

noSpam proxy®

Gute Nachrichten für Ihren Mailserver

NoSpamProxy läuft als Software auf Ihrem Windows Server und wehrt Spam, Phishing und Malware intelligent ab. Ein Regelwerk gibt Ihnen die Möglichkeit, sein Verhalten auf Ihre Bedürfnisse anzupassen.

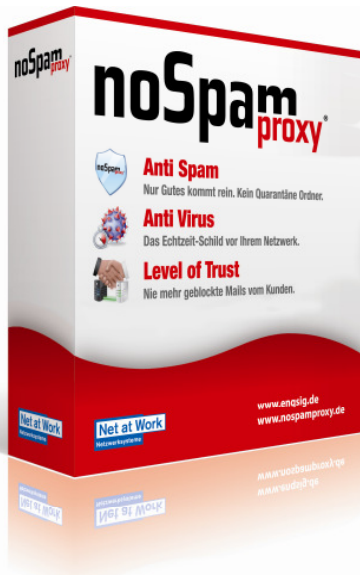
NoSpamProxy tritt gegen die drei Hauptprobleme von Spam an:

- betrügerische Angebote oder verlockende Websites mit Schädlingen
- verlorene Arbeitszeit durch manuelles Kontrollieren vorsortierter Spam Mails
- verlorene Kommunikation durch unbedachtes Löschen oder unbeaufsichtigte Filter-Systeme

Anti-Spam – Nur Gutes kommt rein. Kein Quarantäne-Ordner.

Anti-Virus – Das Echtzeit-Schild vor Ihrem Netzwerk.

Level of Trust – Nie mehr geblockte Mails von Kunden.



Nur erwünschte E-Mails erreichen Ihren Mailserver und Ihr Postfach

NoSpamProxy scannt Emails schon während des SMTP-Empfangs und klassifiziert die Email anhand von unterschiedlichen Filtern. Wird eine Email als Spam klassifiziert, so wird diese Email nicht vom System angenommen. Wird die Email als vertrauenswürdig eingestuft, darf diese passieren.

Bekannte Kommunikationspartner werden nicht abgewiesen

Auch ausgehende Emails werden von NoSpamProxy gescannt. Die Software vergibt bei ausgehenden Emails Vertrauenspunkte an den Empfänger der Email. Die Vertrauenspunkte-Datenbank wird dann bei eingehenden Emails genutzt, um bei einer bestehenden Kommunikationsbeziehung die Email passieren zu lassen, auch wenn andere Filter diese Email als nicht vertrauenswürdig einstufen (z.B. Sender steht auf einer Blacklist).

Absender erfahren, wenn ihre Mail als Spam klassifiziert wird

Sollte dennoch eine vertrauenswürdige Email nicht angenommen werden, so wird der Sender der Email über die verhinderte Zustellung durch seinen Mailserver informiert!

NoSpamProxy setzt auf die folgenden Filtersysteme und Funktionen:

- Level-of-Trust
- Unscharfe Prüfsummen
- Greylisting
- Statistische Analyse (Bayes)
- Realtime Blocklists
- Spam URI Realtime Blocklists
- Wortübereinstimmungen
- Spam Assassin Konnektor
- Zero Hour™ Virus Protection
- Dateibasierter Virenschanner
- Adressmanipulation
- E-Mail Archivierung
- Attachment Manager

Microsoft®-like und auf die konkrete Situation anpassbar

NoSpamProxy ist als Windowsdienst konzipiert und lässt sich mit Windows Server 2003 und 2008 betreiben. Die Verwaltung erfolgt über die für Administratoren vertraute Microsoft Management Console (MMC) vom Server oder PC aus. NoSpamProxy wurde mit dem Microsoft-Siegel „Works with Windows 2008“ ausgezeichnet.

NoSpamProxy wird mit einem optimierten Regelwerk für die Spam- und Virus-Abwehr geliefert, und ist damit sofort einsatzbereit. Über die Konfigurationsmöglichkeiten und das Regelwerk kann er auf Ihre konkreten Bedürfnisse detailliert eingestellt werden.

Die Gefahr herkömmlicher Anti-Spam Lösungen

Das Problem aller Spamschutzlösungen ist, dass eine Software entscheidet, ob eine Mail als "Spam" klassifiziert wird oder passieren darf. Das generelle Problem hierbei ist, dass nicht alle Spamnachrichten erkannt und auch gute Mails fälschlicherweise blockiert werden (False Positive).

Genau diese False Positives sind es, die bei herkömmlichen Lösungen ein Risiko darstellen. Nachteilig wird diese Fehlerkennung dann, wenn solche Mails gelöscht oder in eine Quarantäne abgelegt werden. Niemand wird in tausenden von erkannten Spamnachrichten die eine falsch klassifizierte Mail suchen wollen.

NoSpamProxy sichert die Kommunikation und informiert Absender

Auch NoSpamProxy kann Nachrichten irrtümlich als Spam erkennen, aber im Gegensatz zu anderen Lösungen verweigert NoSpamProxy die Annahme der Mail. Damit erhält der Absender eine Unzustellbarkeitsnachricht und kann darauf reagieren. Ein guter Absender wird informiert, dass die Mail nicht zugestellt wurde. Er kann über einen anderen Weg den Kontakt herstellen. Für Spammer wird die Empfängeradresse aufgrund des Mehraufwandes uninteressant.

Das Problem „False Positive“ erklärt

False Positives sind durch keine Lösung zu vermeiden. Zwar können Sie mit entsprechenden Einstellungen der Filter die Wahrscheinlichkeit des Auftretens verringern, aber zugleich verschlechtert sich damit auch die Erkennungsrate. 0% False Positive erreichen sie nur dann, wenn Sie keinen Filter einsetzen.

