Ein umfassender Sicherheitsansatz für Ransomware-Resilienz

236,1 MILLIONEN

Ransomware-Angriffe gab es in der ersten Hälfte des Jahres 2022 weltweit

Bei Ransomware handelt es sich um bösartige Software (Malware), die in Computersysteme oder Netzwerke eindringt, wertvolle Daten verschlüsselt und vom Opfer ein Lösegeld für den Decryption Key verlangt, der erforderlich ist, um wieder Zugriff auf die kompromittierten Daten zu erhalten. Sie werden in der Regel von Cyber-Kriminellen ausgeführt, die einen finanziellen Gewinn anstreben. Sie können sich gegen Einzelpersonen, Unternehmen oder sogar kritische industrielle oder staatliche Infrastrukturen richten. Diese Angriffe können zu Datenverlusten, Betriebsunterbrechungen und erheblichen finanziellen Schäden führen, was sie zu einer der größten Bedrohungen in der Welt der Cyber-Sicherheit macht.

Wie funktioniert Ransomware?

Sobald ein Computersystem oder Netzwerk infiltriert ist, verschlüsselt Ransomware Dateien mit komplexen Algorithmen und sperrt sie für Anwender. Nach dem Verschlüsselungsvorgang wird eine Lösegeldforderung angezeigt, die das Opfer über den Angriff informiert und eine Zahlung – häufig in Kryptowährung – im Austausch für den Decryption Key verlangt, der erforderlich ist, um wieder Zugriff auf die kompromittierten Daten zu erhalten. Das Opfer erhält in der Regel Anweisungen, wie die Zahlung zu leisten ist. Nach Erhalt der Zahlung müssen die Cyber-Kriminellen den Decryption Key bereitstellen, damit das Opfer seine Dateien entsperren kann.

3,5 WOCHEN

Durchschnittliche Zeit bis zur Wiederherstellung nach einem Ransomware-Angriff

Ransomware verschafft sich meist über eine der folgenden Methoden Zugang:

- **Menschliches Versagen.** Am häufigsten verbreitet sich Ransomware über Phishing-E-Mails, die den Empfänger dazu verleiten, einen infizierten Anhang zu öffnen oder auf einen bösartigen Link zu klicken. Sobald die Ransomware ausgeführt wird, kann sie sich auf andere Geräte im Netzwerk ausbreiten.
- **Ungepatchte Schwachstellen.** Angreifer nutzen häufig bekannte Schwachstellen in Software aus, um sich Zugang zum Computer eines Opfers zu verschaffen. Dies ist ein einfacher Einstiegspunkt, wenn die Software nicht mit den neuesten Sicherheitspatches aktualisiert wurde.
- **Malvertising.** Hierbei handelt es sich um eine Art von Online-Werbung, die zur Verbreitung von Malware genutzt wird. Angreifer können Opfer mit Ransomware infizieren, sobald sie auf eine bösartige Werbeanzeige klicken.
- **Drive-by-Downloads.** Bei diesen Angriffen wird Malware ohne das Wissen oder die Zustimmung des Opfers auf dessen Computer heruntergeladen, wenn das Opfer eine kompromittierte Website besucht oder auf einen bösartigen Link klickt.
- **Ungesicherte Wechseldatenträger.** Ransomware kann sich auch über ungesicherte Wechseldatenträger wie USB-Laufwerke verbreiten. Sobald ein Opfer ein infiziertes Wechselmedium in seinen Computer einsteckt, kann die Ransomware auf den Computer kopiert und auf andere Netzwerkgeräte übertragen werden.

Ransomware-Angreifer sind ständig auf der Suche nach neuen Wegen zur Verbreitung ihrer Malware. Wenn Sie diese gängigen Methoden zur Verbreitung von Ransomware verstehen, können Sie Maßnahmen zum Schutz davor ergreifen.

58
AKTIVE
Ransomware-Gruppen

101
BEKANNTE
Arten von Ransomware

Warum verbreitet sich Ransomware?

Ransomware verbreitet sich aus mehreren Gründen. Erstens ist die Rentabilität von entscheidender Bedeutung. Lösegeldzahlungen, die oft in Kryptowährungen gefordert werden, die ein gewisses Maß an Anonymität bieten, haben sich als lukrativ erwiesen. Dieser finanzielle Anreiz ermutigt etablierte kriminelle Organisationen und einzelne Hacker, in die Entwicklung und Verbreitung von noch mehr Ransomware zu investieren.

