HEIDELBERG iT Management

noSpam proxy®

Komfortable Sicherheit für die gesamte E-Mail Kommunikation

Protection 

Encryption 

Large Files 

Disclaimer 

”NoSpamProxy® hat unsere internen Security-Experten so nachhaltig überzeugt, dass wir die Mail-Security-Suite nun auch in unser Portfolio aufgenommen haben. Wir freuen uns, dieses exzellente Produkt nun im ALSO B2B Marketplace unseren Kunden und Partnern anbieten zu können.

Mike Rakowski,
Leiter Business Unit Technology
bei ALSO Deutschland

”Wir kennen viele Produkte aus unseren Research-Aktivitäten. NoSpamProxy® hat uns durch Leistung und Bedienbarkeit wie kein anderes Produkt überzeugt. Allen Unternehmen, die auf Office 365 umsteigen, kann ich NoSpamProxy® als Ergänzung für Mail-Security empfehlen.

Oleg Ludwig,
IT Manager bei techconsult

HEIDELBERG iT Management

Die Heidelberg iT Management GmbH & Co. KG ist ein führender IT-Dienstleister in der Metropolregion Rhein-Neckar und vereint als Internet-Service-Provider, Rechenzentrumsbetreiber und IT-Systemhaus alle Kernkompetenzen der Informations- und Telekommunikationstechnik unter einem Dach. Als Spezialist für IT-Outsourcing, Cloud-Services und IT-Sicherheit erbringt Heidelberg iT für Unternehmenskunden alle IT-Beratungs- und IT-Serviceleistungen rund um Infrastruktur, Netzwerk und Internet aus einer Hand, einschließlich Geschäftstelefonie und Beschaffung von Hard- und Software. Professionelle Glasfaser-Dienstleistungen, LWL-Produkte und ein Glasfaser-Notdienst ergänzen das Repertoire des IT-Infrastrukturdienstleisters.

noSpamproxy®

nospamproxy.de

PROTECTION.

Gute Nachrichten für Ihren Mailserver.

82 Prozent aller Cyberangriffe erfolgen per E-Mail*

Cyberattacken gehören für Unternehmen auf der ganzen Welt mittlerweile zum Alltag. Die Folgen eines solchen Angriffs können Ihr Geschäft im Extremfall komplett lahmlegen - von Schadensersatzforderungen betroffener Kunden bis hin zum Imageschaden. Die klassische E-Mail ist dabei immer noch Haupteinfallstor für Cyberangriffe. Grund genug, diese Schwachstelle besonders gut zu sichern.

NoSpamProxy® Protection nimmt problematische E-Mails gar nicht erst an

Um einen vollständigen Schutz vor Spam, Ransomware, Spyware und Malware zu ermöglichen, scannt NoSpamProxy Protection jede Mail bereits beim Empfang als erstes SMTP-Gateway und klassifiziert sie anhand unterschiedlicher Anti-Spam-Filter. Wird eine E-Mail als Spam oder potenziell gefährlich eingestuft, nimmt das System die E-Mail nicht an. Nur als vertrauenswürdig eingestufte Nachrichten können das Gateway passieren. Die Besonderheit: Wenn eine vertrauenswürdige E-Mail nicht angenommen wird, stellt NoSpamProxy Protection sicher, dass der Absender über die verhinderte Zustellung informiert wird. Damit ist NoSpamProxy eines der wenigen Produkte auf dem Markt, die volle Konformität mit dem anspruchsvollen deutschen Recht gewährleisten (insbesondere gemäß §206 StGB, §88 Telekommunikationsgesetz).

NoSpamProxy Protection macht gefährliche Inhalte unschädlich

E-Mail-Anhänge im Word-, Excel- oder PDF-Format können regelbasiert in ungefährliche PDF-Dateien umgewandelt bzw. entschärft werden, so dass dem Empfänger ein garantiert ungefährlicher Anhang zugestellt wird. Der „Klick aus Neugier" wird entschärft.

NoSpamProxy Protection nimmt Absender genau unter die Lupe

Mit der automatisierten Absenderidentifikation kann NoSpamProxy eindeutig feststellen, ob eine E-Mail tatsächlich vom angegebenen Absender stammt. Dabei nutzt NoSpamProxy die Methoden der Absenderreputation, also SPF, DKIM und DMARC. Um gezielt vor Phishing- und CEO-Fraud-Angriffen zu schützen, wird zudem eine umfangreiche Prüfung des Header-FROM - der Kopfzeile einer E-Mail - durchgeführt. So wird beispielsweise verhindert, dass sich Angreifer in E-Mails als Ihr Chef oder Kollege ausgeben können.

NoSpamProxy Protection lernt, mit wem Sie kommunizieren

Mit Hilfe der Level-of-Trust-Technologie lernt NoSpamProxy ständig, mit wem Sie oder Mitarbeiter Ihres Unternehmens kommunizieren. Dabei werden anhand vieler Merkmale Vertrauenspunkte vergeben, die mehr sind als eine dynamische Whitelist. NoSpamProxy Protection scannt auch ausgehende Mails und vergibt Vertrauenspunkte für die Empfänger dieser E-Mails. So werden gewünschte Kommunikationsbeziehungen erlernt und Ihr System wächst intelligent mit.

