SONICWALL®

8 METHODEN, WIE SIE IHR NETZWERK VOR RANSOMWARE SCHÜTZEN KÖNNEN

Effektive Maßnahmen, um Ransomware-Angriffe zu verhindern und Geld zu sparen

Manchmal kommen alte Dinge wieder in Mode, so etwa Ransomware, ein Schadprogramm, das 1989 erstmals in Erscheinung trat. Diese Malware infiziert ein System und hindert den Benutzer daran, auf das Gerät oder die darauf gespeicherten Dateien zuzugreifen. Erst nachdem das Opfer ein Lösegeld – gewöhnlich in Form von Bitcoins – zahlt, kann das System entsperrt und wieder genutzt werden.

Das vorliegende E-Book stellt acht Methoden vor, wie Sie Ihr Netzwerk vor Ransomware-Angriffen schützen und eine Lösegeldzahlung vermeiden können.

Die Höhe des Lösegelds ist variabel, beträgt aber oft zwischen 200 und 400 $.[1]

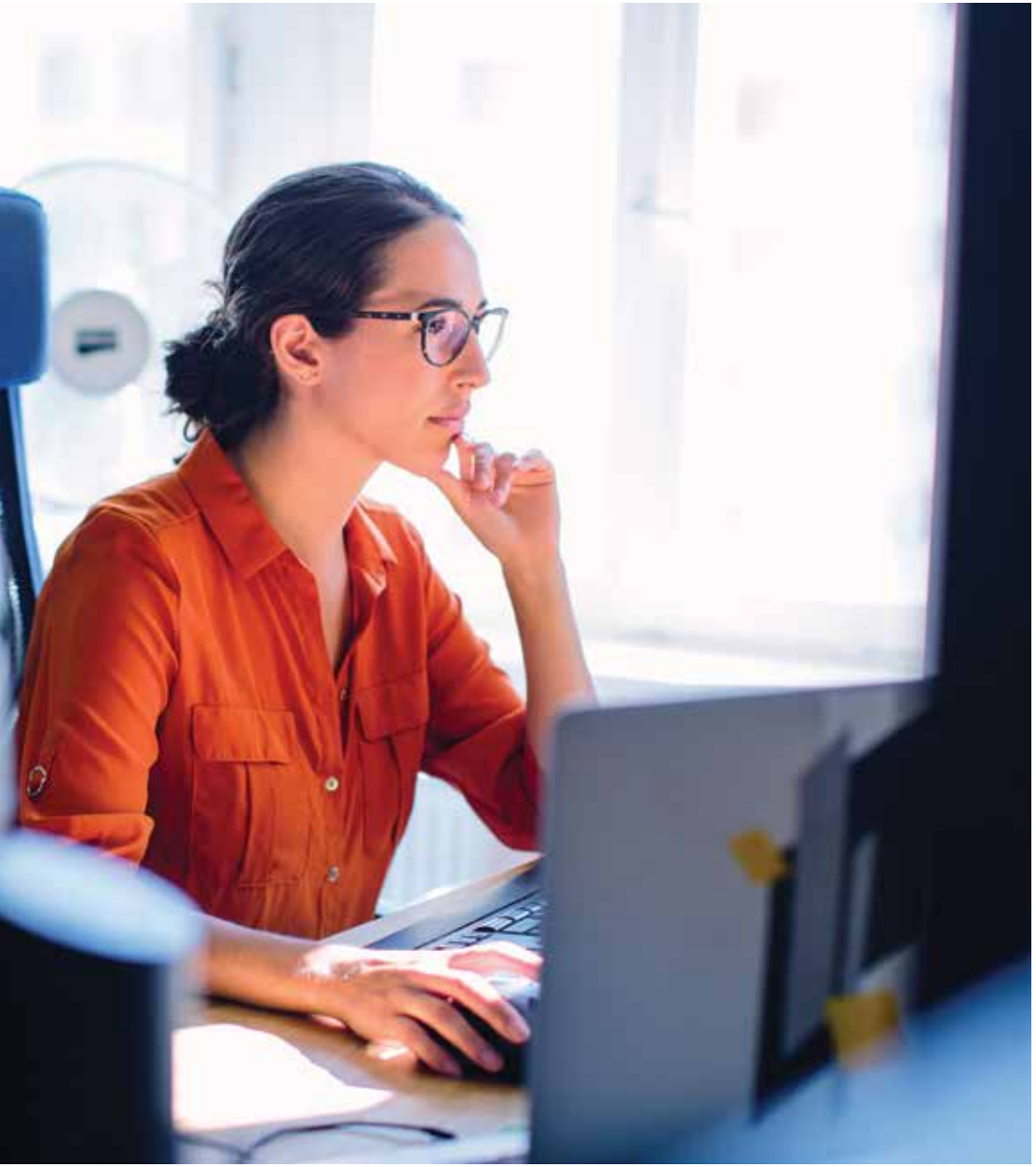
1. Schulen Sie Ihre Mitarbeiter

Im Kampf gegen Ransomware ist die Sensibilisierung und Schulung von Benutzern besonders wichtig. Verdächtige E-Mails sollten immer mit Vorsicht behandelt werden. Wichtig ist es auch, sich den Domain-Namen anzuschauen, von dem die E-Mail stammt, auf Rechtschreibfehler zu achten sowie die Signatur und Zulässigkeit der Anfrage zu überprüfen. Außerdem sollte man den Mauszeiger über den Link bewegen und prüfen, wohin er führt.