Zweitens schafft die zunehmende Vernetzung unserer digitalen Welt mehr Möglichkeiten für die Verbreitung von Ransomware. Die wachsende Popularität von Cloud Computing erleichtert es Angreifern, Opfer ins Visier zu nehmen, da sie auf Dateien zugreifen können, die auf Cloud-Servern gespeichert sind.

Darüber hinaus können Angreifer dank der relativ einfachen Bereitstellung von Ransomware und der Verfügbarkeit von Ransomware-as-a-Service-Plattformen (RaaS) im Dark Web auch mit begrenzten technischen Kenntnissen Angriffe starten. RaaS-Anbieter stellen benutzerfreundliche Schnittstellen, Kundensupport und detaillierte Anweisungen bereit, mit denen Anwender die Ransomware für bestimmte Ziele anpassen können. Nach dem Einsatz kassieren die Anwender Lösegeld von den Opfern und teilen den Gewinn mit dem RaaS-Anbieter, d. h. es kommt zu einer Gewinnbeteiligung.

Letztendlich ist die Bekämpfung der Verbreitung von Ransomware aufgrund ihrer globalen und dezentralen Natur eine Herausforderung. Kriminelle aus verschiedenen Ländern verwenden anonyme Kommunikationsmethoden, was es für die Strafverfolgungsbehörden schwierig macht, sie zu verfolgen und festzunehmen.

Wie sollten Sie auf einen Ransomware-Angriff reagieren?

Wenn Sie glauben, dass Sie von einem potenziellen Ransomware-Angriff betroffen sind, geraten Sie nicht in Panik. Gehen Sie stattdessen wie folgt vor:

- Raten Sie dem Unternehmen von der Zahlung des Lösegelds ab. Die Zahlung garantiert nicht, dass der Angreifer die Daten zurückgibt, und bietet nur zusätzliche Anreize für weitere Ransomware-Angriffe.
- Wenden Sie sich an die Behörden, um den Angriff zu melden, damit sie die Angreifer ermitteln und aufspüren können.
- Versuchen Sie, die Daten aus einem Backup wiederherzustellen. Ein aktuelles Backup ist die beste Versicherung für Geschäftskontinuität.
- Ziehen Sie Spezialisten hinzu. Wenn Sie die Daten nicht aus einer Sicherungskopie wiederherstellen können, sollten Sie einen Datenwiederherstellungsspezialisten hinzuziehen.

der Unternehmen fühlen sich nicht ausreichend auf den Umgang mit Ransomware vorbereitet

Wie können Sie sich vor Ransomware schützen?

Das FBI betont eine vielschichtige Strategie mit den Schwerpunkten Prävention, Geschäftskontinuität und Wiederherstellung. Die sich ständig weiterentwickelnde und ausgefeilte Natur von Ransomware erfordert einen umfassenden Ansatz. Die Notfall- und Wiederherstellungsplanung gewährleistet eine schnelle Wiederaufnahme des Geschäftsbetriebs und unterbrechungsfreie Abläufe. Dazu gehören die Implementierung proaktiver Maßnahmen wie das Whitelisting von Anwendungen und virtualisierte Umgebungen, die Kategorisierung von Daten nach ihrem Wert und die Durchsetzung der Netzwerktrennung, die alle zu einer robusten Verteidigung gegen Ransomware beitragen.

Im breiteren Kontext müssen Einzelpersonen und Organisationen wachsam und proaktiv bleiben, um sich vor Angriffen zu schützen. Es ist wichtig, sich der Risiken bewusst zu sein und proaktive Schritte zu unternehmen. Sowohl Einzelpersonen als auch Unternehmen können ihre Widerstandsfähigkeit gegen diese allgegenwärtige Cyber-Bedrohung erheblich verbessern, indem sie bewährte Verfahren anwenden und robuste Cyber-Sicherheitsmaßnahmen implementieren, wie zum Beispiel:

- Sichern Sie regelmäßig wichtige Daten und Dateien, damit Sie sie wiederherstellen können, falls sie verschlüsselt werden.
- Überprüfen Sie E-Mail-Anhänge und -Links; lassen Sie nur vertrauenswürdige E-Mails zu.
- Halten Sie Betriebssysteme und Software mit den neuesten Sicherheitspatches und -updates auf dem neuesten Stand.
- Verwenden Sie Antivirensoftware und aktualisieren Sie diese regelmäßig.
- Deaktivieren Sie unnötige Dienste und Anwendungen, die für die Arbeit eines Kunden nicht erforderlich sind.
- Verwenden Sie Firewalls, um unbefugten Zugriff auf ein Netzwerk zu verhindern.
- Beschränken Sie die Benutzerrechte, damit nur autorisierte Anwender Software installieren oder Änderungen daran vornehmen können.
- Informieren Sie sich und Ihre Kunden über Ransomware und wie man sie vermeiden kann.
- Implementieren Sie strenge Sicherheitsrichtlinien und -verfahren, um eine sichere Arbeitsumgebung zu gewährleisten.
- Erstellen Sie einen Plan, um auf einen Ransomware-Angriff zu reagieren, einschließlich der Frage, wer zu kontaktieren ist und welche Schritte zu ergreifen sind.

Selbst mit diesen vorbeugenden Maßnahmen könnte Ransomware immer noch in ein Netzwerk eindringen. Vollständig integrierte Sicherheitsebenen sind der ultimative Schutz. Die Architektur der Unified Security Platform von WatchGuard ist entscheidend bei der Bekämpfung von Ransomware-Angriffen.

UMFASSENDE SICHERHEIT

Ein umfassendes Portfolio aus Produkten und Services für **Endpoint-Sicherheit, Multifaktor-Authentifizierung** und**Netzwerksicherheit** zum Schutz von Umgebungen, Anwendern und Geräten.

TRANSPARENZ UND KONTROLLE

Zentralisierte Sicherheitsverwaltung, Transparenz und erweitertes Reporting über **WatchGuard Cloud™**.

BETRIEBLICHE AUSRICHTUNG

Vereinfachte Geschäftsabläufe mit direktem **API-Zugang,** einer umfangreichen Auswahl an **einsatzbereiten Integrationen** und Tools für eine schnelle, effiziente Bereitstellung.

KOLLEKTIVE INTELLIGENZ

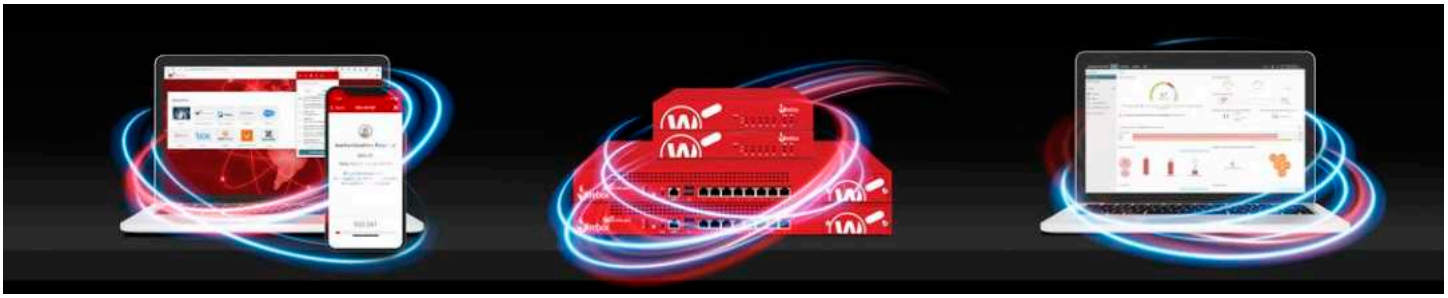
Eine umfassend integrierte Plattform zur Einführung eines Zero-Trust-Sicherheitskonzepts über das **Identity Framework** von WatchGuard und zur Bereitstellung eines echten XDR-basierten Ansatzes für Bedrohungserkennung und -beseitigung über **ThreatSync™**.

AUTOMATION

Automation Core™ von WatchGuard ermöglicht die Vereinfachung und Skalierung sämtlicher Aspekte der Nutzung, Bereitstellung und Verwaltung von Sicherheitsdiensten.

Besserer Schutz vor Ransomware – Der Weg von WatchGuard

Die Sicherheitslösungen von WatchGuard bieten einen wirksamen Schutz vor Ransomware-Angriffen. Die Firebox-Firewall und ergänzende Sicherheitsdienste schützen Ihr Netzwerk vor externen Bedrohungen, während Endpoint Security Ihre Endgeräte gegen interne Bedrohungen verteidigt. Total Identity Security von WatchGuard schützt Anwender vor dem Diebstahl von Anmeldeinformationen und verhindert den unbefugten Zugriff auf Ihre Systeme, eine gängige Methode zur Einschleusung von Ransomware. Dieser einheitliche, mehrschichtige Sicherheitsansatz stellt sicher, dass Ihr gesamtes Netzwerk vor Ransomware-Angriffen geschützt ist, wodurch das Risiko von Datenverlust und Ausfallzeiten minimiert wird.