Die Quarantäne-Falle herkömmlicher Anti-Spam-Lösungen

Das Problem aller Spamschutz-Lösungen ist, dass eine Software entscheidet, ob eine E-Mail als Spam klassifiziert wird oder nicht. Dabei werden häufig nicht alle Spam-E-Mails erkannt - und in einigen Fällen auch unbedenkliche E-Mails blockiert. Genau diese False Positives stellen bei herkömmlichen Anti-Spam-Lösungen ein Risiko dar. Wenn solche Nachrichten gelöscht oder in Quarantäne gelegt werden, können diese eigentlich erwünschten E-Mails verloren gehen.

Virus Bulletin bestätigt 0% False-Positive-Rate von NoSpamProxy

„Mit 99,69 von 100 möglichen Punkten erzielt NoSpamProxy ein Traumergebnis und erhält das Prädikat VB Spam+ Gold der renommierten Zertifizierungsstelle für IT-Security, Virus Bulletin. NoSpamProxy hat mit einer Erkennungsrate von 99,69% im Anti-Spam-Test von Virus Bulletin ein exzellentes Ergebnis erreicht. Dazu konnte es mit 0,00% False Positives punkten. Außerdem brilliert NoSpamProxy nicht nur bei der Spam-Abwehr, sondern bietet auch Leading-Edge-Schutz vor Malware und Ransomware, um den wir die aktuellste Version unseres Tests erweitert haben.

Martijn Grooten,
Chefredakteur Virus Bulletin

SecurITy made in Germany

Trust Seal
www.teletrust.de/itsmig

*Studie des BSI vom April 2016

noSpamproxy®

nospamproxy.de

Anbindung mehrerer AV-Engines über ICAP-Standard

NoSpamProxy® unterstützt den ICAP-Standard und ermöglicht damit die Anbindung mehrerer AV-Engines im Parallelbetrieb. AVIRA ist als NoSpamProxy-Option als Virtuelle Appliance verfügbar.

Transparenter Spamschutz ständig im Blick

Mit den Reporting-Funktionen von NoSpamProxy Protection haben Sie Ihren E-Mail-Verkehr immer unter Kontrolle. So lassen sich das Datenvolumen und das E-Mail- und Spam-Aufkommen detailliert bis auf die Benutzerebene analysieren. Die integrierte Nachrichtenverfolgung protokolliert jede E-Mail und wie sie weiterverarbeitet wurde. Welche Regeln waren aktiv? Welche Anti-Spam-Filter am Mail-Gateway haben Einfluss genommen und welche Aktionen wurden für die E-Mail ausgeführt? Administratoren haben mit den Protokollen und Berichten von NoSpamProxy Protection alle Meldungen ständig im Blick und können Rückfragen einfach und ohne langes Suchen beantworten.

Optionaler Sandbox-Service

Der optionale NoSpamProxy Sandbox-Service steigert die Wahrscheinlichkeit der Erkennung neuer Viren signifikant. Dies ist möglich, weil Dateien nicht nur in einer einzelnen Sandbox, sondern in einem Sandbox-Array überprüft werden.

Perfektes Zusammenspiel mit den Modulen Encryption und Large Files

Wenn Sie NoSpamProxy nicht nur zur zum Schutz vor Spam und Malware nutzen, sondern auch die Funktionen zur E-Mail-Verschlüsselung und zur sicheren Übertragung großer Dateien, gewinnen Sie zusätzliche Sicherheit:

- Die Schwellen zur Ablehnung von Nachrichten mit Spam- und Malware-Verdacht können erhöht werden, wenn die reguläre Kommunikation mit Geschäftspartnern verschlüsselt und signiert abgewickelt wird.
- Die Spam- und Malwareprüfung kann effizient am gleichen Gateway nach der Entschlüsselung von Mails durchgeführt werden, während beim Einsatz anderer Lösungen ein Re-Routing mit Zeit- und Performanceverlusten erforderlich ist.
- Für das intelligente Anhangsmanagement, Content Disarm und das Large-Files-Modul wird das selbe Webportal genutzt. Entsprechend flexibel sind die Möglichkeiten, die Behandlung von großen Dateien und unterschiedlichen Dateitypen zu konfigurieren.
- Auch Large Files nutzt die Level-of-Trust-Technologie: Entscheiden Sie ganz einfach, ob Anhänge von bekannten Kommunikationspartnern den Empfänger direkt erreichen und nur Anhänge von Unbekannten in die Anhangsquarantäne kommen.
- Weitere Vorteile durch Abstimmung der Funktionalitäten der NoSpamProxy-Module aufeinander.

