Anlagen und Erklärungen

Was ist SPAM?

Als Spam oder Junk (englisch für ‚Abfall' oder ‚Plunder') werden unerwünschte, in der Regel auf elektronischem Weg übertragene Nachrichten bezeichnet, die dem Empfänger unverlangt zugestellt werden und häufig werbenden Inhalt haben. Dieser Vorgang wird Spamming oder Spammen genannt, der Verursacher ist der sogenannte Spammer.

Spam verursacht im System der weltweiten Kommunikation erheblichen Schaden. Dieser ist vor allem auf die zusätzliche Datenmenge und den Aufwand der damit verbundenen Bearbeitung zurückzuführen.

- Das Aussortieren und Lesen von Spam kostet Arbeitszeit.
- Spamfilter sind in der Regel für gewerbliche Zecke kostenpflichtig.
- Spamfilter müssen beschafft und gewartet werden.
- Die Bearbeitung der Mails kann zu einem Ausfall oder zu einer Verlangsamung des erwünschten Mailverkehrs führen. Die Kompensation der Belastung erzeugt wiederum Kosten für neue leistungsfähigere Hardware.

Warum ist eine frühe SPAM-Abwehr so wichtig?

Gelangt eine E-Mail in den Verfügungsbereich des Unternehmens, unterliegt das Unternehmen bestimmten gesetzlichen Vorschriften.

Wird Spam selbst gefiltert, laufen Unternehmen Gefahr, mit dem Strafgesetzbuch aneinanderzugeraten. Ihnen könnte unter Umständen "Unterdrückung von E-Mails" oder "Datenveränderung oder -unterdrückung" vorgeworfen werden. Der Landesbeauftragte für den Datenschutz Sachsen-Anhalt hat nun einen Vorschlag gemacht, wie man diese Klippen sicher umschifft.

Gelangt eine E-Mail erst gar nicht in den Verfügungsbereich des Empfängers, können Spam-Filter rechtlich sauber eingesetzt werden

Der Landesbeauftragte für den Datenschutz in Sachsen-Anhalt hat in seinem Tätigkeitsbericht 2007-2009 ein Vorgehen vorgeschlagen, um nicht in Konflikt mit § 206 Abs. 2 Nr. 2 StGB (Unterdrückung von E-Mails) oder § 303a Abs. 2 StGB (Datenveränderung oder -unterdrückung) zu geraten:

Umschlags- und Inhalts-Daten ankommender E-Mails werden bereits überprüft, noch bevor die E-Mail vollständig übertragen wurde, also noch bevor sie in den Verfügungsbereich des Empfängers gelangt.

Wird ein Spam-Verdacht z.B. mittels Black-List erkannt, wird der E-Mail-Empfang einfach ohne Empfangsbestätigung oder mit Fehlermeldung abgebrochen, so dass der „einliefernde Server" von einer fehlerhaften Übertragung ausgehen muss.

Damit ist die E-Mail nicht in den Verfügungsbereich des Empfängers gelangt. Rechtliche Probleme durch den dann folgenden Einsatz von Antivirensoftware oder auch SPAM-Filtern können ausgeschlossen werden, ohne dass die Adressaten im Bereich des Empfängers vorab um Erlaubnis zur inhaltlichen Prüfung gefragt werden müssten.

(Quelle: http://www.datenschutz-praxis.de/fachwissen/fachnews/spam-erkennung-bei-201eumschlagprufung201c/)

§ 206 Verletzung des Post- oder Fernmeldegeheimnisses

(1) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Unternehmens bekanntgeworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer als Inhaber oder Beschäftigter eines in Absatz 1 bezeichneten Unternehmens unbefugt
1.
eine Sendung, die einem solchen Unternehmen zur Übermittlung anvertraut worden und verschlossen ist, öffnet oder sich von ihrem Inhalt ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft,
2.
eine einem solchen Unternehmen zur Übermittlung anvertraute Sendung unterdrückt oder
3.
eine der in Absatz 1 oder in Nummer 1 oder 2 bezeichneten Handlungen gestattet oder fördert.

(3) Die Absätze 1 und 2 gelten auch für Personen, die
1.
Aufgaben der Aufsicht über ein in Absatz 1 bezeichnetes Unternehmen wahrnehmen,
2.
von einem solchen Unternehmen oder mit dessen Ermächtigung mit dem Erbringen von Post- oder Telekommunikationsdiensten betraut sind oder
3.
mit der Herstellung einer dem Betrieb eines solchen Unternehmens dienenden Anlage oder mit Arbeiten daran betraut sind.

(4) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die ihm als außerhalb des Post- oder Telekommunikationsbereichs tätigem Amtsträger auf Grund eines befugten oder unbefugten Eingriffs in das Post- oder Fernmeldegeheimnis bekanntgeworden sind, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(5) Dem Postgeheimnis unterliegen die näheren Umstände des Postverkehrs bestimmter Personen sowie der Inhalt von Postsendungen. Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

§ 303a Datenveränderung

(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
(2) Der Versuch ist strafbar.
(3) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.

(Quelle: http://bundesrecht.juris.de/)

Warum ist eine E-Mail-Archivierung so bedeutsam für Ihr Unternehmen?

