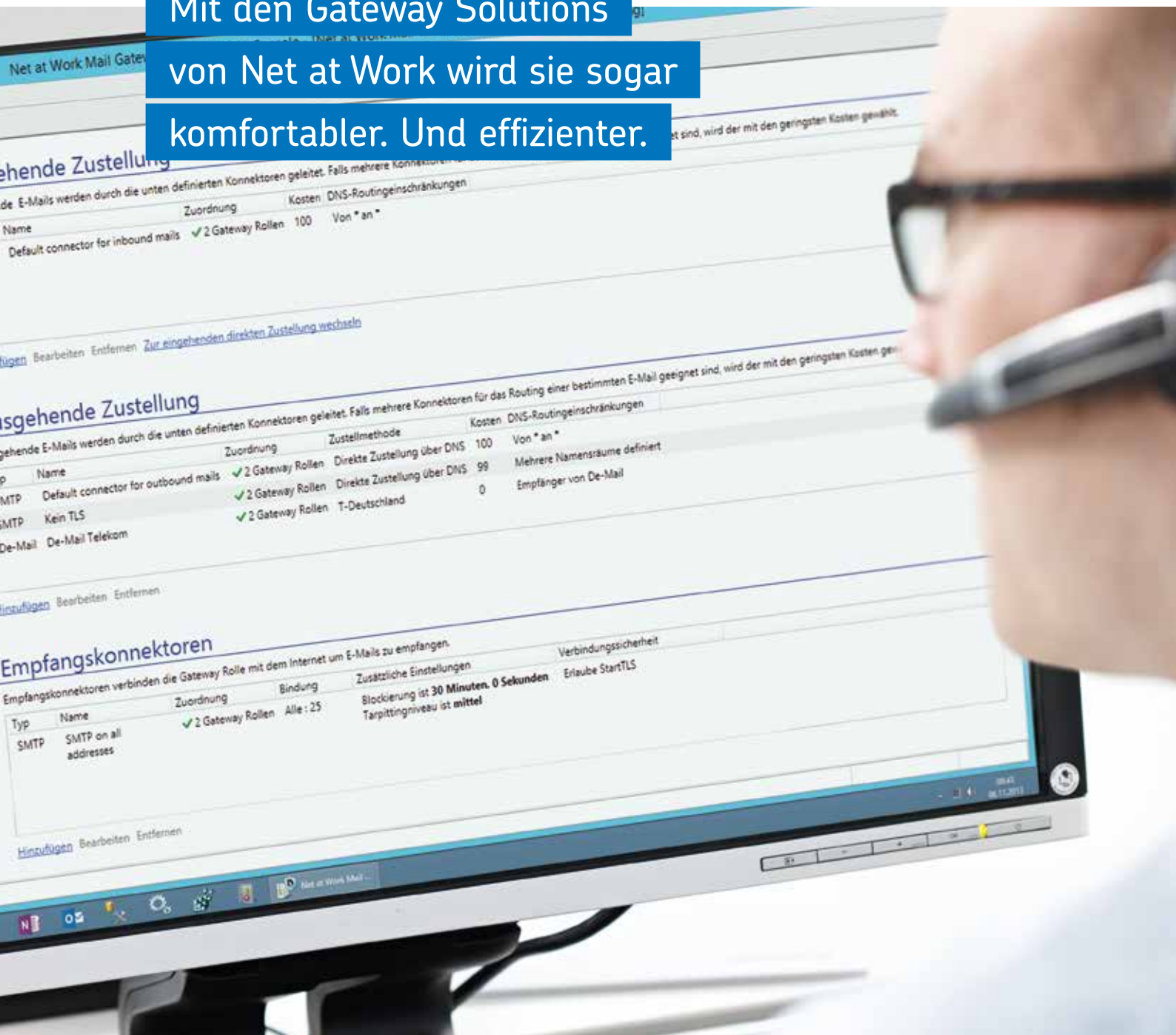
Net at Work
Building IT-Excellence.

