Forcepoint

Die Lösung im Überblick

Forcepoint Zero Trust Content Disarm and Reconstruction für Mail

Einfach bedrohungsfreie E-Mails

Herausforderungen

- Bekämpfen von Phishing-Angriffen – laut CISCO waren 2021 90 % der Sicherheitsverletzungen auf Phishing zurückzuführen.
- Zero-Day-Exploits

Lösung

- Verstärken Sie Ihre E-Mail-Sicherheit mit Zero Trust Content Disarm and Reconstruction (CDR): die einzige Möglichkeit, bekannte, unbekannte und Zero-Day-Bedrohungen in Inhalten abzuwehren, die über E-Mails eingeschleust werden.

Vorteile

- Übermittelt sichere, bedrohungsfreie E-Mail-Nachrichten und Anhänge über die Netzwerkgrenze, ohne dass die Bedrohung identifiziert oder die von Benutzern benötigten Inhalte isoliert werden müssen. Zero-Day-Exploits, Ransomware, Steganografie-Exploits, dateilose Malware und Bedrohungen, die sich in polymorphen Dateien verbergen, werden entfernt.
- Funktioniert mit Ihren bestehenden E-Mail-Sicherheitsgateways, Spam-Filtern und Ihrer Virenschutztechnologie am Netzwerkrand, kann nahtlos in die Cyber-Sicherheitsmechanismen am Netzwerkrand eingefügt werden und bietet ein geringes Risiko und einen kostengünstigen Ansatz für den umfassenden Schutz vor Bedrohungen, die sich in Inhalten verbergen.

Benutzer in Unternehmen können normalerweise über eine E-Mail-Funktion E-Mail-Nachrichten von ihrem Arbeitsplatz aus mit Benutzern in ihrem Unternehmen und auch im Internet austauschen. E-Mails enthalten häufig auch Anhänge und können dadurch viel Inhalt umfassen. Zudem werden E-Mails meist im HTML- oder Rich Text-Format erstellt und enthalten neben Anhängen auch Formatierungen, Hyperlinks, Farben und Bilder. Dadurch besteht die Gefahr, dass im umfangreichen Inhalt dieser E-Mails Malware versteckt wird und so ihren Weg ins Unternehmen findet.

Herkömmliche E-Mail-Sicherheitsgateways beruhen auf der Erkennung potenzieller Bedrohungen. Es hat sich jedoch herausgestellt, dass sie den heutigen, extrem ausgeklügelten Angriffen nicht gewachsen sind.

Abwehr unbekannter Bedrohungen

Bestehende E-Mail-Schutzmechanismen und Gateways am Netzwerkrand (die Virenschutz, Bedrohungsdaten, Sandboxing und Spam-Filterung kombinieren) sind die erste Verteidigungslinie und sollen bekannte Bedrohungen erkennen, indem nach Signaturen von bisher aufgetretenen Exploits und nach unsicheren Verhaltensweisen gesucht wird. Unternehmen sind jedoch immer wieder Zero-Day-Bedrohungen ausgesetzt, die in das Unternehmen eindringen, bevor erkennungsbasierte Abwehrmechanismen greifen. Auch völlig unbekannte Bedrohungen können in Unternehmen eindringen, ohne jemals richtig identifiziert zu werden.

Zero Trust CDR für E-Mail ist die einzige Lösung, die nicht nur vor bekannten Bedrohungen, sondern auch vor Zero-Day- und unbekannte Bedrohungen in Inhalten schützt, die über E-Mail-Schnittstellen eindringen, da diese Technologie nicht auf Erkennung oder der Ausführung in einer Sandbox-Umgebung beruht. Daten werden stattdessen in einem einzigartigen Verfahren so umgewandelt, dass ein umfassender Schutz gewährleistet ist.

Revolutionierung Ihrer E-Mail-Sicherheit

Zero Trust CDR für E-Mail extrahiert am Netzwerkrand geschäftliche Informationen aus den E-Mail-Nachrichten und Anhängen. Die Daten, die Informationen enthalten, werden zusammen mit potenziellen Bedrohungen verworfen. Anschließend werden neue Nachrichten und Anhänge erstellt und dem Benutzer bereitgestellt. Somit werden nur sichere Inhalte an den Benutzer weitergeleitet. Angreifer bleiben draußen und Unternehmen bekommen die Informationen, die sie brauchen.

