IT-Security
Firewall & VPN
Managed Services
Secure Server
Spam- & Virenschutz

Electronic Service Center

SpamFix

Technische Informationen

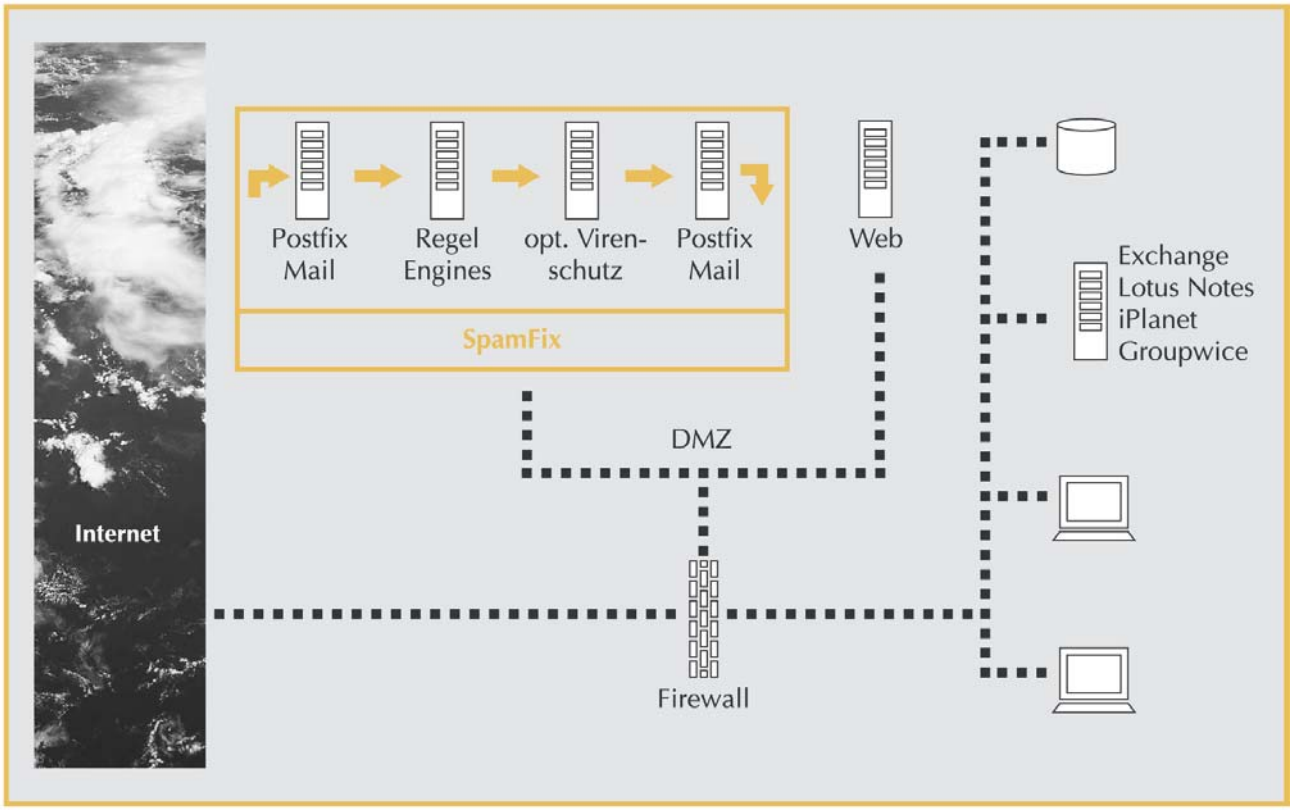
ESC – Electronic Service Center
Schulstr. 13, 06108 Halle (Saale)
Tel: 0345 - 55844 0
Fax: 0345 - 55844 99
Mail: info@esc.de
Web: www.esc.de

Die professionelle Lösung zur Abwehr von Spam

SpamFix ist eine umfassende, flexible und sehr weitgehend konfigurierbare Lösung für die Erkennung und Behandlung von unerwünschten Spam-Mails. SpamFix kann an die jeweils besonderen Bedürfnisse von Unternehmen und Institutionen oder sogar bestimmten Bereichen angepasst werden.

SpamFix wird als Mail-Relay logisch zwischen dem Internet und dem Mailserver platziert und ist somit als transparente Ergänzung kompatibel zu allen bekannten Mailservern. Die Erkennung von Spam basiert auf mehreren Verfahren, die durch individuelle Gewichtungen kombiniert werden. Hierfür stehen Regelwerke aus öffentlichen Datenbanken ebenso zur Verfügung wie die jeweils aktuellen Erkenntnisse aus dem Verbund der SpamFix-Lösungen. Ergänzt werden diese Maßnahmen durch Regeln, die aus dem firmen- oder mitarbeiter-individuellen Mailaufkommen manuell oder auch automatisiert generiert werden können.

