

X-SPAM

Spamschutz und Inhaltssicherheit am Mail-Gateway



X-SPAM für SMTP-Server ist eine selbstlernende Spamschutzsoftware, um SMTP-Server vor Spam zu schützen. X-SPAM verwendet komplexe reguläre Ausdrücke und Meta-Tests, um den Spam positiv zu erkennen und zu blockieren. X-SPAM für SMTP-Server ist eine wartungsfreie Spamschutzsoftware, die einmal installiert, praktisch von sich aus funktioniert und sich selbst auf dem neuesten Stand hält. Über eine benutzerfreundliche Benutzeroberfläche können Filter-, Bewertungs- und andere spambekämpfenden Optionen weiter angepasst werden. X-SPAM verwendet heuristische Bewertung, um die Wahrscheinlichkeit zu reduzieren, legitime E-Mails als Spam zu klassifizieren. Diese Werte werden mittels eines speziellen Algorithmus aus dem Bereich der Künstlichen Intelligenz erzeugt

Wie funktioniert X-SPAM?

X-SPAM für SMTP-Server bekämpft Spam auf zwei Ebenen:

- Bevor eine E-Mail auf der Mail-Protokoll-Ebene angenommen wird, wird überprüft, ob der Mailserver, der versucht, die Verbindung herzustellen, in der Schwarzen Liste der Spamsender eingetragen ist. Falls das der Fall ist, wird die E-Mail von diesem Mailserver nicht angenommen.
- Nachdem die Mail angenommen wurde, passiert sie eine Reihe Spezialfilter, die ihr Spamwerte zuweisen. Danach wird für jede Mail ein Spamwert ausgerechnet. Falls sie den Spammengrenzwert übersteigt, wird sie als Spam markiert.

Hauptmerkmale von X-SPAM

Webbasierte Verwaltungskontrolle

Auf die X-SPAM-Verwaltungskontrolle kann durch den Browser zugegriffen werden. Dadurch wird die Fernverwaltung dieser Anwendung aktiviert.

Umsetzung integrierter Mailsicherheitsrichtlinien

Dieses Modul befähigt die Systemverwalter, gemäß den universellen bzw. firmenspezifischen Richtlinien Regelsätze zu erstellen, um integrierte Mailsicherheitsrichtlinie im ganzen Unternehmen umzusetzen.

Authentifizierung

X-SPAM verwendet das Modul "Webbasierte Verwaltung" zur LDAP- und POP3-Authentifizierung. Diese Authentifizierung wird gebraucht, um die Identität der berechtigten Benutzer zu verifizieren und den unautorisierten Zugang zu den Mails einzuschränken. Der Sender kann auf der SMTP-Ebene authentifiziert werden.

POP3-Downloader

Dieses Modul lädt eingehende Mails mithilfe eines eingebauten SMTP-Servers und POP3-Downloaders herunter.

SMTP-Transparenter-Proxy

Für Microsoft Exchange Server 2007 hat MicroWorld den SMTP-Transparenten-Proxy eingeführt, um eine durch die Transport Layer Security (TLS=Transportschichtssicherheit) gestützte Kommunikation zwischen dem Hub-Transport-Server und dem Edge-Transport-Server zu ermöglichen. Die TLS kann sowohl den Client als auch den Server authentifizieren, um eine verschlüsselte Verbindung zwischen diesen beiden herzustellen.

E-Mail-Anhänge filtern

Dieses Modul blockiert das Versenden oder Empfangen bestimmter Anhänge mit den Dateierweiterungen wie EXE, COM, CHM oder BAT.

Hochentwickelter Spam- und Phishing-Schutz

Dieses Modul verwendet eine Kombination von Technologien wie die Realtime-Blackhole-Liste (RBL)/DUL, Überprüfung der in Echtzeit abfragbaren Schwarzen Liste der URLs der Spamsender (SURBL), MX/A DNS Rekordüberprüfung, Reverse-DNS-Abfrage, X-SPAM-Regelüberprüfung, Sender Policy Framework, Graue Liste und Unaufdringliches Lernen (NILP*), um Spam- und Phishing-Mails auszufiltern.

Unaufdringliches Lernen (NILP*)

Die NILP-Technologie ist ein hochentwickelter Spamfilter, der jede E-Mail analysieren und sie gemäß den Verhaltensmustern der Benutzer als Spam bzw. Ham klassifizieren kann.

Graue Liste (Greylisting)

Bei der Methode „Graue Liste“ werden die E-Mails von unbekanntem Absendern temporär abgewiesen, da die meisten Spamsender nicht versuchen, eine Mail wiederzuschicken, die bereits einmal abgewiesen wurde. Wenn es eine legitime Mail gibt, wird der Quellrechner in meisten Fällen versuchen, sie wiederzuschicken. Dann wird sie angenommen.

Bilderspam blockieren

X-SPAM verwendet leistungsstarke Technologien, um Bilderspam herauszufiltern.

Weißer Liste der E-Mail-Adressen

Wenn ein lokaler Benutzer eine E-Mail schickt, wird die Adresse des Empfängers automatisch durch das System der Weißen Liste der E-Mail-Adressen hinzugefügt.

Aufnahme der IP-Adressen in die Weiße Liste

IP-Adressen der Webseiten, die der Überprüfung durch den Spamblocker, die Realtime-Blackhole-Liste (RBL) und die Reverse-DNS-Abfrage nicht unterzogen werden sollen, werden in die Weiße Liste der IP-Adressen aufgenommen.



Echtzeitanhaltskontrolle

Alle ein- und ausgehenden Nachrichten werden gemäß den Sicherheitsrichtlinien des Unternehmens in Echtzeit auf anstößige Wörter und Inhalt für Erwachsene (Adult-Content) geprüft.

Clusterbildung

Clusterbildung ermöglicht Lastenteilung durchs Verteilen der Mails auf mehrere Computers zum Scannen.

Relaykontrolle

Die Relaykontrolle hindert Spammern daran, die IP-Adresse und den Mailserver Ihrer Firma zum Versenden von Spam zu verwenden.

Umfangreiche Archivierung der E-Mails und Anhänge

Dieses Modul archiviert ein- und ausgehende E-Mails und E-Mail-Anhänge. Diese Eigenschaft hilft auch bei der umfassenden Inhaltskontrolle.

Komprimierung und Dekomprimierung

X-SPAM bietet Optionen an, Dateien automatisch zu komprimieren bzw. dekomprimieren, um die Bandbreite zu sparen.

Benutzerdefinierte Fußtexte

X-SPAM enthält benutzerfreundliche Optionen, benutzerdefinierte Fußtexte einfach allen ausgehenden und internen E-Mails anzuhängen.

Ausführliche Reports

Dieses Modul bietet ausgereifte analytische Reports in grafischen und nicht-grafischen Formaten an.

TCP-Verbindungen

Dieses Modul zeigt alle TCP/UDP-Verbindungen wie Prozesse, Protokolle, lokale Adresse, Fernadresse und Status auf dem Bildschirm an.

24x7 Kostenfreier Technischer Dienst

X-SPAM wird rund um die Uhr durch kostenfreien technischen Dienst per Telefon und Online (per E-Mail, Live Chat und Forums) unterstützt.

Minimale Systemvoraussetzungen:



Prozessor: Pentium II 200 MHz oder höher
RAM: 128 MB (256 MB empfohlen)
Festplatte: 500 MB freier Plattenplatz
Betriebssystem: Windows 2008 / Vista / XP / 2003 (32-/64-Bit) / 2000 / NT / ME / 98
Internet Explorer 5.0
CD-ROM-Laufwerk

*NILP = Non-Intrusive Learning Patterns