1. Erfüllen Sie rechtliche Vorschriften und vermeiden Sie Sanktionen
Der Gesetzgeber hat inzwischen der E-Mail praktisch die gleiche rechtliche Bedeutung zugeschrieben, wie sie Dokumente in Papierform besitzen. Dies trifft auf alle Handels- und Geschäftsbriefe sowie auf alle Dokumente mit steuerrechtlich relevantem Inhalt zu.
Die Notwendigkeit zur E-Mail-Archivierung ergibt sich unter anderem aus den Vorschriften des Handels- und Steuerrechts über die Ordnungsmäßigkeit der Buchführung (§§ 238 ff. und § 257 HGB sowie §§ 140 ff. AO), den Grundsätzen ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) und aus den Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU).
Unternehmen sind dazu verpflichtet, alle relevanten E-Mails bis zu zehn Jahre lang vollständig aufzubewahren und jederzeit maschinell auswertbar vorzuhalten. Zudem muss sichergestellt werden, dass die Daten nicht nachträglich manipuliert werden können. Hierzu ist im Unternehmen entsprechende Software vorzuhalten.
Werden diese Archivierungspflichten nicht beachtet, drohen empfindliche Strafen bis hin zur persönlichen Haftung durch die Unternehmensleitung.

2. Steigern Sie die Produktivität und Informationsverfügbarkeit
Viele Informationen wie Angebote, Preisabsprachen und Verträge liegen oft nur noch in Form von E-Mails und deren Anhängen vor. Aus diesem Grund ist es für die Sicherheit und Produktivität eines Unternehmens entscheidend, dass diese Informationen zu jeder Zeit vollständig und schnell abgerufen werden können.

3. Führen Sie zusammen, was zusammen gehört
Oft verteilen sich die E-Mails in einem Unternehmen über zahlreiche Rechner, Softwaresysteme und Dateien. Dies erschwert die Verwaltung, aber auch die Nutzung der E-Mails durch die Mitarbeiter.

4. Verhindern Sie das Löschen von E-Mails durch Mitarbeiter
Mitarbeiter können für das Unternehmen wichtige E-Mails jederzeit löschen. Dies kann aus Versehen oder gezielt erfolgen. Nicht selten werden auch ganze Postfächer beim Verlassen des Unternehmens durch einen Mitarbeiter unwiederbringlich gelöscht.
Durch die E-Mail-Archivierung können Sie das Löschen von E-Mails durch Mitarbeiter vollständig unterbinden. Die E-Mails stehen dem Unternehmen so zuverlässig und langfristig zur Verfügung.

5. Schützen Sie sich vor Datenverlusten
Neben dem Löschen von E-Mails durch Mitarbeiter können diese auch durch technische Probleme oder Fehler verloren gehen. Dazu zählen zum Beispiel auch defekte Microsoft Outlook PST-Dateien und unvollständige Datensicherungen.

6. Schaffen Sie Postfachbegrenzungen ab
Nicht selten soll durch die Begrenzung von Postfachgrößen die Überlastung des E-Mail-Servers reduziert werden. In der Praxis zwingt dies die Anwender jedoch zur zeitaufwändigen Verwaltung ihrer Postfächer und zum Löschen von E-Mails.

Probleme der E-Mail-Archivierung im Zusammenhang mit lokalen SPAM-Filtern

Spam-Filterung vor der E-Mail-Archivierung
Die lokale Spam-Filterung vor der Archivierung birgt grundsätzlich das Risiko, dass archivierungspflichtige E-Mails nicht durch den Spam-Filter und somit auch nicht in das Archiv gelangen, obwohl die E-Mail bereits im Verfügungsbereich des Unternehmens gelangt ist. Die Archivierung wäre somit nicht vollständig und streng genommen auch nicht rechtssicher.
In der Praxis bestehen dazu drei Handlungsmöglichkeiten:

1. Es wird auf die Spam-Filterung vor der Archivierung verzichtet
Auf diese Weise ist zwar die Vollständigkeit der Archivierung sichergestellt, jedoch geht dies mit technischen Nachteilen einher. So wird durch das extrem hohe (da ungefilterte) E-Mail-Volumen der Speicherbedarf des Archivs stark erhöht. Die Folge sind höherer Aufwand und Kosten beim Speichermanagement und bei der Datensicherung. Zudem nimmt die Qualität der Suchergebnisse bei der Archivsuche durch den hohen Spam-Anteil deutlich ab.

2. Empfangene E-Mails werden von einer lokalen Anti-Spam-Lösung gefiltert und danach archiviert
Auf diese Weise wird zwar der Speicherbedarf des Archivs deutlich verringert und die Qualität von Suchabfragen erhöht, jedoch kann eine vollständige Archivierung aller relevanten E-Mails nicht zu 100% sichergestellt werden. Diese E-Mails können fälschlicherweise vom Spam-Filter abgewiesen werden. Das Verfahren geht demnach mit einem gewissen rechtlichen Risiko einher.

