

Es gibt gute Nachrichten für Ihren Mailserver

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

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

Level of Trust – nie mehr geblockte E-Mails von Kunden.

■ 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-E-Mails
- verlorene Kommunikation durch unbedachtes Löschen oder unbeaufsichtigte Filter-Systeme

Nur erwünschte E-Mails erreichen Ihren Mailserver und Ihr Postfach

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

Bekanntes Kommunikationspartner werden nicht abgewiesen

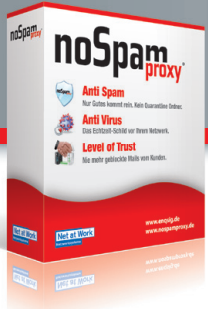
Auch ausgehende E-Mails werden von NoSpamProxy gescannt. Die Software vergibt bei ausgehenden E-Mails Vertrauenspunkte an ihren Empfänger. Die Vertrauenspunkte-Datenbank wird dann bei eingehenden E-Mails genutzt, um eine E-Mail bei einer bereits bestehenden Kommunikationsbeziehung passieren zu lassen. Das geschieht auch, wenn andere Filter diese E-Mail als nicht vertrauenswürdig einstufen, z.B. weil ihr Absender auf einer „Blacklist“ steht.

Absender erfahren, wenn ihre E-Mail als Spam klassifiziert wird

Sollte dennoch eine vertrauenswürdige E-Mail nicht angenommen werden, so wird der Sender der E-Mail über die verhinderte Zustellung durch seinen E-Mail-Server informiert!

NoSpamProxy setzt auf folgende 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
- Attachment Manager
- Zeichensatzfilter



Datenblatt

Anpassbar und im vertrauten Look

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 R2“ 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 das Produkt auf Ihre konkreten Bedürfnisse detailliert eingestellt werden.

Die Gefahr herkömmlicher Lösungen

Das Problem aller Spam-Schutzlösungen ist, dass eine Software entscheidet, ob eine E-Mail als „Spam“ klassifiziert wird

oder passieren darf. Die generelle Schwierigkeit hierbei ist, dass nicht alle Spam-Nachrichten erkannt und auch gute E-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 E-Mails gelöscht oder in eine Quarantäne abgelegt werden. Niemand wird in tausenden von erkannten Spam-Nachrichten die eine falsch klassifizierte E-Mail suchen wollen.

NoSpamProxy sichert die Kommunikation und informiert Absender

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

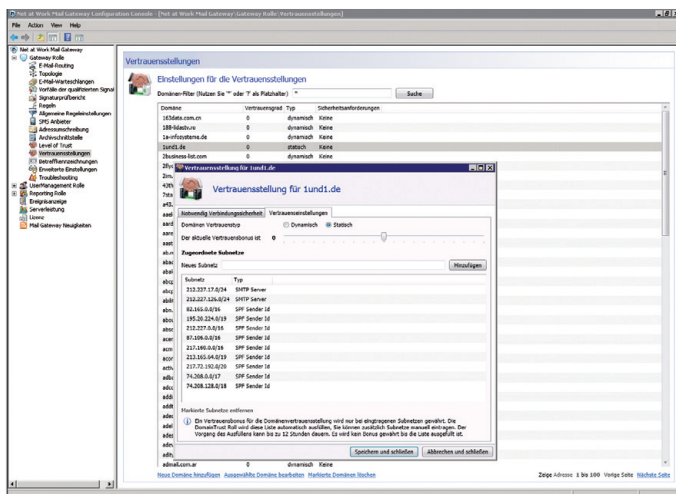
#	Aktiv	Name	Richtung	Quell Gateway	Absender	Empfänger	Entscheidung	Filter	Aktionen
1	✗	Outbound mails without signature and/or encryption	Ausgehend	Interner Absender	Alle	Alle	Zustellen		
2	✓	All outbound mails	Ausgehend	Interner Absender	Alle	Alle	Zustellen		Signieren und/oder Verschlüsseln von E-Mails E-Mail in ein PDF Dokument konvertieren Anhänge mit einem Passwort schützen
3	✓	Whitelist	Eingehend	Externer Absender	Alle	Lokale Benutzer	Zustellen	Zusätzliche Filter werden angewendet	
4	✓	Blacklist	Eingehend	Externer Absender	Alle	Lokale Benutzer	Abweisen	Zusätzliche Filter werden angewendet	
5	✓	Inbound mails with internal sender	Eingehend	Externer Absender	Eigene Domänen	Eigene Domänen	Abweisen		
6	✓	All other inbound mails	Eingehend	Externer Absender	Alle	Lokale Benutzer	Überprüfen Abweisen wenn SCL 4 erreicht	CommTouch AntiSpam Dienst (1) Spam URI Realtime Blocklists (2) Realtime Blocklists (2)	CommTouch Zero Hour Virus Outbreak Protection Überprüfen der Signatur und/oder entschlüsseln von