Ihre E-Mail-Kommunikation muss sicher funktionieren. Mit den Gateway Solutions von Net at Work wird sie sogar komfortabler. Und effizienter.



Hier sind Sie sicher

Die Sicherheit der Kommunikation gewinnt für Unternehmen, Behörden und Institutionen zunehmend an Bedeutung. Dabei geht es zum einen um die Bewahrung der Vertraulichkeit von Informationen. So sollen E-Mails und Dateien den Empfänger erreichen, ohne dass unbefugte Dritte Einsicht erhalten können. Zum anderen geht es um den Schutz vor unerwünschten Nachrichten. Denn die Flut an Spam und Malware sorgt für hohen Arbeitsaufwand und Gefahren für die gesamte IT-Infrastruktur.

Es beginnt an der Quelle
Untersuchungen haben bewiesen: Der größte Risikofaktor für sichere Kommunikationsprozesse sind die Beteiligten selbst. Herkömmliche Sicherheitsmaßnahmen erfordern Zeit und Aufmerksamkeit, die viele Mitarbeiter nicht aufbringen können. Wenn hier das entsprechende Bewusstsein nicht vorhanden ist, können Security-Systeme nicht zuverlässig funktionieren.

Die Gateway Solutions von Net at Work gehen einen neuen Weg. Als Software auf dem Windows Server werden zahlreiche Funktionen zur sicheren Übertragung und zum Schutz vor Spam und Viren automatisch ausgeführt. Das Ergebnis: Die Anwender sind entlastet und Administratoren können die IT-Infrastrukturen einfacher, transparenter und effizienter sichern.

Die sicheren Verbindungen
Mit den Gateway Solutions von Net at Work schützen Sie Ihre Kommunikation und Zusammenarbeit durch die intelligente Verbindung zahlreicher Sicherheitsfunktionen.

enQsig sichert die Vertraulichkeit und Rechtssicherheit der E-Mail-Kommunikation
- zuverlässige E-Mail-Verschlüsselung
- passwortbasierte PDF Mail
- flexible De-Mail-Anbindung

NoSpamProxy tritt gegen die drei Hauptprobleme von Spam an
- Malware in Mails und betrügerische Angebote oder verlockende Websites mit Schädlingen
- verlorene Arbeitszeit durch manuelles Kontrollieren vorsortierter Spam-E-Mails
- ineffiziente Kommunikation durch unbedachtes Löschen oder unbeaufsichtigte Filtersysteme

Produktedition
- NoSpamProxy
- enQsig
- enQsig CS

Lizenzierung
- Benutzer
- Domain
- Nutzung

Vertrauliche E-Mail-Kommunikation
braucht Datenschutz und Rechtssicherheit.
Die Schlüssel dazu hat enQsig.

enQsig®

Vertrauen und Vertraulichkeit

E-Mail-Kommunikation in Unternehmen ist heute der Lebensnerv für das Tagesgeschäft und beinhaltet oftmals sensible Vorgänge. enQsig unterstützt den sicheren und datenschutzkonformen E-Mail-Verkehr durch eine flexible Auswahl von Standardtechnologien.

Der erste Schritt ist die elektronische Verschlüsselung und Signatur mit S/MIME oder PGP der E-Mails. enQsig führt diese Signatur am Gateway ohne Aufwand für die Benutzer durch. Mit der E-Mail-Signatur wird sichergestellt, dass E-Mails unverändert beim Empfänger ankommen. Der nächste Schritt ist die Verschlüsselung der Nachrichten. enQsig verschlüsselt E-Mails nach den Internetstandards S/MIME oder PGP. Für die sichere Ad-hoc-Kommunikation bietet die Softwarelösung auch das passwortbasierte Verfahren PDF Mail an.

Einfach und zentral

Bei herkömmlicher E-Mail-Verschlüsselung müssen Benutzer diese manuell aktivieren und die Zertifikate der Kommunikationspartner verwalten. Dies ist aufwändig und kann die Akzeptanz gefährden. Mit enQsig werden die für Ver- und Entschlüsselung benötigten kryptographischen Schlüssel zentral verwaltet.