3. Als Spam identifizierte E-Mails werden von einer Anti-Spam-Lösung noch vor Annahme durch den eigenen E-Mail-Server abgewiesen
Solange als Spam identifizierte E-Mails nicht angenommen werden, besteht auch keine Pflicht zur Verarbeitung oder zur Archivierung dieser E-Mails. Technisch gesehen darf die Annahme der E-Mail nicht mittels Statuscode 250 vom SMTP-Server als erfolgreich „quittiert" werden. In diesem Fall ist nicht der eigene, sondern der zustellende E-Mail-Server für die Versendung eines NDR (Non-Delivery Report - Unzustellbarkeitsbericht) an den Absender verantwortlich.
Ein sehr gutes Beispiel für eine solche Lösung ist der NoSpamProxy.

Fazit

NoSpamProxy kann über die bloße Spam-Abwehr hinaus Ihrem Unternehmen einen zusätzlichen Mehrwert hinsichtlich der Realisierung der gesetzlich geforderten E-Mail-Archivierung erbringen.

Die korrekte Archivierung und „Sichtbarmachung" ist eindeutig Sache Ihres Unternehmens. Hierzu muss Software vorgehalten werden. Eine mögliche Lösung ist der MailStore-Software der deutschen Firma deepinvent GmbH. Der MailStore Server wurde durch eine unabhängige Wirtschaftsprüfungsgesellschaft geprüft und für Deutschland, Österreich und die Schweiz zertifiziert, so dass hiermit die Einhaltung der rechtlich relevanten Vorschriften möglich ist.

Einige der Voraussetzungen für MailStore oder ähnliche Lösungen können jedoch bei kleineren oder verteilten Unternehmensstrukturen ohne einen eigenen Mailserver nur sehr umständlich oder gar nicht realisiert werden. Hier kann NoSpamProxy einen weiteren Mehrwert erbringen, indem alle an Ihr Unternehmens ausgelieferten Mails noch einmal zusätzlich (und somit unabhängig von der individuellen Behandlung der Postfächer) zunächst auf unserem Server archiviert und (nur) diese Archivdateien Ihrem Archivierungssystem zur Verfügung gestellt werden. MailStore ist auf eine solche Variante vorbereitet.

Die in diesem Dokument erwähnten Rechtsgrundlagen dienen lediglich der Information und stellen keine Rechtsberatung dar. Im konkreten Einzelfall wenden Sie sich bitte an einen spezialisierten Rechtsanwalt. Eine Gewähr und Haftung für die Richtigkeit aller Angaben wird nicht übernommen.

Das Prinzip von NoSpamProxy

Spam und Spam-Schutz

Mit immer ausgefeilteren Methoden versuchen Spammer, bestehende Schutzsysteme auszuhebeln und ihre „Botschaften" an den Adressaten zu bringen. Mit dem täglichen Aufräumen des Posteingangs ist es oft leider nicht getan; Spam bedeutet längst eine gravierende ökonomische Belastung für viele Unternehmen. Für Deutschland wird gegenwärtig eingeschätzt, dass bis zu 99 % des Mailverkehrs vom Empfänger nicht erwünscht sind.
Spam wirkt störend auf die Geschäftsprozesse und bindet Mitarbeiter ebenso wie System-Ressourcen. Die ungewünschten E-Mails können zudem die Mailserver erheblich beeinträchtigen und im Extremfall sogar lahm legen. Einige Spam-E-Mails haben darüber hinaus erhebliche kriminelle Energie. Sie können Inhalte und Anhänge aufweisen, die Ihr System angreifen oder ausspähen. Eine weitere besonders perfide Spam-Attacke ist der Versuch, Ihr System als Relay zu missbrauchen. Dann versenden Spammer E-Mails mit „Ihrem Namen" – und auf Kosten Ihrer Kapazität. Die Folge kann sein, dass seriöse E-Mail-Partner Ihre Domain als Spam-Sender bewerten und wichtige Verbindungen unversehens gesperrt werden.
Nicht nur die „Angriffs"-Szenarien sind vielfältig und komplex; hinzu kommt, dass Spam nicht immer gleich Spam ist. So verschieden die Interessen von Unternehmen sein können, so unterschiedlich kann die Bewertung einer E-Mail ausfallen. Ob Sie eine E-Mail-Werbung, einen Newsletter oder eine E-Mail mit chinesischen Schriftzeichen als Spam einstufen, sollten Sie selbst definieren können. Und genau das ermöglicht Ihnen NoSpamProxy.

