AI POWERED

HORNETSECURITY

FACT SHEET

SPAM & MALWARE PROTECTION

Wirksamer Schutz vor Spam und Malware durch ein vollautomatisches, mehrstufiges Filtersystem.

Spam macht mehr als 50 % des gesamten E-Mail-Verkehrs aus und ist die aufdringlichste Methode, mit der Cyber-Kriminelle Malware und Viren in Unternehmenssysteme einschleusen. Neben der Gefahr einer Infektion mit Ransomware, Spyware oder einem Kryptominer können auch wichtige Arbeitsabläufe durch die lästige Flut unerwünschter Spam-E-Mails unterbrochen werden. Ein mehrstufiges Filtersystem ist ein Muss, wenn Sie verhindern wollen, dass Spam- und Phishing-E-Mails Ihre Posteingänge erreichen und den Arbeitsablauf stören.

Ihre Postfächer verdienen die stärksten Filter

- **Dynamische Erkennung von Virenausbrüchen**
- **Mehrstufige Spam-Erkennung und dynamische Filterstufen**
- **Ausgehende Filterung**

Was ist betroffen?

E-Mail-Umgebung

Wie kann Ihnen Spam & Malware Protection helfen?

Höchste Spam- (99,9 %) und Virenerkennungsraten (99,99 %) auf dem Markt.

Maximierung der Sicherheit für spezifische Tenant-Anforderungen durch erweiterte Regelerstellung innerhalb des Compliance-Filters.

Ausgehende E-Mails werden auf Spam und Viren geprüft.

Was verbessert sich?

Sichere ein- und ausgehende E-Mail-Kommunikation

HORNETSECURITY

FACT SHEET

PRÄZISE ANALYSEMECHANISMEN UND ZUVERLÄSSIGE FILTER:

Phishing-Filter: Link-Tracking und weitere Mechanismen schützen wirksam vor Phishing-E-Mails. Dazu werden u. a. nachladbare schädliche Script-Befehle erkannt. Dies ermöglicht z.B. die Erkennung von gefährlichen Drive-By-Downloads.

Infomail-Filter: Nicht als Spam klassifizierte Newsletter und andere Infomails, die den Arbeitsablauf unnötig unterbrechen, werden aussortiert und zum späteren Abruf vorgehalten. Sie werden im individuellen Quarantäne Report aufgelistet und lassen sich von dort bei Bedarf per Mausklick zustellen und whitelisten.

Link-Tracking: Eingehende und ausgehende E-Mails werden automatisch nach schädlichen URLs gescannt.

Automatische Virus-Signatur-Aktualisierung: Die Malwarefilter werden ständig aktualisiert und sind stets auf dem neuesten Stand. Eingesetzt werden u. a diverse eigene Scanner, der auf per E-Mail verbreitete Malware spezialisiert sind.

Outbound Filtering: Ausgehende E-Mails werden auf Spam und Viren geprüft, um zu vermeiden, dass der Kunde ungewollt Malware und Spam-Mails verschickt bzw. weiterleitet.

Bounce-Management: Im eingehenden Mailverkehr erreichen nur echte Bounces den Empfänger, Bounces als Antwort auf Spam mit gefälschten Absenderadressen werden zuverlässig ausgefiltert.

Content Filter für Dateianhänge: Unerwünschte Anhänge können zurückgewiesen oder in die Quarantäne verschoben werden.

Dynamic Virus Outbreak Detection: Neue und bisher nicht bekannte Viren werden durch das Frühwarnsystem gestoppt. Hornetsecurity analysiert dazu permanent eingehende Mails auf sogenannten Honeypot-Accounts (E-Mail-Adressen, die nur den Zweck haben Spam zu empfangen) auf ungewöhnliche Anhänge, Links, Absender oder Inhalte. Die Ableitung von Signaturen daraus erfolgt innerhalb kürzester Reaktionszeit (i.d.R. < 5 Minuten).

Weniger als 0,00015 False Positives: Die Zahl der versehentlich als Spam klassifizierten, jedoch regulären E-Mails liegt bei weniger als 0,00015.

EINFACHE VERWALTUNG UND EINHALTUNG VON **COMPLIANCE RICHTLINIEN**

Quarantäne Report in konfigurierbaren Intervallen: Benutzer können die Zustellung ihrer Quarantäne Reports an ihre Arbeitsweise anpassen und auf bestimmte Uhrzeiten legen, auch mehrmals am Tag.

One-Click-Release: E-Mails in der Quarantäne lassen sich aus dem Quarantäne Report per Mausklick zustellen, egal, ob vermeintliche Spam-Nachrichten oder Infomails.

Gute Übersicht dank Blocking: Die überwiegende Mehrzahl aller Spam-E-Mails wird direkt geblockt. Der Benutzer erhält dadurch schnell einen Überblick über aktuelle E-Mails in der Quarantäne.

Entlastung des Mailservers: Spam and Malware Protection lässt nur gültige Nachrichten durch, was die Performance des Kunden-Mail-Servers deutlich erhöht.