SpamFix ist eine Komplettlösung, die vollständig und individuell konfiguriert auf der gewünschten Hardware einsatzbereit ausgeliefert wird. SpamFix läuft sowohl auf Sun Sparc-Rechnern unter Solaris als auch auf Appliance- und Server-Systemen (Intel, AMD) unter einem speziellen Linux, das nach den Richtlinien der ESC für Security-Lösungen (Firewalls, VPNs, Viruswalls etc.) abgehärtet wurde und nur mit dem minimal notwendigen Funktionsumfang ausgestattet ist.



Spam-Erkennung durch Bayes-Klassifizierung

SpamFix kombiniert etliche Klassifizierungs- und Erkennungsmethoden unter denen der sogenannten Bayes-Klassifizierung eine zentrale Funktion zukommt. Dieses statistisch-heuristische Verfahren ermittelt anhand einer vorab trainierten Liste von Wörtern und deren Häufigkeiten die Wahrscheinlichkeit, ob der Inhalt einer Mail erwünscht oder unerwünscht ist.

Für die Bayes-Klassifizierung werden Daten aus öffentlichen Datenbanken (Erkenntnisse der Open-Source-Community) sowie Daten aus Spamfix-Datenbanken verwendet, in denen die Analyseergebnisse zur Positiv-Klassifizierung aller Mail-Relays stets aktuell abgelegt werden.

Daneben verfügt jedes SpamFix über eine individuelle Bayes-Datenbank, die durch die manuelle Angabe von „erwünschten" Mails erstellt werden kann. Dieses Training erfolgt am besten mit nicht erkannten Spam-Mails (False Negatives) und mit falsch erkannten erwünschten Mails (False Positives). Der Bayes-Klassifizierer lernt aber auch automatisch: Überschreitet eine Mail den Spam-Schwellwert sehr deutlich, wird diese Mail automatisch als neuer „Spam" zur Verbesserung der Erkennung trainiert. Wird der Schwellwert sehr deutlich unterschritten, wird die Mail als „erwünschte Mail" ebenfalls automatisch trainiert.

SpamFix-Service

Das System wird lauffähig installiert und konfiguriert an den Kunden ausgeliefert und in die jeweilige Umgebung intergriert. SpamFix wird vor Ort beim Kunden betrieben und remote über geschützte Verbindungen von der ESC administriert, kontrolliert und gewartet. Hierfür bieten wir unterschiedliche Serviceleistungen und Reaktionszeiten an. Die laufende Pflege und Weiterentwicklung der Regelwerke wie auch der Basiskomponenten ist ein notwendiger Service, um die dauerhafte Sicherheit und stetig hohe Erkennungsraten zu gewährleisten. Folgende Dienstleistungen sind grundsätzlich im SpamFix-Service enthalten:

- **SpamFix Softwarepflege:** Die Lösung besteht aus bis zu vier Hauptkomponenten und ca. 30 notwendigen Untermodulen, die ständig weiterentwickelt werden. Die Komponenten müssen daher kontinuierlich aktualisiert werden.
- **Security-Patches des Betriebssystems:** Für die dauerhafte Sicherheit ist die Pflege und Aktualisierung des jeweiligen Betriebssystems und der dort notwendigen Komponenten unerlässlich.
- **Administration und Konfiguration:** Grundsätzliche Administrationsleistungen und Konfigurationsänderungen auf Kundenwunsch sind ebenfalls im Service inbegriffen.
- **Betreuung der Lernphase:** Wie beschrieben kann SpamFix anhand von empfangenen Mails automatisch lernen. Diese Lernphase ist aber deutlich effizienter, wenn SpamFix in der Einführungsphase einmalig manuell mit Spam-Mails und „erwünschter Mail" durch die ESC trainiert wird. In dieser Phase können auch individuell gewünschte Hinweise und Mitteilungen an die Nutzer eingerichtet werden.
- **Regeloptimierungen und Anpassung der Schwellwerte:** Im Rahmen des SpamFix-Services wird kontinuierlich daran gearbeitet, die Regelwerke und deren Gewichtung weiter zu optimieren, um die Erkennungsrate zu steigern. Diese Verbesserungen werden dann umgehend implementiert.
- **Spam-Beobachtung und -korrelation:** Die Methoden der Versender von Spam-Mails werden fortlaufend raffinierter. Darauf muss zeitnah reagiert werden. Wir entwickeln ständig neue Regeln und Filter-Methoden und testen diese. Sobald sich neue Regeln als robust und zuverlässig herausstellt, werden sie auf allen von uns betreuten SpamFix-Lösungen bereitgestellt.