Durch das Gateway entschlüsselte E-Mails können vor der Zustellung mit NoSpamProxy auf Spam und Viren geprüft werden. Über ein flexibles Partnermanagement wird das Verschlüsselungsverfahren für ausgehende E-Mails zentral konfiguriert. Für Hochverfügbarkeit kann die Softwarelösung auf mehreren Server installiert und zugleich zentral verwaltet werden. Die zentrale Steuerung reduziert den Verwaltungsaufwand wesentlich und erleichtert die Compliance- und Governance-Anforderungen.

Sicher kommunizieren mit PDF Mail

Für die E-Mail-Verschlüsselung sind Internetstandards wie S/MIME und PGP die sicherste Methode. Allerdings unterstützen viele Kommunikationspartner diese nicht. enQsig bietet mit der automatisierten PDF-Verschlüsselung ein passendes Verfahren. Dabei werden E-Mails mit allen Dateianhängen in ein PDF gewandelt und mit einem Passwort verschlüsselt. Das Passwort kann dem Empfänger über enQsig automatisiert per SMS zugesandt oder auf anderem Wege übermittelt werden. PDF Mail ist vor allem für Unternehmen interessant, die personenbezogene Daten versenden wie z.B. Versicherungen, Banken, Rechtsanwälte oder Steuerberater.

Schlüsselverwaltung

Für die E-Mail-Verschlüsselung nach dem S/MIME-Verfahren benötigen Anwender und Unternehmen Zertifikate nach dem X.509-Standard. enQsig zentralisiert und automatisiert die Verwaltung dieser Zertifikate. Anwender sind von den Verwaltungsaufgaben vollständig entlastet und Administratoren profitieren von einer Vielzahl hilfreicher Funktionen.

Das Zertifikatsmanagement unterstützt Benutzer- und Domänenzertifikate beliebiger Trustcenter und importiert Zertifikate automatisiert aus eingehenden E-Mail-Signaturen. Für die einfache und schnelle Verteilung von Benutzerzertifikaten hat enQsig eine Schnittstelle für das Trustcenter der Deutschen Post Signtrust integriert. Darüber hinaus können PGP-Schlüssel generiert, importiert und verwaltet werden. Über eine interne Active-Directory-Zertifizierungsstelle lassen sich Zertifikate direkt anfordern und über Active-Directory-Gruppen auch gezielt verteilen. Die Anbindung an öffentliche Schlüsselverzeichnisse ermöglicht die automatische Suche nach Verschlüsselungszertifikaten oder PGP-Schlüsseln. Durch die automatisierten und zentralisierten Managementfunktionen können Verschlüsselungsprojekte wesentlich günstiger umgesetzt werden und liefern auch im Betrieb nachhaltige Kosteneinsparungen.

Web Portal: sicher ohne Zertifikat

Die verschlüsselte E-Mail-Kommunikation mit Partnern, die keine Verschlüsselung nutzen, ist mit dem enQsig Web Portal sehr bequem. Das Web Portal ermöglicht es dem Empfänger einer geschützten PDF Mail, sich selbst ein Passwort zu vergeben. Dies erleichtert den Umgang mit den verwendeten Passwörtern erheblich und trägt zudem zur höheren Sicherheit bei. Darüber hinaus kann der Empfänger der PDF Mail mit dem Web Portal direkt auf die Nachricht antworten. So wird eine gesicherte E-Mail-Kommunikation in beide Richtungen möglich.

Outlook Add-In: mehr Möglichkeiten

Neben dem zentralen Gateway liefern wir ein Outlook Add-In, das die Verschlüsselungsfunktionen komfortabel steuert. Das Add-In ermöglicht Benutzern, Einstellungen für die E-Mail-Verschlüsselung und PDF Mail vorzunehmen und unterstützt darüber hinaus die besonderen Funktionen von De-Mail. Eine zentrale Verwaltung des Outlook Add-Ins durch Administratoren ist über Gruppenrichtlinien möglich.

