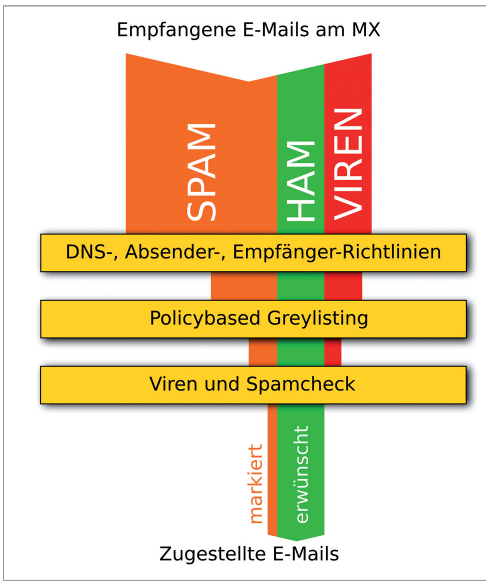
IT – iSPAMone



IT-Leistungspaket

iSPAMone ist der E-Mail Filterdienst der IT-Informatik GmbH

- Keine False-Positives
- Kein Administrationsaufwand
- Zuverlässige Mailkommunikation
- Hohe Verfügbarkeit
- Schutz der eigenen Infrastruktur
- Kategorisierung aller E-Mails

mailfiltering – the smart way

iSPAMone ist der E-Mail Filterdienst der IT-Informatik GmbH. Alle Mails werden zentral im IT-Rechenzentrum gefiltert und danach ihrem Mailserver zugestellt.

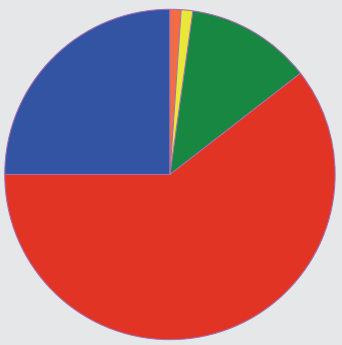
iSPAMone kombiniert bewährte OpenSource-Technologien mit den Produkten führender Antispam- und Antivirushersteller und kann dadurch den optimalen Schutz ihrer E-Mail-Infrastruktur – zu niedrigen Kosten – sicherstellen.

Der ASP Lösungsansatz bietet höchstmöglichen Komfort bei gleichzeitiger Flexibilität und maximaler Skalierbarkeit. Die vorhandene E-Mail-Infrastruktur muss nicht verändert werden und kann, durch das frühzeitige Blocken von unerwünschten E-Mails, erheblich entlastet werden.

Im Gegensatz zu herkömmlichen Spamfilterlösungen teilt iSPAMone E-Mails nicht nur in Spam und Nicht-Spam ein, sondern ordnet jeder E-Mail eine von 20 Kategorien zu, welche anschließend nach individuellen Richtlinien gefiltert werden.

Filtertechnologie

iSPAMone verwendet neben zwei Virenscannern, einer Antispam Engine und speziellen Antiphishing-Signaturen ein fortgeschrittenes DNS- und SMTP-Profiling um alle Arten von modernen Spam effektiv zu filtern. Durch die einmalige Technologie der Antispamengine kann modern gewordener Image-Spam genau wie jede andere Spammail gefiltert werden.



63% Drop
Der größte Anteil aller Zustellversuche werden schon durch einfache Checks beim Verbindungsaufbau abgelehnt. Zusätzlich werden ungültige Empfängeradressen bereits im SMTP-Dialog geblockt.

25% Defer
Über ein Viertel aller Verbindungen werden zurückgewiesen, bevor überhaupt die Übertragung der eigentlichen E-Mail begonnen hat. Durch die intelligente Kombination von RBLs, DNS-Checks und darauf basierendes Greylisting wird die Gefahr von False-Positives gebannt.

1% Quarantine, 1% Tag
Jede E-Mail wird mit den zwei integrierten Virenscannern und der Antispam Engine untersucht und je nach Richtlinie in Quarantäne gestellt oder markiert. Auch hier werden die E-Mails auf SMTP-Ebene abgewiesen, so dass E-Mails, die in der Quarantäne sind, offiziell nicht angenommen wurden.

10% Deliver
Nachdem die erwünschten E-Mails alle Checks bestanden haben, werden sie dem Kunden-Mailserver zugestellt und bei Verbindungsproblemen bis zu einer Woche zwischengespeichert.

Magirusstraße 17 · 89077 Ulm · Tel. +49 731 / 9 35 42-0 · info@it-informatik.de

IT – iSPAMone

ASP Lösung

99,5% Verfügbarkeit

Der iSPAMone-Dienst läuft auf einem hochskalierbaren Cluster im IT-Rechenzentrum. Genauso verfügbar ist auch der direkte Anschluss ans Internet gestaltet. Die Konnektivität ist mit redundanten Firewalls und mehreren schnellen Uplinks sichergestellt. Jede einzelne Komponente von iSPAMone wird rund um die Uhr 365 Tage im Jahr überwacht.

Kein administrativer Aufwand

iSPAMone ist ein wartungsfreier Dienst. Es müssen keine Black- und Whitelist gepflegt, keine Filter trainiert, keine Updates eingespielt und keine umfangreichen Quarantäneordner durchsucht werden. Manuelles nachjustieren der Filterregeln ist genauso unnötig wie Enduser-Quarantäneordner. Der iSPAMone Spamfilter hat ab dem ersten Einsatz eine kontinuierlich gute Trefferquote, so dass manuelles Eingreifen einfach unnötig ist.

