das Risiko von lateralen Bewegungen innerhalb des Netzwerks durch Segmentierung von LANs
- Isolieren Sie infizierte Systeme automatisch
- Verwenden Sie starke Passwörter und mehrstufige Authentifizierung für Ihre Remote-Management- und File-Sharing-Tools

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

200806 WPDE(TN)

SOPHOS