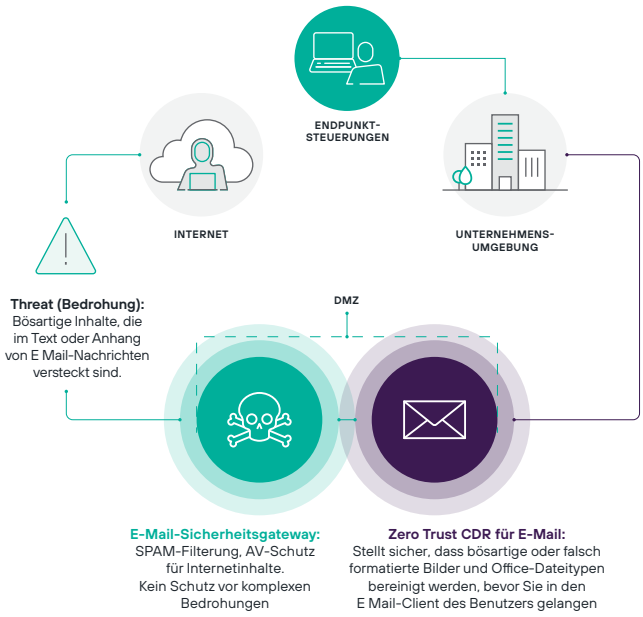
Dieser Prozess wird Transformation genannt. Dieses Verfahren ist unschlagbar: Das Sicherheitsteam ist zufrieden, weil die Bedrohung entfernt wird, und die Benutzer im Unternehmen sind zufrieden, weil sie die benötigten Informationen bekommen.

Zero Trust CDR ist die einzige Möglichkeit, Bedrohungen in Inhalten zuverlässig zu entfernen. Die einzigartige Forcepoint-Technologie Zero Trust CDR verzichtet auf die unzuverlässigen Verfahren der Bedrohungserkennung und -isolierung. Die Technologie geht davon aus, dass alle Daten nicht sicher und nicht vertrauenswürdig sind und versucht gar nicht erst, gut von böse zu unterscheiden.

Erweiterung Ihrer bestehenden Abwehr

Zero Trust CDR für E-Mail erweitert den bestehenden E-Mail-Sicherheitsgateway und E-Mail-Server, um Bedrohungen in E-Mail-Text und in Dateitypen, die häufig an E-Mails angehängt werden (Bilder, Microsoft Office-Dokumente und PDFs) zu entfernen. Zero Trust CDR für E-Mail kann lokal und in der Cloud bereitgestellt werden.

Zero Trust CDR für E-Mail ergänzt bestehende E-Mail-Sicherheitskontrollen. Dazu wird bei der Verarbeitung des ein- und ausgehenden E-Mail-Verkehrs eine zusätzliche Komponente eingefügt.



Nahtlose Integration

Zero Trust CDR für E-Mail wird auf einem Server am Unternehmensstandort eines bestehenden E-Mail-Sicherheitsgateways ausgeführt. Eingehende E-Mails werden vom E-Mail-Sicherheitsgateway an Zero Trust CDR für E-Mail weitergeleitet, wo die Nachrichten umgewandelt werden, um sicherzustellen, dass keine Bedrohungen mehr vorhanden sind, bevor sie an den E-Mail-Server des Unternehmens übermittelt werden.

Verhindern von Infiltration von Malware in Inhalten

Office-Dokumente, Dokumente im Adobe Portable Document-Format (PDFs) und Bilder sind die häufigsten Träger von Malware. Durch die Komplexität dieser Dateiformate und die Anwendungen, mit denen sie bearbeitet werden, sind sie ein beliebtes Ziel für Angreifer. Unabhängig von der Malware – ob Ransomware, Banktrojaner oder Remote-Zugriffskits und Keylogger – Cyber-Kriminelle wissen, wo sie die neuesten Zero-Day-Bedrohungen in einem ganz gewöhnlichen Geschäftsdokument am besten verstecken können. Durch Techniken wie die Verwendung von dateiloser Malware und Polymorphismus von Dateien ist es noch schwieriger, mit herkömmlicher erkennungsbasierter Cyber-Sicherheit Bedrohungen zu beseitigen. Zudem sind E-Mails der perfekte Vektor zum Einschleusen von Malware.