Das bietet Ihnen nur NoSpamProxy:

noSpamproxy® vb VERIFIED SPAM + virusbtn.com

Microsoft Azure Certified

Office 365

SecurITy made in Germany
Trust Seal www.teletrust.de/itsmig

Viren-Schutz in Echtzeit mit Anti-Spam und Anti-Malware Zero Hour Technologie

NoSpamProxy Protection integriert die Zero-Hour-Technologie unseres Technologiepartners Cyren. Dazu untersucht die patentierte Technologie große Teile des globalen Internetverkehrs in Echtzeit und analysiert bis zu 100 Milliarden Nachrichten pro Tag, von denen bis zu 88 Milliarden spam- und virenverseucht sind. Die Lösung scannt das Internet proaktiv und identifiziert potenzielle Virusausbrüche besonders schnell. Im Gegensatz zu signaturbasierten Verfahren erkennt diese Lösung den Ausbruch neuer Viren bereits während des Auftretens. Ihr Exchange-Server sowie Ihre gesamte E-Mail-Infrastruktur werden innerhalb der ersten Sekunden geschützt.

techconsult PUR 2019 Professional User Rating ★ CHAMPION ★ E-Mail Security Security Solutions

> Der Level-of-Trust-Filter ist eine ausgezeichnete Idee. Er stoppt sehr zuverlässig bekannte Spammer und stellt sicher, dass E-Mails unserer regelmäßigen Korrespondenzpartner garantiert zugestellt werden.
>
> Jürgen Lalla,
> IT Leiter Swiss Life Select

SwissLife Select

Alle Highlights auf einen Blick:

- ✓ Keine Quarantäne
- ✓ Entlastung der Administratoren
- ✓ Innovatives Level of Trust
- ✓ Content Disarm and Reconstruction
- ✓ Prüfung der Absenderreputation
- ✓ Cyren Anti-Spam und Anti-Virus Engine
- ✓ Optionaler Sandbox-Service

ENCRYPTION.

Der Schlüssel zur sicheren E-Mail-Kommunikation.

Ohne E-Mail-Verschlüsselung kein zeitgemäßer Datenschutz!

E-Mail-Verschlüsselung - nicht so wichtig? Diese Einstellung hat sich deutlich geändert, wie in vielen aktuellen Umfragen sichtbar wird. Auch der Gesetzgeber fordert mit der Datenschutz-Grundverordnung (DSGVO) den Stand der Technik zum Schutz von personenbezogenen Daten ein – und damit auch, dass die Übertragung dieser Daten verschlüsselt erfolgen muss.

Vertraulichkeit schnell und einfach erreichen

Durch zentrale E-Mail-Signatur und E-Mail-Verschlüsselung am NoSpamProxy® Encryption Gateway kommunizieren Sie mit Partnern besonders sicher und einfach. Da Schlüssel und Zertifikate nur auf dem Gateway und nicht auf den Clients verwaltet werden, entfällt für Anwender der umständliche Umgang mit elektronischen Schlüsseln – und die privaten Schlüssel sind bestmöglich vor Angriffen geschützt. Die Sicherheitsregeln im Sinne der Corporate Governance des Unternehmens werden automatisch zentral umgesetzt. Natürlich werden auch empfangene Nachrichten bereits am Gateway entschlüsselt und stehen dem Anwender wie gewohnt für die Weiterverarbeitung zur Verfügung. Dies ermöglicht den Zugriff über TLS-verschlüsselte Verbindungen mit Smartphones und Tablets, sowie die Archivierung der E-Mails in unverschlüsselter Form.

S/MIME-Signatur und Verschlüsselung

S/MIME ist der empfohlene und international vereinbarte Standard zur elektronischen Signatur und Verschlüsselung von E-Mails. Dabei handelt es sich um ein asymmetrisches Verschlüsselungsverfahren mit öffentlichen und privaten Schlüsseln. Um S/MIME nutzen zu können, müssen Sender und Empfänger über ein Zertifikat verfügen. NoSpamProxy bietet dabei die volle Unterstützung der jeweils neuesten im Standard veröffentlichten Verschlüsselungsverfahren. Ältere Verfahren werden zur Wahrung der Kompatibilität ebenso unterstützt.

PGP Mail: Pretty Good Privacy

Natürlich können mit dem Encryption-Modul auch PGP-Schlüssel generiert, importiert und verwaltet werden. Mit der Unterstützung von PGP-Verschlüsselung bietet NoSpamProxy Encryption eine weitere Möglichkeit zum bequemen Austausch von verschlüsselten Daten und Nachrichten.

PDF Mail: auch ohne Zertifikat oder Schlüssel sicher versenden

Für den häufigen Fall, dass Empfänger keinen PGP-Schlüssel oder kein persönliches Zertifikat haben, bietet NoSpamProxy Encryption mit der PDF-Mail-Funktion einen zusätzlichen Weg für den sicheren Versand von E-Mails und Dokumenten, der keine Anforderungen an den Empfänger stellt. Dazu wandelt NoSpamProxy Encryption die E-Mail mit allen Anhängen automatisch in ein passwortgeschütztes PDF-Dokument um. Das Passwort wird dem Empfänger automatisch per SMS zugesandt. Alternativ kann der Empfänger über die Anmeldung im NoSpamProxy-Webportal ein eigenes Passwort vergeben. Zum Öffnen des Dokuments braucht er dann lediglich einen PDF-Reader.