Große Dateien einfach, sicher und ohne Medienbruch versenden

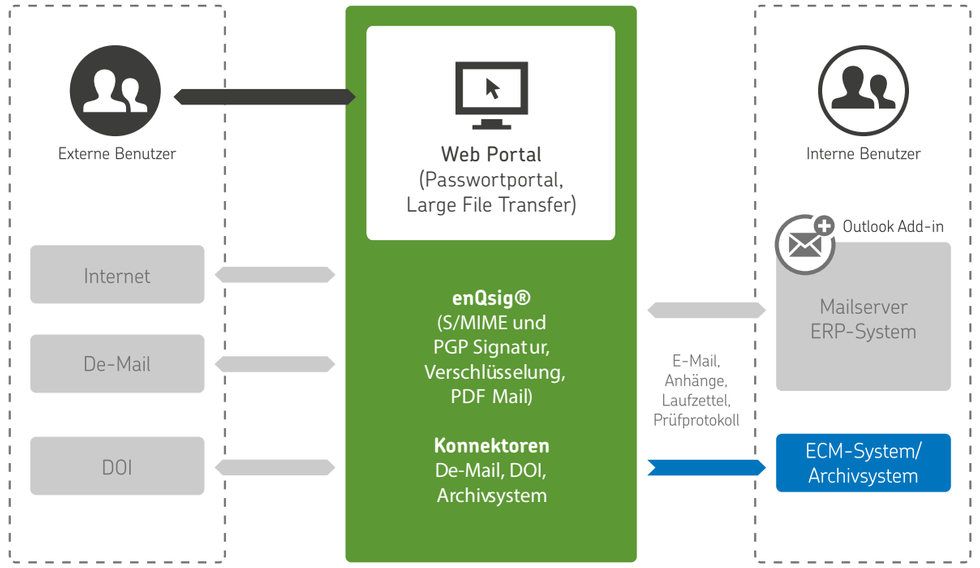
Das Erweiterungsmodul Large File Transfer erlaubt es Nutzern, beliebig große Dateien direkt aus dem Outlook zu versenden. Anwender können auf diese Weise auch große Dateien, die die Beschränkungen des Mail-Programms überschreiten, ohne Medienbruch mit einem einzigen Klick versenden. Der Einsatz des Tools ist unkompliziert und mit dem Versand herkömmlicher Dateianhänge vergleichbar. Im Gegensatz zu den weit verbreiteten Cloud-basierten File-Transfer-Diensten werden die Daten über einen Kunden-eigenen Web-Server bereitgestellt und via SSL verschlüsselt übertragen. Das Sicherheitsniveau der Lösung wird damit auch kritischen Business-Anforderungen jederzeit gerecht.

Flexible Anbindung an De-Mail

enQsig CS ermöglicht Unternehmen und Behörden den sicheren und zentralen Zugang zum De-Mail-System. De-Mails können somit direkt aus den internen Mailsystemen versandt und dort empfangen werden. enQsig CS verfügt über Schnittstellen für die Integration von Fachverfahren, ECM- und E-Mail-Systemen. Durch die Umstellung auf das rechtssichere elektronische System De-Mail können Geschäftsprozesse ohne Medienbruch effizient umgesetzt werden. Damit sind auch beträchtliche Kostensenkungen im Briefverkehr mit Kunden und Bürgern verbunden. enQsig CS ist Teil von enQsig und als weitere Produktvariante auch separat erhältlich.