Das Problem „False Positive“ verstehen

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

Ein Filter schafft Vertrauen: Level of Trust

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



Leichtes Freischalten von Kommunikationspartnern spart Administrationsaufwand

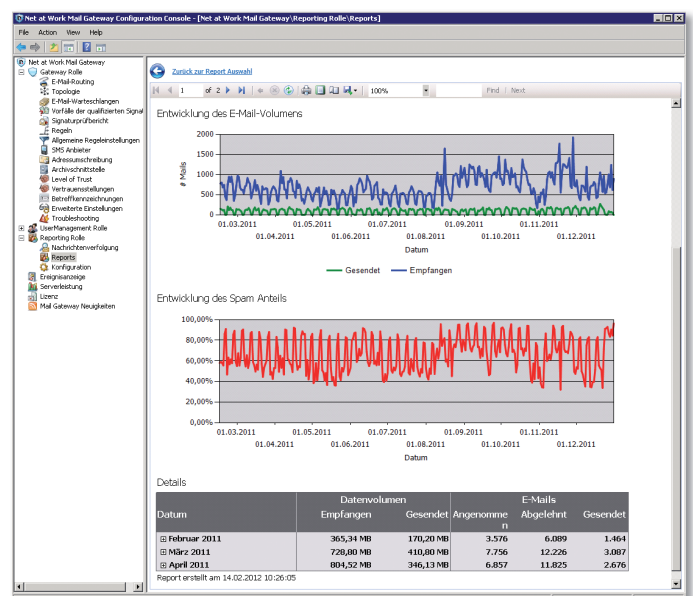
Level of Trust bietet damit auch die Funktion der dynamischen Whitelist. Wird ein Kommunikationspartner irrtümlich als Spammer klassifiziert und damit abgelehnt, genügt es ihm eine E-Mail zuzusenden. Durch Level of Trust erhält er Vertrauenspunkte und ist somit wieder für NoSpamProxy freigeschaltet.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

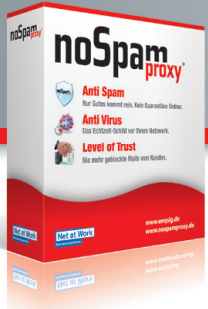
Auskunftsfähig durch E-Mail-Archivierung

NoSpamProxy bietet ab der Version 7.6. eine einheitliche Konfiguration der Funktionen zur E-Mail Archivierung. Damit kann am Gateway eine vollständige Journal-Archivierung erreicht werden. Im Journal-Archiv werden alle eingehenden und ausgehenden Nachrichten gespeichert und stehen so für Auskünfte und als Beweisgrundlage noch nach Jahren zur Verfügung. Durch die Kopplung mit den Anti-Spam-Funktionen werden nur gewünschte und tatsächlich angenommene Nachrichten archiviert. Als Speicherlösung stehen neben dem Filesystem die Archivschnittstellen zu d.velop d3 und Ceyonig nscale zur Verfügung.