E-Mail-Verschlüsselung und Zertifikate

Im Rahmen der sicheren Verschlüsselung von E-Mails sind Zertifikate erforderlich, die für das S/MIME-Verfahren nach dem X.509-Standard oder mit einem PGP-Schlüssel genutzt werden können. NoSpamProxy Encryption zentralisiert und automatisiert die Verwaltung und den Erwerb dieser Zertifikate. IT-Administratoren profitieren von einer Vielzahl hilfreicher Managementfunktionen.

Weitere Funktionen von NoSpamProxy Encryption sind die Anbindung an

- DOI (für die Kommunikation zwischen Behörden, die an DOI angeschlossen sind)
- De-Mail (für die Kommunikation per De-Mail mit De-Mail Teilnehmern)

De-Mail

Im Rahmen der sicheren Verschlüsselung von E-Mails können Sie NoSpamProxy auch an eine De-Mail-Domain anschließen und De-Mails über die normalen Mail-Clients der Anwender versenden und empfangen.

SecurITy made in Germany

Trust Seal
www.teletrust.de/itsmig

Open Keys – kostenfreier Suchdienst für öffentliche Schlüssel

Mit unserem kostenfreien Dienst Open Keys können Sie einfach und schnell prüfen, ob Ihre Kommunikationspartner Zertifikate besitzen und ohne vorherigen Austausch signierter Mails sofort verschlüsselt kommunizieren. Ebenso können Sie Ihren öffentlichen Schlüssel und die Ihrer Organisation auf Open Keys veröffentlichen. Auch Nicht-NoSpamProxy®-Kunden können den Dienst nutzen und über LDAP oder Web-API automatisiert unter www.openkeys.de öffentliche Schlüssel suchen.

Open Keys

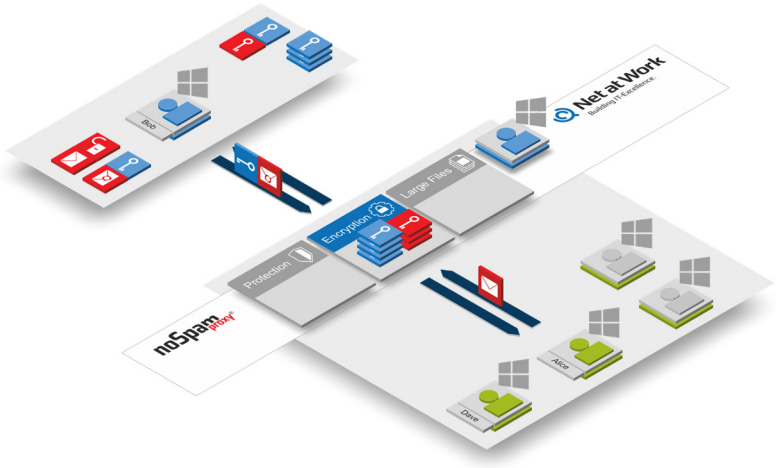
All inclusive

Viele Anbieter bieten Zusatzdienste, Sonderfunktionen oder Schnittstellen zur Anbindung an andere Verfahren nur als kostenpflichtige Zusatzoptionen an. Bei NoSpamProxy Encryption sind Schnittstellen zu führenden Trust-Centern, De-Mail, NdB (ehemals DOI) und EDI@Energy inklusive. Und natürlich fallen keine zusätzlichen Kosten an, die von der Zahl der ausgetauschten EDI-Nachrichten abhängig sind.

Perfektes Zusammenspiel mit den Modulen Protection und Large Files

Wenn Sie NoSpamProxy nicht nur zur Verschlüsselung nutzen, sondern auch die Funktionen zum Schutz vor Spam und Malware und zur sicheren Übertragung großer Dateien, gewinnen Sie zusätzliche Sicherheit:

- Die Schwellen zur Ablehnung von Nachrichten mit Spam- und Malware-Verdacht können erhöht werden, wenn die reguläre Kommunikation mit Geschäftspartnern verschlüsselt und signiert abgewickelt wird.
- Die Spam- und Malwareprüfung kann effizient am gleichen Gateway nach der Entschlüsselung von Mails durchgeführt werden, während beim Einsatz anderer Lösungen ein Re-Routing mit Zeit- und Performanceverlusten erforderlich ist.
- Große Dateianhänge nicht mit der Mail inhaltsverschlüsselt zu übertragen, sondern über einen sicheren Up- und Download, steigert die Performance und minimiert Zeitverzögerungen.
- Weitere Vorteile durch Abstimmung der Funktionalitäten der NoSpamProxy-Module aufeinander.