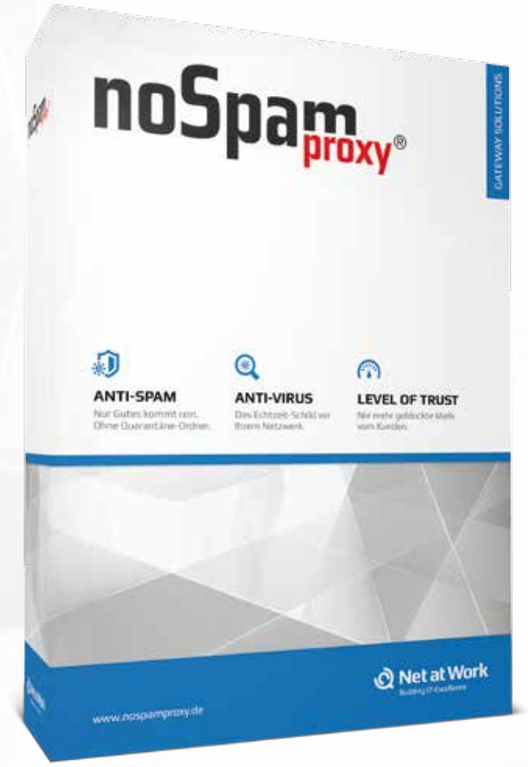
Mehrwert durch Antivirus

NoSpamProxy integriert die vielfach ausgezeichnete Antivirus-Komponente von CYREN. Sie bietet eine höchsteffiziente Erkennung bei geringem Ressourcenbedarf und blockt jede Art von Malware wie Würmer, Trojaner und Spyware ab. Die einzigartige Kombination von signaturbasierten Verfahren und Mustererkennung ermöglicht die extrem hohe Erkennungsrate sowohl von bekannten wie auch unbekannten Schädlingen.

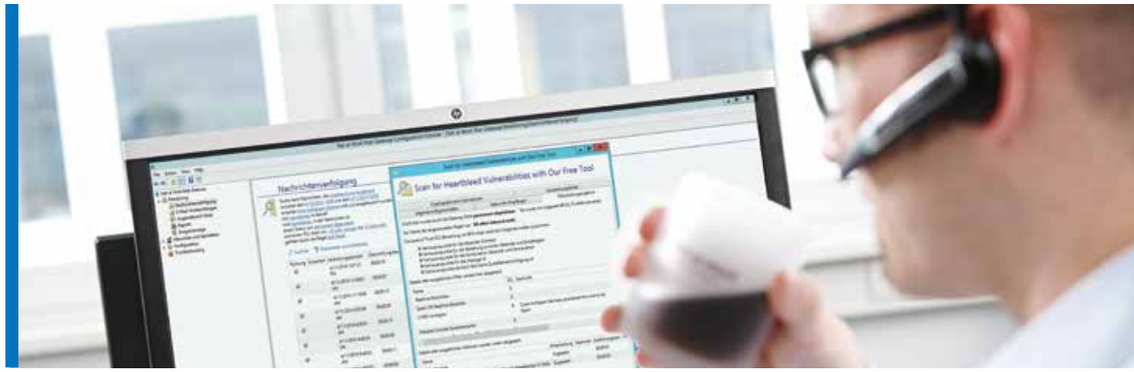


Systemvoraussetzungen enQsig: Windows Server 2003 SP2 oder höher • .NET Framework 4.5.1 oder höher für Windows 2008, Framework 4.0 auf Windows 2003, Microsoft SQL Server 2005 oder höher, SQL Express Edition 2005 oder höher • SMTP zum internen Mailsystem Microsoft Report Viewer 2010 Systemvoraussetzungen enQsig Web Portal: Windows Server 2008 R2 oder höher mit installiertem IIS • .NET Framework 4.5.1 oder höher • Express Edition 2008 oder höher, SQL Express Edition 2008 oder höher

Haben Sie etwas gegen
Spam, Phishing oder Malware?
Wir haben NoSpamProxy.



noSpamproxy®



Nur echte E-Mails für Ihren Mailserver

NoSpamProxy läuft auf Ihrem Server und prüft E-Mails anhand von zahlreichen Filtern bereits vor dem Empfang. Klassifiziert die Anwendung eine E-Mail als Spam, so wird die Annahme verweigert. Wird die E-Mail als vertrauenswürdig und virenfrei eingestuft, darf sie passieren. Auch ausgehende E-Mails werden von NoSpamProxy überprüft. Die Softwarelösung lernt dabei automatisch Ihre vertrauenswürdigen Kommunikationspartner. Dies wird bei zukünftigem E-Mail-Verkehr berücksichtigt.