WatchGuard Network Security

Um Ihren Netzwerkperimeter vor Ransomware zu schützen, benötigen Sie eine umfassende Sicherheitslösung, die zuverlässigen Schutz auf mehreren Ebenen bietet. WatchGuard bietet eine breite Palette von Funktionen, die Ihnen helfen, Ihr Netzwerk zu schützen, darunter:

- Erweiterte Bedrohungsabwehr: Nutzt Angriffserkennung und -prävention in Echtzeit, um Ransomware-Angriffe aktiv zu identifizieren und zu blockieren, bevor sie in Ihr Netzwerk eindringen können.
- Mehrschichtige Sicherheit: Kombiniert signaturbasierte Erkennung, Verhaltensanalyse und heuristisches Scannen, um bekannte und neue Ransomware-Varianten zu identifizieren.
- Sicheres VPN und Zugriffskontrolle: Bietet integrierte VPN- und Zugriffskontrollfunktionen, um Remote-Verbindungen zu schützen und das Risiko des Eindringens von Ransomware über Remote- oder Mobilgeräte in Ihr Netzwerk zu verringern.
- Frühzeitige Erkennung: Bietet Warnungen und Berichte in Echtzeit, um das Bewusstsein der Anwender zu schärfen und sofort auf verdächtige Aktivitäten zu reagieren.
- Schnelle Reaktion: Isoliert betroffene Geräte und hilft bei der Wiederherstellung von Daten während Ransomware-Angriffen, wodurch Ausfallzeiten und finanzielle Verluste minimiert werden.
- Skalierbarkeit: Die Sicherheitslösungen von WatchGuard können skaliert werden, um Unternehmen jeder Größe zu schützen, von kleinen Unternehmen bis hin zu Großkonzernen.
- Kontinuierliche Updates: WatchGuard aktualisiert seine Sicherheitslösungen regelmäßig, damit Sie neuen Ransomware-Bedrohungen immer einen Schritt voraus sind.

Bleiben Sie mit WatchGuard Netzwerksicherheit immer einen Schritt voraus.

WatchGuard Endpoint Security

Die Anzahl der Ransomware-Erkennungen auf Endpoints ist im vergangenen Jahr um 627 % gestiegen. WatchGuard-Endpunkt-Sicherheitslösungen können Ransomware-Angriffe frühzeitig erkennen, indem sie auf verdächtiges Verhalten überwachen, z. B. auf eine große Anzahl von Dateien, die gleichzeitig verschlüsselt werden, oder auf Versuche, mit bekannten Ransomware-Befehls- und Kontrollservern zu kommunizieren. Um sicher zu sein, benötigen Ihre Endpoints die neuesten Entwicklungen im Bereich Endpoint-Schutz, darunter:

- Bedrohungserkennung in Echtzeit: Unser Threat Hunting Service überwacht Systeme und Netzwerke in Echtzeit auf Bedrohungen zur proaktiven Erkennung und Abwehr von Ransomware-Angriffen, bevor diese Fuß fassen können.
- Verhaltensanalyse: Der Zero Trust Application Service verwendet Verhaltensanalysen, um Ransomware-Aktivitäten zu erkennen, selbst von neuen Varianten. Durch das Monitoring des Verhaltens von Prozessen und Dateien können verdächtige Aktionen identifiziert und unter Quarantäne gestellt werden, um potenzielle Angriffe zu stoppen.
- Anti-Ransomware-Signaturen: WatchGuard aktualisiert seine Signaturen kontinuierlich, um sicherzustellen, dass bekannte Ransomware-Stämme sofort identifiziert und blockiert werden.
- Filterung der Web-Reputation: Dies verhindert, dass Anwender versehentlich bösartige Websites besuchen, die bekanntermaßen Ransomware verbreiten, und reduziert so Ihre Angriffsfläche.
- Zentrale Verwaltung: WatchGuard Cloud ermöglicht Administratoren die einfache Überwachung und Konfiguration von Sicherheitsrichtlinien für alle Endpoints, um sicherzustellen, dass alle Geräte in Ihrem Netzwerk einheitlich und zuverlässig geschützt sind.
- Quarantäne und Abhilfe: Bei einem Ransomware-Vorfall kann unsere Endpoint-Sicherheit infizierte Geräte isolieren und bei der Wiederherstellung verschlüsselter Daten helfen, wodurch Ausfallzeiten und Verluste minimiert werden.
- Unterstützung mehrerer Plattformen: Unsere Endpoint-Sicherheit unterstützt verschiedene Plattformen, einschließlich Windows, macOS und Linux, und eignet sich somit für unterschiedliche IT-Umgebungen.

