SONICWALL™

LÖSUNGSÜBERSICHT: SO SCHÜTZEN SIE SICH EFFEKTIV VOR RANSOMWARE

Acht Best Practices, um zu verhindern, dass Ihre Daten Erpressern in die Hände fallen

Bei Ransomware handelt es sich um Malware, die den Zugriff auf Daten oder Systeme blockiert, bis ein Lösegeld an den Angreifer gezahlt wird. Jede Organisation kann Opfer eines Ransomware-Angriffs werden. Glücklicherweise gibt es viele Möglichkeiten, um die Risiken für Ihre Organisation zu minimieren. Im Folgenden stellen wir Ihnen acht Best Practices vor, mit denen Sie Ihre Organisation effektiv vor Ransomware-Angriffen schützen können.

1. Schulungen und Sensibilisierung

Benutzerschulungen und die Sensibilisierung von Mitarbeitern sind extrem wichtig und stellen den ersten Schritt im Kampf gegen Ransomware dar. Benutzer sollten folgende Hinweise beachten:

- Alle verdächtigen E-Mails mit Vorsicht behandeln
- Den Domain-Namen anschauen, von dem die E-Mail stammt
- Auf Rechtschreibfehler prüfen, die Signatur und Zulässigkeit der Anfrage überprüfen
- Den Mauszeiger über den Link bewegen und prüfen, wohin er führt. Falls eine URL verdächtig aussieht, sollte man die Website direkt in die Suchleiste eintippen oder in Suchmaschinen recherchieren, anstatt auf den Link in der E-Mail zu klicken

2. E-Mail-Sicherheit

Sie sollten eine E-Mail-Sicherheitslösung implementieren, die nicht nur Spyware und Spam herausfiltert, sondern auch alle Anhänge prüft. Neben regelmäßigen Benutzerschulungen und Risikobewertungen sollten Sie Ihr Unternehmen auch auf Phishing-Schwachstellen testen.

3. Malware-Schutz

Endpunkte sind besonders gefährdet, wenn sie nicht von der IT verwaltet werden oder über keinen geeigneten Malware-Schutz verfügen. Dabei spielt es keine Rolle, ob es sich um private oder unternehmenseigene Geräte handelt. Die meisten Virenschutzlösungen sind signaturbasiert und erweisen sich als ineffektiv, wenn sie nicht regelmäßig aktualisiert werden. Neuere Ransomware-Varianten verfügen über individuelle Hashcodes und können daher nicht mittels signaturbasierter Methoden erkannt werden.

Viele Benutzer deaktivieren außerdem ihren Virenscanner, weil sie nicht möchten, dass ihr System dadurch verlangsamt wird. Zur

Lösung dieser Probleme gibt es Endpunktsicherheitslösungen, die erweiterte Funktionen für maschinelles Lernen und künstliche Intelligenz verwenden, um Malware aufzuspüren. Zudem sind sie extrem genügsam und verursachen daher nur minimale Leistungseinbußen.

4. Mobile Endpunkte

Die Verwaltung von Endpunkten wird auch immer schwieriger, weil sehr unterschiedliche Geräte und Betriebssysteme im Netzwerk genutzt werden. Laut dem Dell Annual Threat Report 2016 sind Mobilgeräte besonders verwundbar, wobei die Android™-Plattform immer wieder mit neuen Arten von Ransomware konfrontiert wird. Um gegen die wachsende Flut an Cyberbedrohungen – darunter auch Ransomware – gewappnet zu sein, ist es zunächst gut, eine Lösung zu wählen, mit der sich Patching und Versionsupgrades in heterogenen Geräte-, OS- und Anwendungsumgebungen automatisieren lassen.

Bei Remote-Benutzern, die sich außerhalb der Firewallgrenze befinden, sollte der VPN-basierte Zugriff nicht nur eine sichere Verbindung gewährleisten, sondern auch entsprechende Geräteabfragen durchführen, um die Regelkonformität des Endpunkts zu überprüfen. Verfügt ein Endgerät nicht über die erforderlichen Sicherheitsupdates, wird es nicht im Netzwerk zugelassen oder es erhält nur einen begrenzten Zugriff auf Ressourcen.

Insbesondere für Benutzer von Android-Mobilgeräten sind die folgenden Schritte zu empfehlen:

- Rooten Sie das Gerät nicht, da dies eine Modifizierung der Systemdateien ermöglicht.
- Installieren Sie immer Apps aus dem Google Play Store, da Apps aus unbekannten Websites und Stores sich als Fälschungen erweisen und möglicherweise schädlich sein können.
- Deaktivieren Sie die Installation von Apps aus unbekannten Quellen.
- Erlauben Sie Google, das Gerät auf Schadsoftware zu prüfen.
- Seien Sie vorsichtig beim Öffnen unbekannter Links, die Sie per SMS oder E-Mail erhalten.
- Installieren Sie Drittanbieter-Sicherheitsanwendungen, die das Gerät regelmäßig auf bösartige Inhalte prüfen.
- Achten Sie darauf, welche Apps als Geräteadministratoren registriert sind.
- Erstellen Sie für Geräte, die vom Unternehmen verwaltet werden, eine Blacklist mit nicht erlaubten Apps.