Einfach und hochflexibel

Die Verwaltung erfolgt über die Microsoft Management Console (MMC). NoSpamProxy wird mit einem optimierten Regelwerk für die Spam- und Virusabwehr geliefert und ist sofort einsatzbereit. Darüber hinaus kann die Lösung auf Ihre persönlichen Anforderungen eingestellt werden. Eine hochverfügbare Umgebung kann durch die Installation der Software auf mehreren Servern geschaffen werden. Die Konfiguration wird dabei automatisch abgeglichen.

Die Gefahr herkömmlicher Lösungen

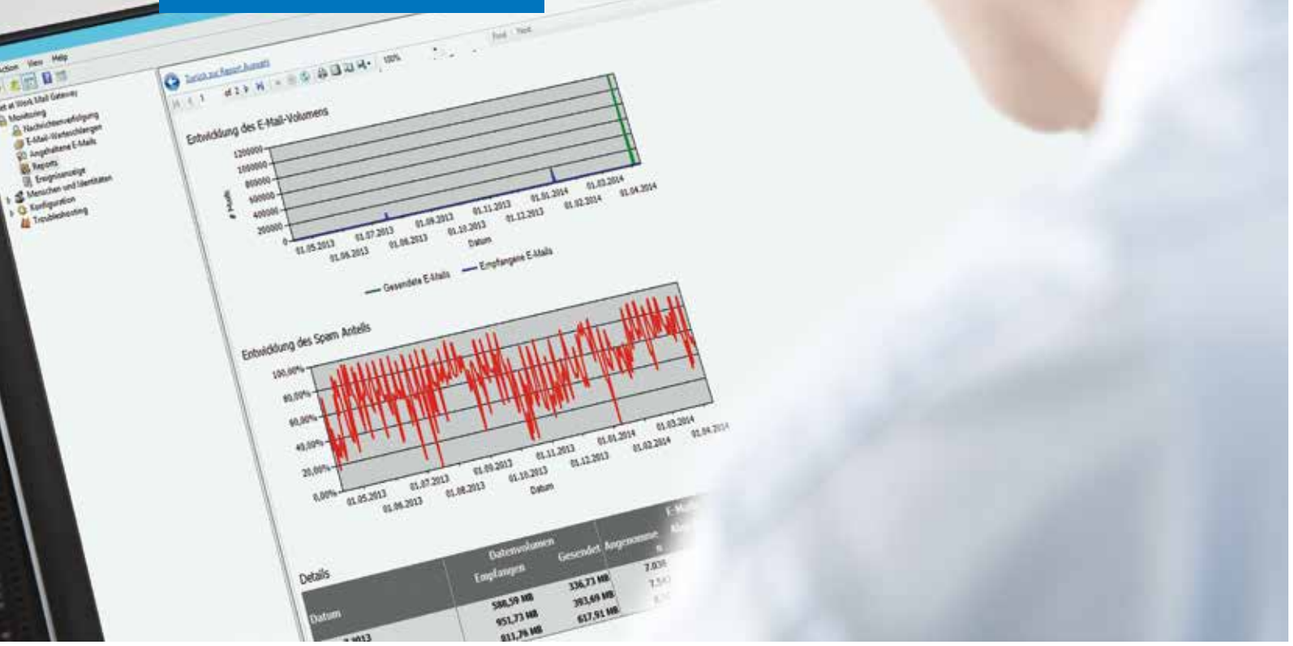
Ein Problem von Anti-Spam-Lösungen ist, dass beim Klassifizieren von E-Mails gelegentlich legitime Nachrichten als Spam eingestuft werden, so genannte „False Positives“. Genau diese False Positives sind es, die bei vielen Lösungen ein Risiko darstellen. Nachteilig wird diese Fehlerkennung dann, wenn solche E-Mails gelöscht oder in Quarantäne abgelegt werden. Die Suche nach der einen falsch klassifizierten E-Mail in Tausenden von Spam-E-Mails gleicht der Suche einer Nadel im Heuhaufen. Besonders gravierend ist die Situation, wenn weder Absender noch Empfänger der E-Mail über den Verbleib in der Quarantäne informiert werden.