Abwehren statt Sortieren

Viele Spammer reagieren immer schneller und versierter auf neue Schutzmethoden. Dies bedeutet, dass statische Spam-Filter kurzfristig mitunter sehr erfolgreich arbeiten – und dennoch morgen schon nutzlos sein können.
Ein effektiver Spam-Schutz muss intelligent, flexibel und lernfähig sein, um wirklich zu greifen. Er sollte nicht nur vor unerwünschten E-Mails schützen. Mindestens genauso wichtig ist es, dass er „gute" E-Mails korrekt bewertet. Eine Quote von 98 % geblockter Spam-E-Mails klingt gut – nur schadet sie mehr als sie nützt, wenn dabei wichtige „gute" E-Mails versehentlich mitgeblockt werden oder im falschen Ordner landen.
Und der Schutz sollte genauso individuell und vielseitig sein, wie es die Anforderungen Ihrer Geschäftsprozesse sind. Gleichgültig, ob Ihr Unternehmen 5 oder 5.000 Mitarbeiter hat.
Letztendlich sollte ein Schutz Ihr System und die Unternehmensabläufe nicht nur vor Spam bewahren, sondern auch vor unnützer Belastung des Systems – denn die Schonung Ihrer Ressourcen steht schließlich im Mittelpunkt.
Diese Anforderungen an einen intelligenten Spam-Schutz waren der Antrieb zur Entwicklung von NoSpamProxy. Der Grundgedanke ist einfach: Im Gegensatz zu anderen Filtern wehrt NoSpamProxy Spam-E-Mails ab, bevor sie in Ihr System gelangen. Strikt nach dem Slogan: Abwehren statt Sortieren.
Der Möbel-Prospekt – ein Vergleich:
Stellen Sie sich vor, Sie erwarten einen bestimmten Werbeprospekt einer Möbelfirma. Der Postbote wirft Ihnen diesen Prospekt eines Morgens in den Postkasten – und mit ihm zusammen zweihundert andere Werbeprospekte, die alle an Sie adressiert sind und von denen Sie keinen einzigen bestellt haben. Ihr Postkasten quillt nun über und kann keine „vernünftige" Post mehr aufnehmen. Davon abgesehen: Hatten Sie an diesem Morgen nicht etwas anderes vorgehabt, als ausgerechnet Werbeprospekte auszusortieren? Das jedoch ist in überspitzter Form die alltägliche Spam-Situation.
Die unerwünschten Prospekte müssen Sie nicht nur aussortieren, Sie müssen sie auch irgendwo ablegen oder speichern. Und bei aller Sortiererei kann es Ihnen passieren, dass Sie den einzigen erwünschten Prospekt der Möbelfirma versehentlich zum Altpapier ordnen! Der ganze Aufwand ist dann umsonst gewesen.

Vorteile der frühen Abwehr

NoSpamProxy übernimmt für Sie die Rolle eines Türstehers, der Ihren Postkasten bewacht. Ein Türsteher, der mitdenkt: Er prüft genau, was für Prospekte der Postbote in Ihren Postkasten werfen möchte. Unerwünschte Prospekte sortiert der Türsteher nicht bloß aus, er drückt sie dem Postboten wieder „aufs Auge". Nur den „guten" Prospekt nimmt der Türsteher vom Postboten an und legt ihn selbst in Ihren Postkasten. Ihr Postkasten bleibt frei für wirklich wichtige Post. Das Beste daran: Sie können währenddessen in Ruhe frühstücken - von dem „Papierkrieg" vor Ihrer Haustür bekommen Sie nichts mit.

NoSpamProxy arbeitet als vorgeschalteter Server, der eine eigene zweite Verbindung zu Ihrem Mailserver aufbaut. NoSpamProxy puffert nur so viel der ankommenden E-Mail, wie für die Spam-Prüfung erforderlich ist. Die E-Mail wird dekodiert und geprüft; bei Bewertung als Spam wird die angefangene E-Mail sofort abgelehnt.
Das NoSpamProxy-Prinzip ist ebenso einfach wie überzeugend. Aus der frühzeitigen Abwehr resultiert eine Reihe von Vorteilen:
Der Mailserver wird gar nicht erst mit den Spam-E-Mails belastet. Rechnerkapazitäten und Posteingänge bleiben frei, man spart Transfervolumen und die damit entstehenden Transferkosten.
Jede abgeblockte E-Mail erzeugt eine Unzustellbarkeits-E-Mail (NDR – Non Delivery Report) durch den einliefernden Mailserver an den Absender. Dies bedeutet: Die E-Mail ist offiziell abgelehnt und gilt als nicht zugestellt. Somit kann der Absender nicht belegen, dass die E-Mail bei Ihnen angekommen ist. Und das bewahrt Sie nicht nur vor Verständigungsproblemen und unliebsamen Überraschungen, sondern im Ernstfall auch vor rechtlichen Konsequenzen.
Die „NDR"-E-Mail wird nicht vom Ziel-Mailserver erstellt, sondern vom Mailserver des Absenders! Dies schont wiederum die Systemressourcen. Die „NDR" enthält zudem eine aussagekräftige Fehlermeldung, warum die E-Mail nicht angenommen wurde.
Manuelle Nachbearbeitung von Quarantäne-E-Mails entfällt. Viele andere Systeme lagern verdächtige E-Mails in einer Quarantäne – versehentlich einsortierte „gute" E-Mails können nur mit hohem Aufwand wieder gefunden werden. Diesen Aufwand können Sie sich mit NoSpamProxy ersparen. Wenn eine „gute" E-Mail geblockt werden sollte, verschwindet diese E-Mail nicht einfach; der Absender erhält eine „NDR"-E-Mail und kann darauf reagieren.
Ihre Mailarchive werden nicht mit Spam belastet, denn dieser wird schon vor dem Empfang abgelehnt. Daher muss auch kein „Datenmüll" archiviert werden.
Spam-Sender werden abgeschreckt. Durch die aktive Ablehnung der E-Mails gehen Spam-Sender von einem Misserfolg aus. Ihre Adresse verliert für unseriöse Absender an Wert.
Das Ärgernis „offene Relays" wird auf den Absender verlagert. Dort laufen die E-Mails in den Warteschlangen auf – ein deutlicher Appell an den Betreiber, die nicht mehr zeitgemäße Praxis der offenen Relays zu überdenken. Schließlich kann Ihnen niemand vorschreiben, welche E-Mails Sie annehmen und welche nicht.
NoSpamProxy verbirgt übrigens auch die Meldungen des annehmenden Mail-Servers vor dem Absender. Dieser kann dann so keine Rückschlüsse auf das eingesetzte Mailsystem erhalten – ein Zugewinn an Sicherheit.