Maximale Vertraulichkeit und Datenschutz

Viele effiziente Anti-Spam-Lösungen erfordern den Umweg über den Server eines Serviceanbieters. Dies verletzt aber die Vertraulichkeit der Mails, da sie jenseits jeder Kontrolle von Dritten gespeichert, bearbeitet und weitergeleitet werden.
SpamFix ist hingegen vor Ort im Netz des Kunden installiert und überträgt lediglich die Analysedaten der als Spam erkannten Mails auf gesicherte Server der ESC, um diese in die zentralen Bayes-Datenbanken einpflegen zu können. Alle Mails selbst hingegen verlassen die lokalen Server der Kunden nicht. Und sogar die lokalen Analysedaten für die Erkennung von „erwünschter Mail“ verbleiben ausschließlich beim Kunden, um selbst die eher theoretische Möglichkeit auszuschließen, dass aus diesen Daten Rückschlüsse auf die Inhalte der Mail gewonnen werden könnten.
Für zusätzliche oder spezielle Nachoptimierungen besteht die freiwillige Möglichkeit, der ESC manuell unerkannt gebliebene Spam-Mails zuzustellen, die wir entsprechend in die SpamFix-Lösungen integrieren können. So kommen die Erkenntnisse aus den Mails all unserer Kunden jedem Kunden zu Gute, ohne die Vertraulichkeit des Mailverkehrs auch nur im Ansatz zu gefährden.

Integration

SpamFix wird typischerweise direkt in einer DMZ platziert. Um eine schnelle und unproblematische Integration zu erleichtern sowie ein jederzeit mögliches Auskoppeln zu ermöglichen, wird nur das Standard-Routing für den Port 25 zum SpamFix-Mail-Relay auf dem Router oder Gateway geändert. Eine Änderung von MX-Einträgen o.ä., die das Tätigwerden externer Stellen erfordern würde, ist so nicht notwendig. Vom SpamFix-Mail-Relay wird die Mail nach der Klassifizierung an den oder die bisherigen Mailserver weiter geleitet.

Optional: Virenschutz

Die ESC betreibt seit Jahren erfolgreich den Schutz von Mailservern gegenüber Viren, Würmern, Trojanern und anderen Schädlingen. Insbesondere das Produkt TrendMicro Interscan VirusWall kam hierfür oft sehr erfolgreich bei unseren Kunden zum Einsatz. Für dieses Produkt wie auch andere Security-Lösungen kann die ESC umfangreiche und verlässliche Service-Leistungen im Rahmen von „Managed Services“ anbieten.
Daher kann die TrendMicro Interscan VirusWall optional direkt in die SpamFix-Lösung integriert werden und von der ESC im Rahmen des SpamFix-Services gewartet, gepflegt und kontrolliert werden.
SpamFix ermöglicht aber auch die Integration von fast allen anderen marktüblichen Virenscannern. Für besonders sicherheitsrelevante Anwendungen kann SpamFix bei Bedarf auch mehrere Virenscanner zur Prüfung der Mails einbinden.

Plattformen

- Sparc Server von Sun Microsystems unter Solaris
- Linux Server von Sun Microsystem unter Linux (abgehärtet)
- Appliance-Plattformen der ESC (Intel, AMD) unter Linux (abgehärtet)
- Server der ESC (Intel, AMD) unter Linux (abgehärtet)
- Bei besonders hohen Anforderungen können zur Erhöhung der Ausfallsicherheit und zur Lastverteilung Loadbalancer (z.B. Alteon) oder Round-Robin-DNS eingesetzt werden.

  Im Rahmen von Managed Services für das Betriebssystem erfolgt auch die dauerhafte Überwachung der Hardware und der Prozesse sowie die umgehende Reaktion auf Störungen und deren Behebung.