Bekannte Kommunikationspartner werden nicht abgewiesen

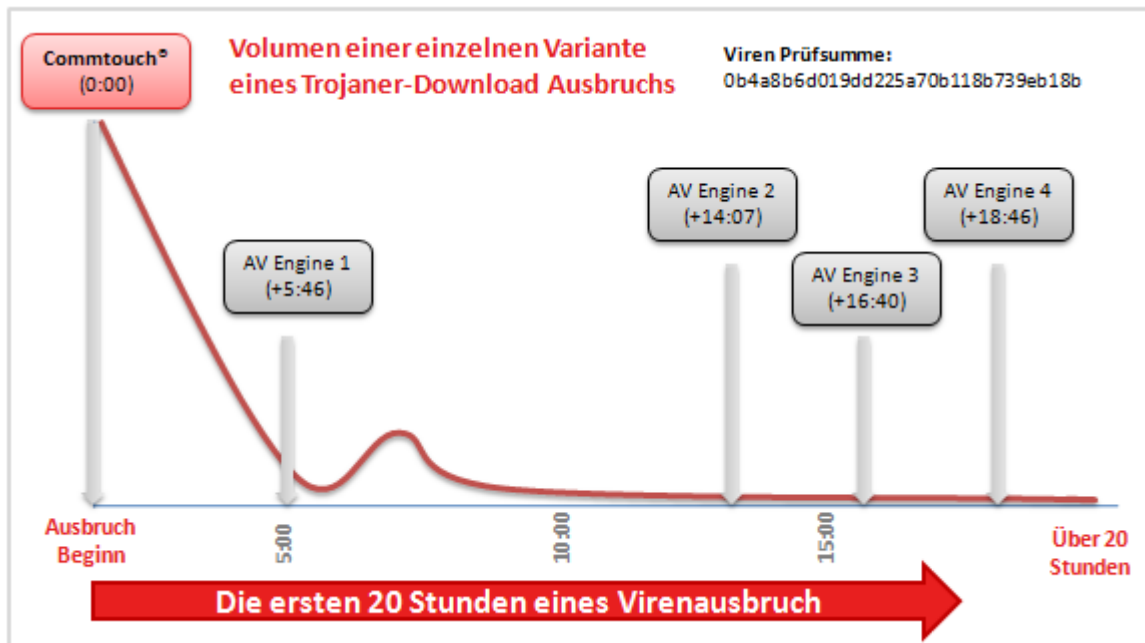
Eine Schlüsselkomponente von NoSpamProxy ist eine Funktion, die es bislang in keiner anderen Anti-Spam-Lösung gibt. Der Filter "Level of Trust". Der Filter lernt die Kommunikationsbeziehungen – Sender- und Empfänger-Adressen – und vergibt hierfür Vertrauenspunkte. Sobald Sie eine Mail an Ihren Kommunikationspartner versandt haben, kann dieser Antworten senden und NoSpamProxy überwinden, selbst wenn seine Mail Spam-Eigenschaften aufweist.

Kinderleichtes Freischalten von Kommunikationspartnern spart Administrationsaufwand

Level of Trust bietet damit auch die Funktion der dynamischen Whitelist. Wird ein Kommunikationspartner irrtümlich als Spammer abgelehnt, genügt es ihm eine Mail zuzusenden. Durch Level of Trust erhält er Vertrauenspunkte und ist somit wieder für NoSpamProxy freigeschaltet. Somit entfällt der administrative Aufwand für das statische Pflegen von Whitelists.

Anti-Virus: Das Echtzeit-Schild vor Ihrem Netzwerk.

Spam und Malware gehen immer öfter Hand in Hand. Cyberkriminelle nutzen Spam, um Malware zu verbreiten, und Malware, um fremde PCs in Spamschleudern zu verwandeln. Um solche kombinierten Bedrohungen abzuwehren, enthält NoSpamProxy einen integrierten Virenschutz. Die integrierte Zero-Hour™ Outbreak Protection Lösung bietet folgende Vorteile:



Kein Warten auf die aktuelle Viren-Signatur:

NoSpamProxy integriert die Zero-Hour Lösung von Commtouch, die auf proaktivem Scannen des Internets und der Identifikation von massiven Virus-Ausbrüchen basiert. Im Gegensatz zu Signatur-basierten Verfahren erkennt diese Lösung Virenausbrüche, wenn Sie auftreten und kann bereits in der ersten Stunde Ihr Mailsystem davor schützen.

Robust und dynamisch für schnellsten Schutz gegen neue Bedrohungen

Robust und von Natur aus immun gegen neu auftretende Angriffe, hat Commtouch's Zero Hour Technologie eine bewährte Historie als eine der besten proaktiven Anti-Virus Lösungen. Der Zero-Hour Schutz basiert auf der Recurrent Pattern Detection™ (RPD™) Technologie die über 35 Millionen Anwender weltweit schützt.

Anstatt jede einzelne Nachricht zu analysieren, untersucht Commtouch's patentierte Technologie große Mengen von Internetverkehr in Echtzeit, über 2 Milliarden Nachrichten pro Tag. Auf Basis der Analyse von wiederkehrenden Verbreitungs- und Struktur-Mustern in den Commtouch Rechenzentren werden neue Spam- und Malware-Ausbrüche identifiziert sobald sie auftreten.

Systemvoraussetzungen

- Windows 2003/2008 Server
- .NET Framework 2.0
- MS SQL oder SQL Express Edition
- TCP/IP und SMTP für eingehende Nachrichten
- Mailempfang per SMTP