„False Positives" und Spam-Quarantäne

Als „False Positives" bezeichnet man „gute" E-Mails, die versehentlich als „verdächtig" bewertet und abgelehnt werden. Wie bereits erwähnt, liegt hierin eine der größten Gefahren einer Filterlösung: Je mehr Spam Sie aussortieren müssen, desto wahrscheinlicher ist es, dass Sie versehentlich eine „gute" E-Mail beseitigen. Die Folgen können unter Umständen fatal sein.

Die meisten Filter archivieren Spam-E-Mails, bevor diese gelöscht werden. Das ist eine zusätzliche Belastung der Speicherkapazitäten. Landet ein „False Positive" mit dem Spam zusammen in einem Archiv-Ordner, ist die „gute" E-Mail nur sehr schwer wieder auffindbar. Vielleicht geht die E-Mail sogar ganz verloren, ohne dass Sie sie je zu lesen bekommen haben. Ablaufstörungen und Missverständnisse sind vorprogrammiert, da der Sender davon ausgeht, dass seine E-Mail bei Ihnen angekommen ist. Im schlimmsten Fall hat der Irrtum gravierende wirtschaftliche und eventuell sogar rechtliche Konsequenzen. Denn der Sender hat einen Nachweis über die erfolgreiche Zustellung seiner E-Mail zu Ihrem System.

Wie NoSpamProxy „False Positives" und die Folgen verhindert

NoSpamProxy bewahrt Sie vor dieser Problematik. Wenn NoSpamProxy eine E-Mail als Spam klassifiziert, verschwindet diese nicht in irgendwelchen Ordnern. Sie wird gar nicht erst angenommen; und der Absender erhält eine „NDR"-E-Mail. Aufgrund dieser Rückmeldung wird ein seriöser Absender sein Anliegen erneut vorbringen, da er weiß, dass die E-Mail nicht ankam. Vor allem: Er hat keinen Zustellungsnachweis. Das heißt, Sie können Missverständnissen mit NoSpamProxy effektiv vorbeugen, und Rechtsstreitigkeiten wegen verschwundener E-Mails werden vermieden.

Dass eine „gute“ E-Mail als Spam beurteilt wird, kann kein Schutzsystem völlig ausschließen. Eine 100%-Trefferquote gibt es leider nicht. Doch ist eine Abweisung eines „False Positives“ mit „NDR“-Rückmeldung in jedem Fall besser, als das Risiko einer in der Quarantäne abgelegten E-Mail, von der Sie nichts erfahren und der Absender nicht über den Vorgang informiert wird.

Wie kann ich als Anwender einen „False Positive“ korrigieren?
Angenommen, Sie erhalten von einem Kunden per Telefon die Nachricht, dass seine E-Mail an Sie nicht durchgekommen ist, sondern als Spam klassifiziert und abgewiesen wurde. Diese unschöne Situation können Sie mit NoSpamProxy auf einfachem Wege auflösen. Sie brauchen hierzu kein Administrator zu sein und keine Einstellungen am System vorzunehmen oder an NoSpamProxy etwas zu ändern; schicken Sie einfach Ihrerseits eine E-Mail an die abgewiesene E-Mail-Adresse des Kunden. Die nächste E-Mail des Kunden wird dann von NoSpamProxy automatisch als Reaktion auf Ihre E-Mail gewertet – auch wenn der Absender nicht die „Antwort“-Funktion verwendet – und als „gut“ bzw. erwünscht beurteilt.
Dies bedeutet, dass ein zweiter Anlauf in der Regel problemlos durchkommt, und keine weiteren „False Positives“ entstehen. Die E-Mail-Adresse des Absenders ist von NoSpamProxy als „vertrauenswürdig“ eingestuft worden.
Das Prinzip, das hinter dieser „Vertrauensbildung“ steckt, wird Level of Trust genannt. Wie das genau vor sich geht und der Level of Trust Filter funktioniert, erfahren Sie weiter unten.

Geht (bei einem „False Positive“) eine „NDR“ an einen seriösen Absender, gibt diese ihm die wichtige Information mit, dass und auch warum seine E-Mail abgewiesen wurde. Er kann dementsprechend aktiv werden und sein Anliegen auf eine andere Art und Weise kommunizieren.

Für den Spammer, der auf direktem Weg versendet, bedeutet eine „NDR“ vor allem eines: Er wird seine E-Mail nicht los. Und das ist für einen unseriösen Absender stets die unangenPartnerte Situation. Er hat im Prinzip nur zwei Möglichkeiten, sein Anliegen weiter zu verfolgen:
Der Spammer sendet die E-Mail erneut, was ihm aber nur eine weitere „NDR“-Reaktion einbringt, welche mit weiteren Kosten und Mühen für ihn verbunden sind.
Der Spammer überlegt sich eine neue Strategie und versucht sein Glück mit einer modifizierten E-Mail.
Kosten und Aufwand hat er in beiden Situationen. Und je mehr Aufwand ein Spammer betreiben muss, desto eher unterlässt er sein Treiben; oder er sucht sich ein leichteres Opfer.
Viele Spammer senden aber Ihre E-Mails über den „Umweg“ eines offenen Relays. Die Spammer werden mit dieser Vorgehensweise durch eine „NDR“ nicht erreicht; vielmehr verlagert sich die Problematik auf den Betreiber des Relays. Die Praxis der offenen Relays ist bei Spam-Schützern längst als äußerst fragwürdig erkannt. Daher ist es aus unserer Sicht vertretbar, wenn ein Relay-Betreiber durch die zusätzlichen „NDR“-Meldungen animiert wird, seine Vorgehensweise zu überdenken.