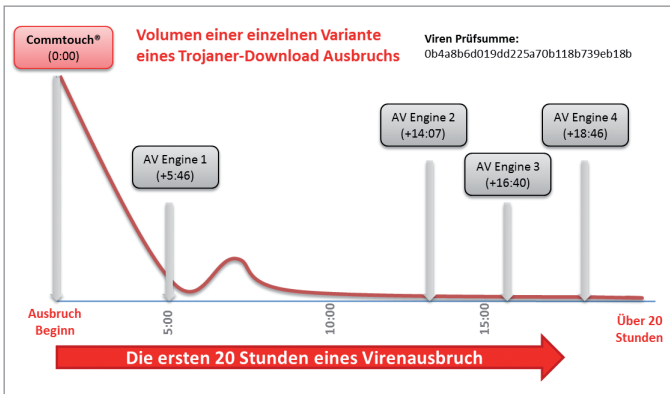
NoSpamProxy ständig im Blick

Mit der Reporting-Funktion von NoSpamProxy haben Sie Ihren E-Mail-Verkehr ständig unter Kontrolle. Durch Reports lassen sich das Datenvolumen sowie das E-Mail- und Spam-Aufkommen detailliert bis auf Benutzerebene analysieren. Die integrierte Nachrichtenverfolgung protokolliert jede E-Mail und zeichnet auf, wie diese behandelt wurde: Welche Regeln waren aktiv? Welche Filter haben Einfluss genommen und welche Aktionen wurden mit der E-Mail ausgeführt? Mit dem NoSpamProxy-eigenen Ereignisprotokoll haben Administratoren alle Meldungen im Windowsprotokoll an einer Stelle im Überblick.





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 „Spam-Schleudern“ zu verwandeln. Um solche kombinierten Bedrohungen abzuwehren, enthält NoSpamProxy einen integrierten Virenschutz, die Zero-Hour™ Outbreak-Protection-Lösung mit folgenden Vorteilen:

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 E-Mail-System davor schützen.

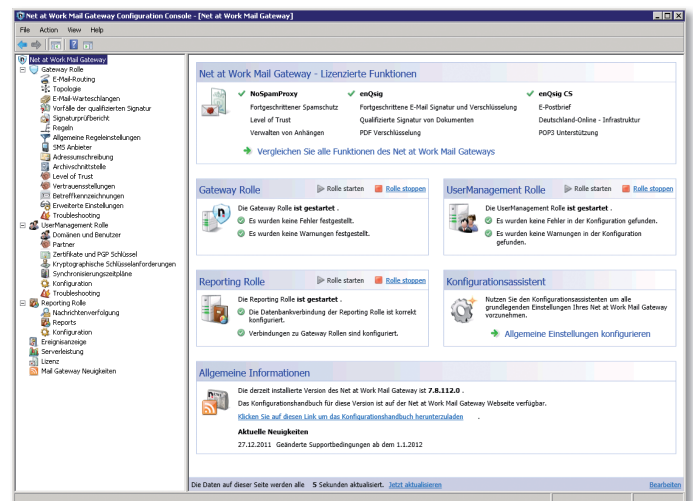
Robust und dynamisch für schnellsten Schutz gegen Bedrohungen

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

Mehrnutzen durch E-Mail-Verschlüsselung und qualifizierte Signatur

Würden Sie Ihre geschäftliche Kommunikation per Postkarte abwickeln? Wohl kaum. Letztlich gleicht die unverschlüsselte E-Mail-Kommunikation in Unternehmen aber dieser Vorgehensweise. Um die geschäftliche E-Mail-Kommunikation besser zu schützen, wird immer häufiger E-Mail-Verschlüsselung eingesetzt. Da NoSpamProxy die Technologiebasis mit unserem Gateway für E-Mail-Verschlüsselung enQsig teilt, lassen sich dessen Funktionen einfach durch eine Lizenzerweiterung freischalten. So kann auf nur einem Gateway und mit einheitlicher Administration auch der Schutz der E-Mail-Inhalte umgesetzt werden.



Systemvoraussetzungen:

- Windows Server 2003/2008/R2 (32/64 Bit)
- .NET Framework 4.0
- MS SQL oder SQL Express Edition
- Mailempfang per SMTP