Intelligentes TLS-Management mit NoSpamProxy

Die sichere Übertragung von E-Mails zwischen zwei E-Mail-Servern mittels TLS (Transportverschlüsselung) sollte mittlerweile selbstverständlich sein. Dennoch kommt es immer noch vor, dass Server dieses wichtige Merkmal nicht oder nur teilweise unterstützen. NoSpamProxy bietet TLS-Sicherheit mit einem einzigen Mausklick. Die Absicherung des E-Mail-Empfangs erledigt der Administrator in den Empfangskonnektoren von NoSpamProxy. Dort kann die Verbindungssicherheit optional erlaubt werden. Das bedeutet, dass NoSpamProxy dem einliefernden Server das StartTLS-Verfahren anbietet. Der einliefernde Server kann dann selbst entscheiden, ob er verschlüsseln möchte oder nicht.

> Mit NoSpamProxy und GlobalSign konnten wir die Anforderungen der EU-DSGVO an eine datenschutzkonforme E-Mail-Kommunikation einfach umsetzen. Die Kombination der beiden Produkte reduzierte dabei den Aufwand im Roll-Out und in der laufenden Administration auf ein Minimum.
>
> Marcus Bethmann,
> IT-Systemadministrator Groupware & Identity Services bei der WWK Versicherungsgruppe

WWK
Eine starke Gemeinschaft

LARGE FILES.

Große Dateien einfach und sicher per E-Mail versenden.

Entlastet E-Mail-Server und Administratoren

NoSpamProxy® Large Files erlaubt es Ihnen, beliebig große Dateien direkt aus dem E-Mail-Client zu versenden. Anwender können auf diese Weise große Datenmengen, die die Beschränkungen des E-Mail-Clients überschreiten, ohne Medienbruch mit einem einzigen Klick absetzen. Der Einsatz ist unkompliziert und mit dem Versand herkömmlicher Dateianhänge vergleichbar. Im Gegensatz zu den verbreiteten File-Transfer-Diensten werden die Daten hier über einen kundeneigenen Webserver bereitgestellt und SSL-verschlüsselt übertragen. Damit werden die Anforderungen an sicherheitskritische Businessprozesse sowie die IT-Governance erfüllt. Große Dateien per E-Mail verschicken – mit NoSpamProxy Large Files ganz einfach!

Das Problem wächst rasant

Die regelmäßig erscheinenden Reports der Radicati Group zur weltweiten E-Mail-Nutzung zeigen, dass die Durchschnittsgröße der Dateien, die Anwender per E-Mail-Anlage als große Dateien verschicken wollen, von Jahr zu Jahr dramatisch steigt. So werden E-Mail-Infrastrukturen stark belastet und das Verschicken großer Dateien durch Setzen von Limits eingeschränkt oder generell verboten. In Einzelfällen muss dann durch individuelle Anforderung bei einem Administrator das Limit erhöht oder ein FTP-Upload oder -Download genehmigt werden. Gehen Sie diesen Problemen aus dem Weg und setzen Sie auf NoSpamProxy Large Files, wenn Sie große Daten per E-Mail versenden möchten.

Per E-Mail einfach geschickter

NoSpamProxy Large Files steuert automatisch die Uploads von Dateien auf ein unternehmenseigenes Webportal. Die Anlage wird durch einen Link ersetzt, den der Empfänger nur noch anklicken muss. So kann die Anlage dann ganz einfach von einer Website mit TLS-Verschlüsselung heruntergeladen werden. Der Empfänger kann dem Absender auch in gleicher Weise antworten und ebenfalls eine oder mehrere Dateien hochladen. Auf diese Weise können Sie einfach und sicher große Anhänge versenden. Auf der Administrationsoberfläche von NoSpamProxy Large Files lassen sich Einstellungen schnell und einfach vornehmen. Das Interface bietet zusätzlich auch Reporting-Funktionen, um beispielsweise bei Vertriebsaktionen festzustellen, welche Adressaten einer E-Mail-Kampagne die angebotene Datei heruntergeladen haben.

Nutzung des Webportals für externe Empfänger ohne Einladung

Bei NoSpamProxy Large Files ist die Nutzung des Webportals für den externen Kommunikationspartner auch ohne Einladungslink möglich. Dadurch können Unternehmen ihren Partnern eine einfache Möglichkeit anbieten, Informationen über einen geschützten Kanal auszutauschen. Dies schließt auch den Austausch großer Dateien ein.

Mit NoSpamProxy Large Files wird das Versenden großer Anhänge und Datenmengen so einfach wie das Senden einer herkömmlichen E-Mail. NoSpamProxy bietet als einziges Secure Mail Gateway diese Funktion nahtlos integriert mit den E-Mail-Security-Funktionen Verschlüsselung, Anti-Spam und Anti-Malware.