Erhalten Sie umfassende Endpoint Protection mit WatchGuard.

WatchGuard Multifaktor-Authentifizierung (MFA)

AuthPoint ist eine Multifaktor-Authentifizierungslösung (MFA), die die Sicherheit erhöht, indem sie von Anwendern verlangt, dass sie ihre Identität durch mehrere Faktoren wie Passwörter, Einmal-Passwörter (OTPs), Push-Benachrichtigungen und biometrische Daten authentifizieren. Dadurch wird das Risiko von unbefugtem Zugriff und Ransomware-Infiltrationen deutlich reduziert. AuthPoint wird vollständig aus der Cloud bereitgestellt und lässt sich daher einfach einrichten und verwalten. Es bietet eine Vielzahl von Vorteilen, darunter:

- Erhöhte Zugriffssicherheit: AuthPoint bietet eine starke Zugriffskontrolle, indem es mehrere Authentifizierungsfaktoren erfordert und die DNA mobiler Geräte verwendet, um nicht autorisierte Geräte zu identifizieren und zu blockieren.
- Schutz vor dem Diebstahl von Anmeldedaten: Ransomware-Angriffe beginnen oft mit gestohlenen oder kompromittierten Anmeldeinformationen. AuthPoint mindert dieses Risiko, indem es von Anwendern verlangt, dass sie sich mit zwei oder mehr Faktoren authentifizieren, selbst wenn ihre Anmeldedaten gestohlen wurden.
- Einhaltung von Branchenvorschriften: Viele regulatorische Standards und Compliance-Rahmen schreiben jetzt MFA vor, um sensible Daten zu schützen. Die Implementierung von AuthPoint erhöht nicht nur die Sicherheit, sondern gewährleistet auch die Einhaltung der Branchenvorschriften.
- Vielseitigkeit: AuthPoint unterstützt eine Vielzahl von Authentifizierungsmethoden, so dass Unternehmen den am besten geeigneten Ansatz für ihre Anwender und Sicherheitsanforderungen auswählen können.
- Skalierbarkeit: Authpoint lässt sich leicht skalieren, um die Anforderungen von Unternehmen jeder Größe zu erfüllen.

Schützen Sie Ihre Anmeldeinformationen mit WatchGuard AuthPoint

Sie benötigen eine umfassende Cyber-Sicherheitslösung, um Ihre Netzwerke vor Ransomware zu schützen. Die Unified Security Platform-Architektur von WatchGuard **vereint Netzwerk-, Endpoint- und Identitätssicherheit**, um Ihr Unternehmen von allen Seiten nahtlos zu schützen und eine robuste Abwehr gegen die unerbittliche Ransomware-Bedrohung aufzubauen.

Sehen Sie sich den Ransomware-Tracker des WatchGuard Threat Lab an.

Über WatchGuard

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Cyber-Sicherheit. WatchGuards Unified Security Platform®-Ansatz ist speziell auf Managed Service Provider ausgelegt, damit sie erstklassige Sicherheit bieten können, die die Skalierbarkeit und Schnelligkeit ihres Unternehmens erhöht und gleichzeitig die betriebliche Effizienz verbessert. Über 17.000 Vertriebspartner und Dienstleister im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Services des Unternehmens, die die Bereiche Network Security and Intelligence fortschrittlicher Endpoint-Schutz, Multifaktor-Authentifizierung sowie sicheres WLAN umfassen, und sorgen somit für den Schutz von mehr als 250.000 Kunden. Gemeinsam bieten diese Bereiche die fünf entscheidenden Elemente einer Sicherheitsplattform: umfassende Sicherheit, kollektive Intelligenz, Transparenz und Kontrolle, operative Ausrichtung und Automatisierung. 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.de**.

Deutschland, Österreich, Schweiz +49 700 92229333 INTERNATIONALER VERTRIEB: +1 206 613 0895 WEB: www.watchguard.de