Erläuterungen zu Filtern und Actions von NoSpamProxy

Schwellenwert (SCL)
Mit „Abweisen“ werden keine Filter oder Action angewandt. Die Mail wird grundsätzlich nicht zugestellt.
Mit „Weitergeben“ werden nur die Filterprüfungen außer Kraft gesetzt. Eingestellte Actions werden dennoch angewandt.
Mit „Überprüfen. Abweisen ab einem SCL von xx“ werden die E-Mails geprüft.
Der Schwellenwert (SCL), ab dem eine E-Mail abgewiesen werden soll, kann zwischen -1 bis 10 ausgewählt werden.
Der SCL-Wert -1 bedeutet, dass der Schwellenwert am niedrigsten ist; E-Mails werden bei dieser Einstellung besonders „früh“ (bei niedrigem Spam-Charakter) geblockt. Bei einem negativen Schwellenwert werden allerdings auch E-Mails abgewiesen, welchen keinen SPAM-Charakter vorweisen und durch NoSpamProxy mit „0“ als neutrale E-Mails bewertet wurden. Um dies zu verhindern, sollten Regeln definiert werden, welche auch negative Bewertungsmöglichkeiten bieten, z.B. ein Wortfilter für positive Wortübereinstimmungen.
Wenn Sie den SCL-Wert 10 eingeben, ist die Schwelle besonders hoch; E-Mails werden bei diesem Wert nur dann geblockt, wenn sie extrem hohen Spam-Charakter haben.
Für jeden Filter kann man einen Maluswert (schlechte Punkte) von 1 bis 10 definieren. Das bedeutet, wenn eine E-Mail von einem Filter wie z.B. dem Wortfilter geprüft wird und ein „böses Wort“ sowohl in der Betreffzeile als auch im E-Mail-Text gefunden wird, dass pro Fund des „bösen Wortes“ der eingestellte Maluswert der zu prüfenden E-Mail zugewiesen wird. Die vergebenen Maluswerte werden nach Prüfung aller in der Regel (Konfiguration) definierten Filter addiert. Übersteigt die Summe der Maluspunkte (schlechte Punkte) den eingestellten Schwellenwert (SCL), so wird die E-Mail abgewiesen.

Level of Trust
Das Level of Trust System ist ein mehrschichtiges Konzept, das die Vertrauenswürdigkeit einer Kommunikationsbeziehung oder einer Domäne beurteilt. „Vertrauen“ muss sich ein Absender „verdienen“; stärkster Pluspunkt dabei ist eine verlässliche und dauerhafte Verbindungs-Historie.
Das System bewertet verschiedene Kriterien, u. a. Absender-Adressen und Prüfsummen, vor allem aber auch die Adressbeziehungen für eingehende und ausgehende E-Mails. Die Informationsdatenbank, mit deren Hilfe der Level of Trust berechnet wird, bezieht ihre Daten aus mehreren Quellen.
Bei ausgehenden E-Mails wird die Kommunikationsbeziehung (zwischen Absender und Adressat) in der Datenbank mit einem sehr hohen Vertrauensbonus gespeichert. Um Daten zu schützen, wird diese Beziehung nicht im Klartext gespeichert, sondern nur in Form eines Hashwertes (einer Art Prüfsumme) fest gehalten. Des Weiteren ist die Relation von Absender und Betreff eine interessante Perspektive. Es liegt nahe, auch eine Antwort eines Kollegen oder eines Stellvertreters und gegebenenfalls eine alternative Adresse als „gut“ bewerten zu können. Zusätzlich wird bei ausgehenden E-Mails das Vertrauen in die Domäne des Adressaten um einen bestimmten Wert erhöht. Damit erhalten auch die Antwort-E-Mails des Adressaten an andere Nutzer des Systems einen Bonus. Wird eine eingehende E-Mail als Spam klassifiziert, verringert sich das Vertrauen in die Domäne.
Ein wichtiger Vorteil dieses Filters liegt darin, dass man nach und nach eine immer genauere „Karte“ mit Kommunikationsbeziehungen aller Mitarbeiter erhält, in die auch Informationen über Spam-Sender einfließen. Aufgrund dieser „Karte“ kann man mit der Zeit die Schwellenwerte für die E-Mails reduzieren und „strenger“ filtern, ohne die Zahl der „False Positives“ signifikant zu erhöhen.
Findet über einen gewissen Zeitraum keine Kommunikation mit einem bestimmten Absender mehr statt, verringert sich der Level of Trust automatisch. Diese Abnahme des Wertes geschieht sowohl bei Bonus- als auch bei Malus-Werten. Einem längeren zwischenzeitlichen „Schweigen“ wird auf diese Art und Weise sowohl im Positiven wie auch im Negativen Rechnung getragen: verlässliche, dauerhafte Kommunikation hinterlässt einen immer besseren Eindruck, Spam-„Wiederholungstäter“ einen immer schlechteren.