Powerpoint, Audio, Video, Multi-Media, CAD: E-Mail-Anlagen werden immer größer

Wie viel Administrationsaufwand und Kopfzerbrechen hat Ihnen die Outlook-Meldung „Anlagengröße überschreitet das erlaubte Maximum“ schon gemacht? Mit NoSpamProxy Large Files können Sie große Anhänge problemlos per E-Mail versenden!

techconsult PUR 2019 Professional User Rating ★ CHAMPION ★ E-Mail Security Security Solutions

SecurITy made in Germany

Trust Seal www.teletrust.de/itsmig

Anhangssteuerung anhand von Dateimerkmalen

Die flexible Anhangssteuerung erlaubt es Administratoren, die Verarbeitung von E-Mail-Anhängen regelbasiert vorzunehmen. Hierbei kann als Bedingung der Dateityp und/oder die Dateigröße dienen. Beim Versenden großer Anhänge können diese beispielsweise von der E-Mail abgetrennt und über das NoSpamProxy® Web Portal versendet werden. Die Trennung erfolgt dabei entweder auf dem Gateway – oder mit Hilfe des Outlook Add-Ins bereits auf dem Client.

Perfektes Zusammenspiel mit den Modulen Encryption und Protection

Wenn Sie NoSpamProxy nicht nur zur zum Versenden großer Dateien nutzen, sondern auch die Funktionen zur E-Mail-Verschlüsselung und zum Schutz vor Spam und Malware, gewinnen Sie zusätzliche Sicherheit:

- Intelligente Kombination mit NoSpamProxy Protection: Große Anhänge versenden mit NoSpamProxy Large Files ist insbesondere für NoSpamProxy-Kunden sinnvoll, die bereits die CDR-Funktion (Content Disarm and Reconstruction) nutzen, um für mehr Sicherheit beim E-Mail-Empfang zu sorgen. CDR kann beispielsweise eine Word-Datei in eine PDF-Datei umwandeln und dem Empfänger so eine garantiert makrofreie Version des Inhalts zustellen. In Kombination mit NoSpamProxy Large Files kann zusätzlich das Original in Quarantäne gelegt werden.
- Die Schwellen zur Ablehnung von Nachrichten mit Spam- und Malware-Verdacht können erhöht werden, wenn die reguläre Kommunikation mit Geschäftspartnern verschlüsselt und signiert abgewickelt wird.
- Die Spam- und Malwareprüfung kann effizient am gleichen Gateway nach der Entschlüsselung von Mails durchgeführt werden, während beim Einsatz anderer Lösungen ein Re-Routing mit Zeit- und Performanceverlusten erforderlich ist.
- Für das intelligente Anhangsmanagement, Content Disarm und das Large-Files-Modul wird das gleiche Webportal genutzt. Entsprechend flexibel sind die Möglichkeiten, die Behandlung von großen Dateien und unterschiedlichen Dateitypen zu konfigurieren.
- Auch Large Files nutzt die Level-of-Trust-Technologie: Entscheiden Sie ganz einfach, ob Anhänge von bekannten Kommunikationspartnern den Empfänger direkt erreichen und nur Anhänge von Unbekannten in die Anhangsquarantäne kommen.
- Weitere Vorteile durch Abstimmung der Funktionalitäten der NoSpamProxy-Module aufeinander.

Alleinstellungsmerkmale:

- Beliebig große Dateien direkt aus dem E-Mail-Client versenden.
- Hohe Sicherheit durch TLS-Verschlüsselung.
- Vermeidung von Mehrfacharchivierung von Dateien in Outlook-Ordnern und Reduzierung der Backup-Kosten.
- Einfach und schnell ohne Medienbruch wie z.B. bei FTP-Servern oder Cloud-Speicherdiensten.
- Entlastung der vorhandenen E-Mail-Infrastruktur und Bandbreite.
- Konfigurierbare Möglichkeit, mit der E-Mail-Antwort ebenfalls große Anhänge über das gleiche Verfahren zu schicken.
- Nutzung des Webportals für externe Empfänger mit und ohne Einladung.

> „Im Gegensatz zu einem klassischen FTP-Server integriert NoSpamProxy Large Files das Daten-Handling in die vertraute E-Mail-Umgebung unserer Mitarbeiter – und ermöglicht ein hohes Maß an Sicherheit.
>
> Peter Gerfer, IT- Systemtechniker beim Deutschen Ärzte-Verlag

Deutscher Ärzteverlag

DISCLAIMER.

Flexible E-Mail-Signaturen.