False Positives

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. Keine False Positives erreichen Sie tatsächlich nur dann, wenn Sie keinen Filter einsetzen.

NoSpamProxy sichert die Kommunikation und informiert Absender

Natürlich kann auch NoSpamProxy Nachrichten irrtümlich als Spam erkennen. Aber im Gegensatz zu anderen Lösungen verweigert NoSpamProxy bereits die Annahme dieser E-Mail. Der Absender erhält eine Unzustellbarkeitsnachricht und kann darauf reagieren. Der Absender einer legitimen E-Mail wird also darüber informiert, warum seine E-Mail nicht zugestellt wurde und kann nun über einen anderen Weg den Kontakt herstellen, z.B. durch einen Anruf bei dem Empfänger.



Level of Trust

Eine Schlüsselkomponente von NoSpamProxy ist das Level-of-Trust-System. Dieses System erfasst die Sender und Empfänger und vergibt hierfür Vertrauenspunkte. Sobald eine Nachricht an den Kommunikationspartner versandt wurde, kann dieser problemlos antworten und NoSpamProxy sogar dann passieren, wenn seine E-Mail Spam-Eigenschaften aufweisen sollte.

Level of Trust bietet eine äußerst intelligente, dynamische Whitelist-Funktion. Wird ein Kommunikationspartner irrtümlich als Spammer klassifiziert und damit abgelehnt, genügt eine ausgehende E-Mail an den gesperrten Versender, um ihn zuverlässig freizuschalten. Für Spammer hingegen wird die Empfängeradresse aufgrund des Mehraufwandes uninteressant. Abwesenheitsbenachrichtigungen oder andere automatisch generierte E-Mails werden vom Level-of-Trust-System übrigens als solche erkannt und haben auf die Vertrauenspunkte keinen Einfluss.

Auskunftsfähig durch E-Mail-Archivierung

Bereits am Gateway können E-Mails vollständig archiviert werden. Ein- und ausgehende Nachrichten werden dabei über Konnektoren in Archivsystemen von Drittanbietern oder in ein internes Dateisystem gespeichert und stehen für Auskünfte und als Beweisgrundlage zur Verfügung. Durch die Kopplung mit den Anti-Spam-Funktionen werden nur gewünschte und tatsächlich angenommene Nachrichten archiviert.

Sicher für große Datenmengen

Mit dem Large File Transfer von NoSpamProxy können Benutzer auch größere Datenmengen direkt aus Outlook heraus. Dazu steht ein Web Portal im unternehmenseigenen System bereit. So lassen sich mit einem Klick auch Dateien verschicken, die aufgrund von Größenbeschränkungen bislang abgelehnt wurden. Die E-Mail-Systeme von Sendern und Empfängern werden nicht belastet. Darüber hinaus erfolgt der Versand mit sicherer SSL-Verschlüsselung.