2. Setzen Sie auf eine mehrschichtige Netzwerksicherheitslösung

Der Schutz vor Ransomware und anderen Malware-Formen beginnt und endet nicht am Gateway. Besonders wichtig ist es, die Sicherheit durch Antiviren-, Anti-Spyware- und Intrusion-Prevention-Lösungen sowie andere gerätegebundene Technologien an der Netzwerkgrenze zu erweitern. Wählen Sie eine mehrschichtige Sicherheitsstrategie. Auf diese Weise vermeiden Sie einen Single Point of Failure in Ihrer Sicherheitsarchitektur und stoppen Ransomware-Angriffe zuverlässig.

1 US Computer Emergency Readiness Team Alert (TA16-091A)



3. Sichern Sie Ihre Dateien regelmäßig

Um sich effizient vor Ransomware zu schützen, ist auch eine durchdachte Backup- und Recovery-Strategie notwendig. 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 intelligente Backup-Strategie, die kritische Faktoren wie die Wichtigkeit Ihrer Daten und die Anforderungen Ihres Unternehmens im Hinblick auf Recovery Point Objectives (RPO) und Recovery Time Objectives (RTO) berücksichtigt.

4. Schützen Sie Ihre Endpunkte

Da die meisten User überwiegend private und unternehmenseigene Geräte nutzen, sind vor allem unverwaltete Endpunkte bzw. Endpunkte gefährdet, die über keinen geeigneten Malware-Schutz verfügen. 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.

Implementieren Sie eine mehrstufige Sicherheitsstrategie für einen größeren Netzwerkschutz.

5. Führen Sie Patches für Ihre Systeme und Anwendungen durch

Viele Angriffe machen sich bekannte Schwachstellen in häufig genutzten Apps und Plug-ins sowie in Browsern wie dem Internet Explorer zunutze. Entscheidend ist daher eine unverzügliche und zuverlässige Durchführung von Updates und Patches. Um gegen die wachsende Flut an Cyberbedrohungen – darunter auch Ransomware – gewappnet zu sein, ist eine Lösung empfehlenswert, mit der sich Patching und Versionsupgrades in heterogenen Geräte-, OS- und Anwendungsumgebungen automatisieren lassen.

6. Segmentieren Sie Ihr Netzwerk, um eine Ausbreitung zu verhindern

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 Apps und Geräte auf einem separaten Netzwerk oder virtuellen LAN kann die Ausbreitung eingedämmt werden.

7. Stellen Sie verdächtige Dateien unter Quarantäne und führen Sie eine Analyse durch

Technologien wie Sandboxing ermöglichen es, verdächtige Dateien unter Quarantäne zu stellen und zu analysieren, bevor sie ins Netzwerk gelangen können. Die Dateien werden am Gateway festgesetzt, bis der Sicherheitsstatus geklärt ist. Wird eine Datei als schädlich eingestuft, müssen Sie entsprechende Schutzmaßnahmen implementieren, wie etwa Regeln, die zugehörige IP-Adressen oder Domains blockieren, oder Signaturen auf Sicherheitsappliances im gesamten Netzwerk anwenden. Nur so können Sie Folgeangriffe vermeiden.

Segmentieren Sie Ihr drahtloses LAN, um interne Anwender von Gastbenutzern zu trennen und für eine zusätzliche Sicherheitsschicht zu sorgen.

8. Schützen Sie Ihre Android-Geräte

Geräte mit dem Betriebssystem Google Android sind ein beliebtes Ziel für Ransomware-Angriffe. Um Ihr Android-Smartphone zu schützen, sollten Sie folgende Maßnahmen befolgen:

- 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/Stores sich als Fälschungen erweisen und 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 unternehmenseigene Geräte eine Blacklist mit nicht erlaubten Apps.

Die Anzahl an Malware für das Android-Ökosystem stieg auch 2015. Somit sind knapp 85 Prozent aller Smartphones gefährdet.

Fazit

Ransomware-Angriffe erfreuen sich immer größerer Beliebtheit bei Cyberkriminellen. Daher sollten Sie unbedingt sicherstellen, dass Ihre Endpunkte geschützt sind. Mit 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 Malware-Informationen, um Sie gegen eine Vielzahl an Bedrohungen wie Ransomware zu wappnen.

Besuchen Sie die SonicWall-Webseite für Netzwerksicherheitsprodukte.

Über SonicWall

Seit über 25 Jahren schützt SonicWall kleine, mittlere und große Unternehmen weltweit vor Cyberkriminalität. Mit unseren Produkten und Partnerschaften können wir eine Echtzeit-Cyberabwehrlösung für die individuellen Anforderungen von über 500.000 globalen Organisationen in über 150 Ländern bereitstellen, damit sie sich voll und ganz auf ihr Geschäft konzentrieren können.

Wenn Sie Fragen zur Nutzung dieser Unterlagen haben, wenden Sie sich an:

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

Weitere Informationen finden Sie auf unserer Website.
www.sonicwall.com

Ebook-8waysRansomware-EU-IMAG-29271-D1

SONICWALL®