NoSpamProxy bietet mehr als E-Mail-Sicherheit

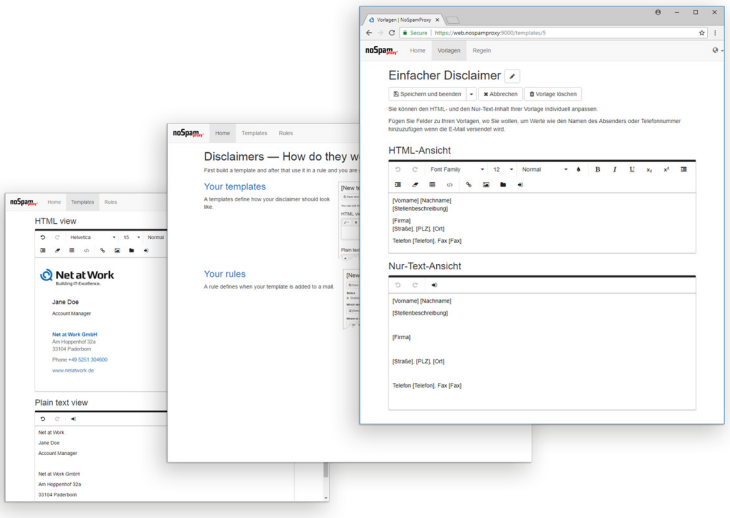
Einheitliche und aktuelle E-Mail-Signaturen sind ein Dauerbrenner in den IT-Abteilungen. Ihre Umsetzung bindet allerdings immer noch unnötig Ressourcen oder muss über Nischenwerkzeuge realisiert werden, die als Erweiterung des jeweiligen Mailservers gepflegt werden müssen. Über das Secure-E-Mail-Gateway NoSpamProxy® lässt sich diese Anforderung elegant und ohne zusätzliche Software lösen.

E-Mail-Disclaimer als Marketing-Instrument nutzen

Häufig scheitert die Anpassung von Disclaimern daran, dass deren Umsetzung nur durch die IT-Abteilung erfolgt - die die Anforderungen des Marketing oft nicht schnell genug umsetzen kann. So werden in vielen Fällen Gelegenheiten verpasst, um beispielsweise auf Events, Produktneuheiten oder Promotions hinzuweisen. Die Disclaimer-Option von NoSpamProxy umfasst ein Web-Interface, über das Berechtigte aus der Marketing-Abteilung nach kurzer Einweisung die Disclaimer eigenständig verwalten, gestalten und ändern können. Über die Auswahl von Attributen aus Active-Directory-Gruppen ist es möglich, unterschiedliche Disclaimer-Texte für unterschiedliche Personengruppen oder Abteilungen zu pflegen. So wird die IT-Administration wirksam entlastet und das Unternehmen kann das große Werbepotenzial von Produkt- oder Veranstaltungshinweisen in E-Mail-Disclaimern nutzen.

Weniger Administrationsaufwand - IT-Administration entlasten

Mit NoSpamProxy Disclaimer hat der Kampf zwischen Marketing und IT um schnelle Umsetzung dieses wichtigen, kostengünstigen und wirksamen Marketinginstruments ein Ende. Der größte Nutzen für Unternehmen liegt dabei in der Entlastung der IT-Administration von der Umsetzung der Marketingideen für Disclaimer. Die so gewonnene Zeit kann zur Umsetzung anderer wichtiger Projekte genutzt werden und steigert damit die Agilität der IT und des gesamten Unternehmens.



Mit der Disclaimer-Option lässt sich das auf E-Mail-Security fokussierte NoSpamProxy-Gateway um eine häufig nachgefragte Funktion erweitern. NoSpamProxy-Kunden ersparen sich damit die Installation eines weiteren Softwareprodukts auf dem Exchange-Server.

Unabhängig von Exchange-Server-Versionen

Nachteil vieler direkt auf dem E-Mail-Server bzw. Exchange-Server installierter Disclaimer-Lösungen ist, dass diese bei einer Exchange-Migration aktualisiert werden müssen. Dies bedeutet einen Neukauf, Neuinstallation und Neukonfiguration.
Da NoSpamProxy Disclaimer unabhängig vom eingesetzten E-Mail-Server als eigenständiges Gateway läuft, fällt bei einer Migration grundsätzlich kein oder nur deutlich geringerer Aufwand an.

SecurITy made in Germany

Trust Seal
www.teletrust.de/itsmig

Mehr Rechtssicherheit - Unternehmensrichtlinien unterstützen

In vielen Unternehmen wird die Disclaimer-Funktion des E-Mail-Clients oder E-Mail-Servers genutzt, also beispielsweise Microsoft Outlook oder Microsoft Exchange. Dabei bleibt es den Nutzern überlassen, von der Unternehmenskommunikation oder dem Marketing vorgegebene Texte sowie die grafische Gestaltung korrekt umzusetzen. Häufig werden diese dann eigenmächtig abgeändert, so dass Unternehmen nach außen nicht mit einheitlicher Corporate Identity auftreten. Noch schwerwiegender ist es jedoch, wenn beispielsweise Klauseln zum Haftungsausschluss nicht übernommen werden - was zu Schadensersatzansprüchen Dritter führen kann.