Immer im Blick

Mit der Reporting-Funktion von NoSpamProxy lassen sich sowohl das Datenvolumen als auch das E-Mail- und Spam-Aufkommen detailliert bis auf die 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 Ereignisprotokoll von NoSpamProxy haben Administratoren alle Meldungen jederzeit im Blick.

noSpamproxy®

Das Echtzeit-Schild vor Ihrem Netzwerk

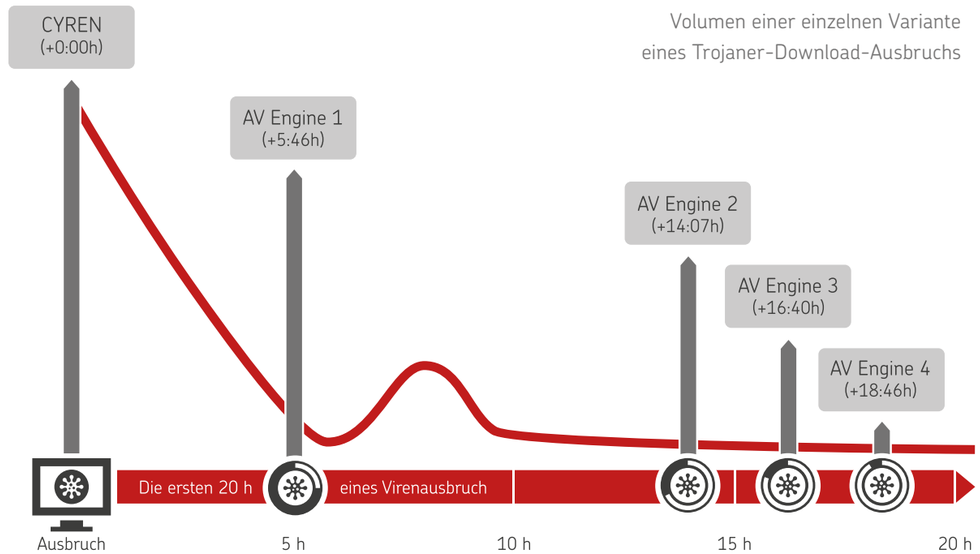
Spam und Malware gehen immer öfter Hand in Hand: Cyberkriminelle nutzen Spam, um Malware zu verbreiten und um fremde Rechner in Spam-Bots zu verwandeln. Um auch solche kombinierten Bedrohungen abzuwehren, enthält NoSpamProxy den prämierten Antivirenschutz von CYREN. Die CYREN-Antiviruslösung basiert auf dem proaktiven Scannen des Internets und der frühzeitigen Identifikation von Virusausbrüchen. Im Gegensatz zu signaturbasierten Verfahren erkennt diese Lösung Viren bereits, sobald sie auftreten, und kann so das Netzwerk unmittelbar schützen.

Die richtige Kombination macht den Unterschied

NoSpamProxy integriert die vielfach ausgezeichnete Antivirus-Komponente von CYREN. Sie bietet eine höchsteffiziente Erkennung bei geringem Ressourcenbedarf und blockt jede Art von Malware wie Würmer, Trojaner und Spyware ab. Die einzigartige Kombination von signaturbasierten Verfahren und Mustererkennung ermöglicht die extrem hohe Erkennungsrate sowohl von bekannten wie auch unbekannten Schädlingen.

Mehrwert durch Verschlüsselung

Um die geschäftliche E-Mail-Kommunikation noch besser zu schützen, ist auch die E-Mail-Verschlüsselung unverzichtbar. Hier kann NoSpamProxy mit der Security-Lösung enQsig erweitert werden. Das Gateway für sichere E-Mail-Verschlüsselung ergänzt den umfassenden Schutz von NoSpamProxy und bietet höchste Vertraulichkeit für die E-Mail-Kommunikation.



Volumen einer einzelnen Variante eines Trojaner-Download-Ausbruchs

Systemvoraussetzungen: Windows Server 2003 SP2 oder höher • .NET Framework 4.5.1 oder höher für Windows 2008, Framework 4.0 auf Windows 2003, Microsoft SQL Server 2005 oder höher, SQL Express Edition 2005 oder höher • SMTP zum internen Mailsystem Microsoft Report Viewer 2010 • Internet Explorer 8 oder höher

Version 9.0

Net at Work GmbH
Am Hoppenhof 32 A
33104 Paderborn
GERMANY

T +49 5251 304-600
F +49 5251 304-650
info@netatwork.de
www.netatwork.de