Bei der globalen Anwendung von Level of Trust können auch sogenannte „Stoppwörter“ definiert werden. Sobald NoSpamProxy eines dieser Wörter im Betreff einer ausgehenden E-Mail findet, werden für diese E-Mail sowohl der AddressPairing- als auch der Domänen-Bonus nicht erhöht. Bei automatisch generierten E-Mails wie Abwesenheitsnotizen ist das eine sinnvolle Einstellung.
Da diese Einstellungen immer für alle Regeln im NoSpamProxy gelten, können wir hier keine kundenspezifischen Einstellungen vornehmen. Im folgendem finden Sie die derzeit eingerichteten „Stoppwörter“. Sollten Sie Anregungen zur Erweiterung dieser List haben, würden wir uns auf ein Feedback von Ihnen freuen.

Read:, Deleted:, Gelesen:, Gelöscht:, Abwesenheitsnotiz:, Out of Office AutoReplay:, Empfangsbestätigung, Return Receipt, noLoT

Mit dem zusätzlichen Wort „noLoT“ in der Betreffzeile Ihrer ausgehenden Mail können Sie manuell das positive Bewerten des E-Mail-Empfängers verhindern.

CommToch AntiSpam Dienst
Der CommTouch AntiSpam Service bewertet eine Mail anhand von „Fingerabdrücken“. Diese werden allgemein als REF-IDs bezeichnet und sind weitaus umfangreicher, als die unscharfe Prüfsumme. Sie enthalten zum größten Teil Informationen über die Versandart und das Verbreitungsverhalten der Mail.

Inhalte werden in der REF-ID nicht übermittelt, auch die Empfängerinformation ist nicht enthalten. Die REF-IDs werden beim Detection Center von CommTouch auf den Spam-Gehalt via HTTP abgefragt und sind ca. 200 Byte klein.
Die Server des CommTouch Detection Center sind durch eine globale Überwachung des Mailverkehrs in der Lage, eine Spamwelle sehr zeitnah zu entdecken. Im CommTouch AntiSpam Service Filter wird allerdings nur der Spam-Gehalt bewertet. Für die Erkennung von vireninfizierten Mails gibt es die CommTouch AntiVirus Action im NoSpamProxy.

CommTouch Zero Hour Virus Outbreak Protection
Die CommTouch Zero Hour Virus Outbreak Protection Action ist das Pendant zum CommTouch AntiSpam Service Filter. Im Gegensatz zu diesem Filter bewertet die Action allerdings ausschließlich den Virusgehalt einer E-Mail. Das ist allerdings kein realer VirenScanner!
Die Server des CommTouch Detection Center sind durch eine globale Überwachung des Mailverkehrs in der Lage, eine Viruswelle sehr zeitnah zu entdecken. E-Mails, welche dem Charakter (Fingerabdruck) von virenbehafteten Massenmails sehr stark ähneln, werden so schneller erkannt und als unerwünschte E-Mails klassifiziert.
Der Vorteil dieser Action liegt darin, dass Massen-E-Mails mit neuen unbekannten Viren sehr schnell erkannt werden können, da solche E-Mails einen immer wiederkehrenden Charakter aufweisen. Diese Art von Schutz wirkt schneller als ein dateibasierter Virenscanner, da letzterer erst nach einem Softwareupdate vorher unbekannte Viren entdecken kann.
Ein realer Virenscanner ist dennoch zum Schutz vor Viren erforderlich, da diese Action nur aufgrund von Massen-E-Mails lernen kann. Ein einzelner Virus, welcher nicht durch Massen-E-Mails versendet wird, würde so ungehindert sein Ziel erreichen.

Realtime Blocklists (RBL)
Der Filter „Realtime Blocklists“ prüft, ob ein Adresseintrag in Realtime-Blocklisten vorliegt. Theoretisch können Sie bestimmen, welche Blocklisten zum Schutz abgefragt werden sollen. Praktisch wenden wir jedoch alle von NoSpamProxy automatisch angebotenen Blocklisten an. Da auch die besten Listen „False Positives“ aufweisen können, sollte man stets mehrere Listen heranziehen. Da jeder „Treffer“ als Maluspunkt gewertet wird, wird das Risiko für eine Mail minimiert, anhand einer einzelnen Sperrliste gleich blockiert zu werden. Bestimmte Listen können auch Bonuspunkte vergeben.

SPAM URI Realtime Blocklists (SURBL)
Spam-URL-Blocklisten (SURBL), verwalten Listen mit verdächtigen Spam-URLs. Der „SURBL Filter“ isoliert aus den Links in einer Mail die Domäne und prüft, ob ein entsprechender Eintrag in den SURBL-Listen vorliegt. Des Weiteren sucht er auch nach URLs die mit „www.“ anfangen und nicht als Link in der Mail auftauchen.
Theoretisch können Sie bestimmen, welche Blocklisten zum Schutz abgefragt werden sollen. Praktisch wenden wir jedoch alle von NoSpamProxy automatisch angebotenen Blocklisten an.