Perfektes Zusammenspiel mit den Modulen Encryption, Protection und Large Files

Wenn Sie NoSpamProxy® nicht nur zur zum Erstellen von E-Mail -Signaturen verwenden, sondern auch die Funktionen zur sicheren Übertragung großer Dateien, zur E-Mail-Verschlüsselung und zum Schutz vor Spam und Malware nutzen, gewinnen Sie zusätzliche Sicherheit:

- Wie zur Steuerung der Disclaimer-Funktion werden auch die Module Protection, Encryption und Large Files über Active Directory umfassend gesteuert. Dadurch ergeben sich deutlich verringerte Pflegeaufwände für die einzelnen Module und Vereinfachungen für den Administrator.
- Intelligente Kombination mit NoSpamProxy Protection: Große Anhänge versenden mit NoSpamProxy Large Files ist insbesondere für NoSpamProxy-Kunden sinnvoll, die bereits die CDR-Funktion (Content Disarm and Reconstruction) nutzen, um für mehr Sicherheit beim E-Mail-Empfang zu sorgen. CDR kann beispielsweise eine Word-Datei in ein PDF umwandeln und dem Empfänger so eine garantiert makrofreie Version des Inhalts zustellen. In Kombination mit NoSpamProxy Large Files kann zusätzlich das Original in Quarantäne gelegt werden.
- Die Schwellen zur Ablehnung von Nachrichten mit Spam- und Malware-Verdacht können erhöht werden, wenn die reguläre Kommunikation mit Geschäftspartnern verschlüsselt und signiert abgewickelt wird.
- Die Spam- und Malwareprüfung kann effizient am gleichen Gateway nach der Entschlüsselung von Mails durchgeführt werden, während beim Einsatz anderer Lösungen ein Re-Routing mit Zeit- und Performanceverlusten erforderlich ist.
- Für das intelligente Anhangsmanagement, Content Disarm und das Large-Files-Modul wird das gleiche Web-Portal genutzt. Entsprechend flexibel sind die Möglichkeiten, die Behandlung von großen Dateien und unterschiedlichen Dateitypen zu konfigurieren.
- Auch Large Files nutzt die Level-of-Trust-Technologie: Entscheiden Sie ganz einfach, ob Anhänge von bekannten Kommunikationspartnern den Empfänger direkt erreichen und nur Anhänge von Unbekannten in die Anhangsquarantäne kommen.
- Weitere Vorteile durch Abstimmung der Funktionalitäten der NoSpamProxy-Module aufeinander.

Einfaches Web-Interface

Die Disclaimer-Option von NoSpamProxy umfasst ein Web-Interface, über das berechtigte Mitarbeiter aus der Marketing-Abteilung alle E-Mail-Disclaimer eigenständig verwalten, gestalten und ändern können.

Vorlagen

Nutzen Sie eine Vielzahl von Vorlagen und erstellen Sie schnell und einfach E-Mail-Disclaimer und -Signaturen

Gruppenspezifisch und individuell

Erstellen Sie Ihre individuellen Disclaimer und E-Mail-Signaturen für Abteilungen, Kampagnen, Messen etc.

Einfache Regeln

Legen Sie hier die Bedingungen für das Versenden von Disclaimern fest.
Wer – Wann – Was.

noSpam proxy®

Die 1995 gegründete Net at Work GmbH ist Softwarehaus und Systemintegrator mit Sitz in Paderborn. Gründer und Gesellschafter des Unternehmens sind Geschäftsführer Uwe Ulbrich sowie Frank Carius, der mit www.msxfaq.de eine der renommiertesten Websites zu den Themen Exchange und Skype for Business betreibt. Als Softwarehaus entwickelt und vermarktet Net at Work mit NoSpamProxy® eine integrierte Gateway-Lösung für Secure E-Mail. NoSpamProxy® bietet sichere Anti-Malware- und Anti-Spam-Funktionen, eine automatisierte E-Mail-Verschlüsselung sowie einen praxistauglichen Large File Transfer auf einer technischen Plattform. So garantiert der modulare Ansatz von NoSpamProxy® eine vertrauliche und rechtssichere E-Mail-Kommunikation. Die Experton Group sieht NoSpamProxy® als Product Challenger für E-Mail und Web-Kollaboration. Zu den mehr als 2.000 Unternehmen, die die Sicherheit ihrer Mail-Kommunikation NoSpamProxy® anvertrauen, gehören u. a. DaimlerBKK, Deutscher Ärzte-Verlag, Hochland, Komatsu Mining, das Kommunale RZ Minden-Ravensberg/Lippe und SwissLife.

Weitere Informationen zur E-Mail Security Suite NoSpamProxy® finden Sie unter
www.nospamproxy.de

Ihr IT-Partner vor Ort:

HEIDELBERG iT Management

Ihr Ansprechpartner für NoSpamProxy bei Heidelberg iT Management & Co. KG

MATTHIAS KOLB
Vordenker / IT-Sicherheit

HEIDELBERG iT
MANAGEMENT GMBH & CO. KG
Kurpfalzring 110 | 69123 Heidelberg
Fon +49 6221 407-578
m.kolb@heidelberg-it.de
www.heidelberg-it.de