Zero Trust CDR für E-Mail stellt sicher, dass Unternehmensbenutzer E-Mail sorgenfrei verwenden können. Der Schlüssel liegt im einzigartigen Verfahren zur Transformation von Nachrichten. Jedes Dokument und Bild wird umgewandelt und ist dadurch bedrohungsfrei.

Anwendungsschicht-Proxy

Zero Trust CDR für E-Mail fungiert als Dual-Homed-Anwendungsschicht-Proxy für SMTP. Es bildet eine sichere Grenze zwischen dem Unternehmensnetzwerk und den externen Systemen und fungiert als Smart Host für den E-Mail-Sicherheitsgateway für eingehende Nachrichten und den E-Mail-Server für ausgehende Nachrichten. Zero Trust CDR wandelt sämtlichen Content, inklusive MIME und E-Mail-Attachments, so um, dass er sicher innerhalb des Unternehmensnetzwerks transportiert werden kann. Zero Trust CDR kümmert sich auch um Anfragen an das User-Portal beziehungsweise dessen Rückmeldungen, um Zugriffe auf vorgehaltene, passwortgeschützte Dokumente zu ermöglichen, und wandelt empfangene, passwortgeschützte Anhänge um.

Zero Trust CDR für E-Mail wandelt die empfangenen Inhalte in ein internes Informationsformat um. Die Originaldaten werden verworfen. Aus den Informationen werden dann neue „sichere" Daten erstellt. Bedrohungen in den Inhalten können somit ausgeschaltet werden, selbst wenn es sich um unbekannte Bedrohungen handelt. Die Informationen können dagegen an ihr Ziel übermittelt werden. Dieser Vorgang wird für alle Inhalte durchgeführt, die umgewandelt werden.

Kennwortgeschützt Anhänge

In manchen Unternehmen werden kennwortgeschützte Dokumente erstellt, die als Anhänge über das Internet gesendet werden. Diese Dokumente sind eine potenzielle Gefahr, weil sie nicht umgewandelt und von möglichen Bedrohungen befreit werden können.

Um geschäftliche Notwendigkeit und Sicherheitsrisiko in Einklang zu bringen, kann Zero Trust CDR für E-Mail so konfiguriert werden, dass Nachrichten mit kennwortgeschützten Anhängen nicht übermittelt bzw. kennwortgeschützte Anhänge aus Nachrichten entfernt werden. Alternativ können Kanäle zwischen bestimmten Benutzern oder Benutzergruppen so konfiguriert werden, dass der Transformationsprozess umgangen wird, wenn das Senden kennwortgeschützter Anhänge unumgänglich ist.

Signierte oder verschlüsselte Nachrichten

Wenn die Unterstützung von Nachrichten notwendig ist, die mit S/MIME oder PGP signiert und/oder verschlüsselt wurden, kann dies auf Gateway-Ebene eingestellt werden. Die Nachrichten werden dann mithilfe von Zero Trust CDR zunächst bedrohungsfrei gemacht und anschließend an einen separaten Forcepoint-Wächterserver weitergeleitet, der die Nachrichten signiert oder verschlüsselt.

Makros und ausführbare Inhalte

In einigen Unternehmen tauschen Benutzer makrofähige Office-Dokumente per E-Mail aus. Diese Dokumente sind eine potenzielle Gefahr, denn Makros sind ausführbarer Inhalt, der durch Transformation nicht von Bedrohungen befreit werden kann.

Um geschäftliche Notwendigkeit und Sicherheitsrisiko in Einklang zu bringen, kann Zero Trust CDR für E-Mail so konfiguriert werden, dass Nachrichten mit Office-Makros nicht übermittelt bzw. Anhänge mit Office-Makros aus Nachrichten entfernt werden. Alternativ können Kanäle zwischen bestimmten Benutzern oder Benutzergruppen so konfiguriert werden, dass der Transformationsprozess umgangen wird, wenn das Senden makrofähiger Office-Dokumente unumgänglich ist.

Weitere Informationen finden Sie unter Forcepoint Zero Trust CDR

forcepoint.com/contact

[Zero Trust CDR for Mail Solution Brief-DE] 10Mar2022