Schutz der eigenen Infrastruktur

An den SMTP-Servern des iSPAMone-Dienstes beträgt der Anteil an Spam und anderen ungewollten E-Mails, wie Viren- oder Phishingmails, im Durchschnitt 90%.

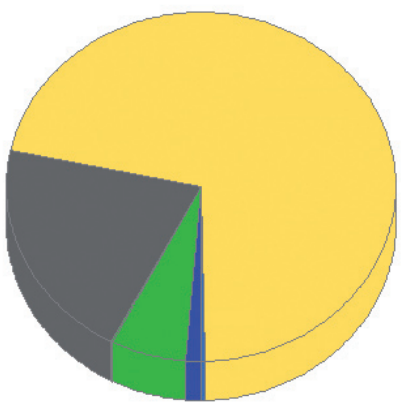
Durch die Verwendung von iSPAMone wird die firmeneigene Infrastruktur somit um 90% entlastet. Teure Internetverbindungen werden nicht mit unnötigem Traffic belastet und die Mailserver in der DMZ müssen nicht mehr kontinuierlich aufgerüstet werden, um mit der Spamflut mitzuhalten. Alle Spamwellen prallen ohne Auswirkungen für den eigentlichen Mailverkehr am iSPAMone-Dienst ab.

Monatliche Statistiken, Logs und Quarantäne

Über die Webseite von iSPAMone hat jeder Kunde Zugriff auf täglich aktualisierte Statistiken seines Mailverkehrs. Über das integrierte Logging kann zu jeder Zeit nachvollzogen werden, wie jede einzelne E-Mail kategorisiert wurde und ob und wann diese zugestellt wurde. Auf den optionalen Quarantäneordner kann mit jedem üblichen Mailprogramm über eine sichere IMAPS Verbindung zugegriffen werden.

Monatsübersicht

Status	Mails	Prozent
Bulk	2279	1.27 %
Bulk - Advertising	15	0.01 %
Bulk - Porn	7	0.00 %
Clean	11152	6.23 %
Clean - Almostempty	23	0.01 %
Clean - Bounce	240	0.13 %
Clean - Empty	1	0.00 %
Clean - Emptybody	16	0.01 %
Dangerous	0	0.00 %
Dangerous - Attachment	0	0.00 %
Dangerous - Code	0	0.00 %
Dangerous - iFrame	0	0.00 %
Error	0	0.00 %
Greylist	36938	20.65 %
Policy	0	0.00 %
Policy - Invalid	76	0.04 %
Policy - Invalid RCPT	127526	71.29 %
Policy - Mimerror	0	0.00 %
Size	0	0.00 %
Spam	553	0.31 %
Spam - ClamAV	47	0.03 %
Suspect	0	0.00 %
Undefined	0	0.00 %
Virus	5	0.00 %
Gesamt	178878	



Kategorisierung

Der iSPAMone Spamfilter ordnet jede E-Mail in eine von 20 Kategorien ein. Richtlinien bestimmen anschließend wie mit der E-Mail weiter verfahren wird. Die Aktion einer Richtlinie kann aus folgenden drei Optionen gewählt werden: Deliver (E-Mail annehmen und versenden), Tag (E-Mail mit „iSPAMone Kategorie" markieren und versenden), Quarantine (E-Mail in Quarantäneordner speichern und abweisen).

Bulk
In Massen versendete E-Mails, wie z. B. Newsletter.

Bulk – Advertising
Werbemails, die kein typischer Spam, aber in der Regel unerwünscht sind.

Bulk – Porn
E-Mails mit pornografischen Inhalten, die nicht „Spam" sind.

Clean
E-Mails, die keine verdächtigen Merkmale aufweisen.

Clean – Bounce
E-Mails, die wegen eines Zustellungsfehlers an den Absender zurück geschickt werden.

Clean – Empty
E-Mails, die weder über einen Betreff noch über einen Mailtext verfügen.

Clean – Emptybody
E-Mails, deren Mailtext leer und deren Betreff nicht leer sind.

Dangerous
E-Mails, die u. U. gefährlichen ausführbaren Code oder entsprechende Dateianhänge enthalten.

Dangerous – Attachment
E-Mails, die ein ausführbares Dateianhang enthalten.

Dangerous – Code
E-Mails mit potentiell gefährlichem Inhalt, wie z.B. Links auf lokale Dateien.

Dangerous – iFrame
E-Mails, die das iFrame-Feature benutzen.

Error
E-Mails, bei denen ein Verarbeitungsfehler aufgetreten ist.

Policy
E-Mails mit unerwünschten Dateianhängen.

Policy – Invalid
E-Mails mit ungültigem Headersyntax.

Policy – Mimerror
E-Mails mit defekter Mime-Codierung.

Spam
Eindeutig identifizierte Spam- und Phishing-E-Mails.

Spam – ClamAV
Eindeutig identifizierte Spam-E-Mails, die von speziellen Phishing-Signaturen erkannt wurden.

Suspect
E-Mails mit Verdachtsmomenten für „Spam" oder „Bulk".

Undefined
E-Mails ohne Kategorisierung, dies sollte nicht vorkommen.

Virus
E-Mails die Viren enthalten.

Magirusstraße 17 · 89077 Ulm · Tel. +49 731 / 9 35 42-0 · info@it-informatik.de