Produkteigenschaften

- **Qualitätssicherung:** Mails werden nicht gelöscht, sondern nur als Spam markiert und die Nutzer können sie mit Mailclienten automatisch filtern oder sortieren und daher bei Bedarf auch regelmäßig überprüfen.
- **Filter:** Als Spam klassifizierte Mails können direkt abgewiesen werden. Dem Absender kann eine Mail geschickt werden. Diese Mail kann weitere Erläuterungen enthalten, z.B. Informationen wie er in die Liste der erwünschten Empfänger aufgenommen werden kann.
- **Plausibilität:** Mails an nicht existierende Empfänger können direkt am externen Mail-Relay abgewiesen werden, wobei der Versand von sogenannten "Bounce-Mails" unterdrückt werden kann.
- **Prüfung:** Mails können auf RFC-Konformität geprüft und abgewiesen werden. Ein eingeschränkter RFC-konformer SMTP-Befehlssatz verhindert unerlaubte und unerwünschte Zugriffe wie etwa Fremdrelaying (Missbrauch des Mailservers durch Mail-Versender); Mails von unbekannten oder nicht existenten Absende-Domains können direkt abgewiesen werden.
- **Geschwindigkeit:** SpamFix basiert auf hochperformanten und skalierbaren Serverprozessen zur effizienten Einbindung der Komponenten sowie ggf. eines oder mehrerer Virenscannern.
- **Virenschutz:** Marktübliche Virenscanner wie z.B. die TREND MICRO Viruswall können optional in die SpamFix-Lösung eingebunden werden.
- **Viele weitere Funktionen:** Alle bekannten Weiterverarbeitungsmöglichkeiten von Mail, wie z.B. Aliase, Verteilerlisten, virtuelle Domains, Mailertables etc. sind mit SpamFix möglich oder können optional zusätzlich zu den vorhandenen Funktionen installiert werden.

Technische Grundlagen und Verfahren

- **Sicherheit:** Alle Prozesse laufen in einer sicheren Unix-Chroot-Umgebung. Eine SSL-Authentifizierung für SMTP ist möglich. Hoher Schutz gegen Buffer Overflows und vergleichbare Attacken durch Einsatz von Perl.
- **Prüfungen und Gewichtungen:** Vielzahl von Mustervergleichen und heuristischen Tests über die gesamte Mail. Jede Regel vergibt Punkte, die für jede Mail zu einem Beurteilungswert summiert werden. Ab einem einstellbaren Schwellwert wird die Mail als Spam klassifiziert.
- **Bayes-Klassifizierung:** Wahrscheinlichkeitsanalyse für Spam-Mails und erwünschte Mails anhand vorab oder nachträglich analysierter Mails (für Spam-Mails und erwünschte Mail).
- **Autolearning:** Die Inhalte der Bayes-Datenbanken und werden automatisch mit den Inhalten von Mails trainiert, die mit sehr hoher Wahrscheinlichkeit korrekt klassizifiert wurden.
- **Blacklists und Datenbanken:** Blacklists von unsicheren Mail-Relays (z.B. mail-abuse.org oder ordb.org) oder auch externe Datenbanken mit Spam-Signaturen (z.B. Razor und DCC) können in die Spam-Auswertung einbezogen werden und automatisch abgefragt werden.
- **Whitelists und Autowhitelisting** Whitelists mit bekannten Absendern können manuell erstellt oder anhand von Klassifizierungen mit sehr hoher Wahrscheinlichkeit automatisch generiert werden.
- **Erweiterbar:** Alle Regeln, Beurteilungs- und Schwellenwerte sowie alle Meldungen sind einfach über Textdateien zu editieren und zu erweitern.

Darstellung als Flussdiagramm

Dieses Flussdiagramm verdeutlicht den Ablauf der Mailverarbeitung durch die einzelnen Komponenten. Die Mail wird vom externen Postfix Mail Transfer Agent (MTA) aus dem Internet angenommen und schon dort einer Reihe von Plausibilitätsprüfungen unterzogen. Erst danach erfolgt die Weiterleitung an den Amavisd-New Daemon

Amavisd-New bindet die Sequenzen zur Klassifizierung der Mail durch datenbankgestützte Regelwerke zur Inhaltsbewertung ein und prüft jede Mail mit einer Reihe von komplexen Tests auf Spam oder „erwünschte Mail“. Befinden sich Absender oder Empfänger in den White- bzw. Blacklists oder überschreitet die Mail eine bestimmte Größe erfolgt keine Prüfung.

Nach der Verarbeitung durch Amavisd-New kann die Mail an ein Antivirus-System weitergeleitet werden. Die letzte Instanz ist wieder der Postfix MTA, der den Versand an die firmeninternen Mailserver bzw. Nutzer durchführt oder die Nachrichten ggf. in einer Mailqueue aufbewahrt.

Neben der technischen Administration und Pflege der Komponenten arbeitet die ESC im Rahmen des SpamFix-Services kontinuierlich an der Weiterentwicklung und Optimierung der Regelwerke.