5. Netzwerksegmentierung

Die meisten Ransomware-Varianten versuchen, vom Endpunkt aus auf den Server/Speicher zu gelangen, auf dem sich alle Daten und geschäftskritischen Anwendungen befinden. Durch Segmentierung des Netzwerks und Isolierung kritischer Anwendungen und Geräte auf einem separaten Netzwerk oder virtuellen LAN kann die Ausbreitung eingedämmt werden.

6. Backup und Recovery

Um sich effizient vor Ransomware zu schützen, ist auch eine robuste Backup- und Recovery-Strategie notwendig. Wichtig ist, dass Sie Ihre Daten regelmäßig sichern. Bei einem Remote-Backup ist der Datenverlust im Falle eines Cyberangriffs geringer. Je nachdem wie schnell die Attacke entdeckt wird, wie großflächig sie sich ausgebreitet hat und welches Maß an Datenverlust akzeptabel ist, stellt die Wiederherstellung aus einem Backup womöglich eine gute Option dar. Dies erfordert allerdings eine intelligentere Backup-Strategie, bei der die Wichtigkeit Ihrer Daten und die Anforderungen Ihres Unternehmens im Hinblick auf Recovery Point Objectives (RPO) und Recovery Time Objectives (RTO) berücksichtigt werden. Die wichtigsten Daten sollten so schnell wie möglich wiederhergestellt werden. Eine Strategie zu haben, reicht alleine allerdings nicht aus. Genauso wichtig ist die regelmäßige Prüfung der Disaster-Recovery- und Business-Continuity-Pläne.

7. Verschlüsselte Angriffe

Es kommt besonders darauf an, eine Enterprise-Firewall zu wählen, die auf die eigenen Anforderungen zugeschnitten ist und den gesamten Datenverkehr unabhängig von der Dateigröße prüfen kann. Angesichts der schnellen Zunahme von SSL-verschlüsseltem Verkehr besteht – wie im SonicWall Threat Report erwähnt – immer das Risiko, verschlüsselte Malware herunterzuladen, die herkömmliche Firewalls nicht erkennen können. Daher sollte man unbedingt sicherstellen, dass die Firewall bzw. das IPS verschlüsselten Verkehr entschlüsseln und prüfen kann, ohne das Netzwerk wesentlich zu verlangsamen.

Darüber hinaus sollte man sich verborgene Dateiendungen immer anzeigen lassen. Sonst kann es passieren, dass Malware als .pdf- oder .mp3-File kaschiert ins System gelangt, obwohl es sich in Wahrheit um eine .exe-Datei handelt.

> Ein effektiver Ansatz zum Schutz vor Ransomware erfordert eine umfassende Koordination von Sicherheitsschulungen, Technologie und Verwaltung.

8. Überwachung und Verwaltung

Die Enterprise-Firewall sollte in der Lage sein, sowohl ein- als auch ausgehenden Verkehr zu überwachen. Weil Ransomware außerdem versucht, Kontakt mit ihren Command-and-Control-Servern aufzunehmen, sollte die Firewall auch die Kommunikation mit IP-Adressen blockieren, die auf der Blacklist stehen.

Wenn ein Befall mit Ransomware festgestellt wird, sollten Sie das infizierte System umgehend vom Unternehmensnetzwerk trennen. Die Firewall sollte über einen automatischen Update- und zentralisierten Verwaltungsprozess verfügen. Auf diese Weise lassen sich Updates und Regeln schnell und einheitlich über sämtliche Nodes hinweg durchführen, sobald eine neue Malware-Variante entdeckt wird. Außerdem sollten Sie Ihre Software und Ihre Betriebssysteme unbedingt in regelmäßigen Abständen aktualisieren.

Fazit

Mit den Lösungen von SonicWall können Sie alle Identitäten effizient verwalten und sämtliche Datenpakete genau durchleuchten, um die Sicherheit in Ihrer Organisation zu verbessern. Egal wo sich Ihre Daten befinden, wir schützen sie überall und nutzen weltweit vernetzte Informationen, um Sie gegen eine Vielzahl an Bedrohungen wie Ransomware zu wappnen.

Erfahren Sie mehr über unsere Next-Generation-Firewalls.

Über uns

Seit über 25 Jahren ist SonicWall als zuverlässiger Sicherheitspartner bekannt. Von Access Security über Netzwerksicherheit bis zu Email Security: Wir haben unser Produktportfolio kontinuierlich weiterentwickelt, damit unsere Kunden Innovationen realisieren, Prozesse beschleunigen und wachsen können. Mit über einer Million Sicherheitsgeräte in nahezu 200 Ländern und Regionen weltweit bietet SonicWall seinen Kunden alles, was sie brauchen, um für die Zukunft gerüstet zu sein.

Wenden Sie sich bei Fragen zu den Nutzungsmöglichkeiten dieses Materials an:

SonicWall Inc.
5455 Great America Parkway,
Santa Clara, Kalifornien (USA) 95054

Informationen zu regionalen und internationalen Niederlassungen finden Sie auf unserer Website.
www.sonicwall.com

SolutionBrief-HowToProtect-EU-IMAG-29233