Statistische Analyse (Bayes)
Anfangs konnten Spam-E-Mails sehr einfach durch Wortlisten erkannt und gefiltert werden. Allerdings ist dies heute kaum mehr möglich. Ein englischer Mathematiker und presbyterianischer Pfarrer namens Thomas Bayes hat einen richtigen Satz zur Wahrscheinlichkeit beschrieben, der im Bayes Filter zur Anwendung kommt. Anhand einer Menge guter und schlechter E-Mails werden Wahrscheinlichkeiten für bestimmte Bruchstücke ermittelt und damit neue E-Mails klassifiziert.
NoSpamProxy ist auch in der Lage, selbstständig, d.h. während des Betriebs, zu lernen. Dazu muss die Action Statistisches Training (Bayes) mit in die Regeln eingebunden werden. Nach diesem Prinzip arbeiten übrigens viele Spam-filternde Mail-Client-Programme (z.B. Microsoft Outlook).

Unscharfe Prüfsumme
Die unscharfe Prüfsumme ist ein Kriterium, um die Ähnlichkeit von E-Mails zu beurteilen. Für jede E-Mail werden diverse unscharfe Prüfsummen erstellt. Wenn in einer ähnlichen E-Mail von einer anderen Domäne übereinstimmende Prüfsummen auftreten, bekommt diese E-Mail Maluspunkte. Je häufiger eine vergleichbare E-Mail eintrifft, desto höher steigt auch der Maluspunkt für die E-Mail.
Weil dieser Filter auch eine Prüfsumme über Anlagen anlegt, werden E-Mails mit vielen identischen Anlagen immer schlechter bewertet. Auf diese Art und Weise blockiert dieser Filter teilweise sogar Viren bei wiederholtem Auftreten weit früher, als der Virenscanner ein aktuelles Patternfile bekommen hat.

Wortübereinstimmungen (Wortfilter)
Es gibt Wortfilter sowohl für die Betreffzeile der E-Mail als auch für den Body. Sie können damit festlegen, welche Ausdrücke Malus- oder Bonuspunkte erhalten.
Mit diesen Filtern können Sie somit Ausdrücke als SPAM-„verdächtig“ festlegen und mit Maluspunkten von 1 bis 10 bewerten. Jedes Auftauchen eines solchen Ausdruckes in einer E-Mail wird „bestraft“.
Im Gegensatz dazu können auch „positive“ Wortlisten geführt werden, in denen man für das Finden von festgelegten Ausdrücken „gute Punkte“ von -10 bis -1 festlegt. Jedes Auftauchen eines solchen Ausdruckes in einer E-Mail wird dann also „belohnt“.
Eine Wortliste kann aus einzelnen Wörtern oder auch Wortgruppen bestehen, sie darf Platzhalterzeichen „?“ und „*“ enthalten. Man kann einstellen, ob die Suche auf exakt das Wort bzw. die Wortgruppe oder auf ähnliche Worte/Wortgruppen durchgeführt werden soll. In diesem Falle wandelt NoSpamProxy den Inhalt der Liste (allerdings nach feststehenden Regeln!) in sogenannte reguläre Ausdrücke um. Alternativ können Sie daher auch eigene reguläre Ausdrücke definieren.

Adressmanipulation
Diese Action eröffnet Ihnen die Möglichkeit, die Zieladresse beim Empfang einer E-Mail zu verändern. So können Sie z. B. nach einem Namenswechsel in der Firma alle an die alte Adresse einkommenden Mails auf die neue Adresse umschreiben.
Ein zweiter Anwendungsfall ist die Definition einer „Geheimadresse“. So können Sie zum Beispiel festlegen, dass alle eingehenden E-Mails mit einem bestimmten Zusatztext (z.B. „_geheim“) im Empfänger-Adressfeld als erwünscht bewertet, der Zusatztext aus dem Empfängernamen gelöscht und im „Pass“-Modus ohne weitere Prüfungen durchgelassen werden.

Anhänge verwalten
Die Action „Anhänge verwalten“ prüft die Dateinamen der Anhänge und löscht relevante Anhänge oder weist die zugehörigen E-Mails ab. Auch hier können Sie die entsprechenden Werte individuell einrichten. So können Sie beispielsweise alle E-Mails mit „*.exe“-Dateien abweisen oder nur die Anlage löschen. Alternativ können Sie auch einstellen, dass Sie generell alle E-Mails mit Anhängen abweisen möchten, außer E-Mails mit von Ihnen festgelegten Anhängen.
Prinzipiell ist es eine sehr gute Idee, ausführbare Anlagen in E-Mails von vorneherein abzuweisen. Im alltäglichen Geschäftsverkehr werden zwar sehr viele Dokumente und andere Dateien ausgetauscht, jedoch in der Regel keine Programme. Sollte der Austausch von ausführbarem Code erforderlich sein, ist es heute nicht zu viel verlangt, diese Dateien in ein Archiv zu verpacken. Sehr viele Viren verbreiten sich über Programm-Anhänge, weil Anwender unbedarft Anlagen direkt ausführen. Dies wird durch eine solche Blockade verhindert.

Dateibasierter VirenScanner

Viren sind neben Spam eine große Bedrohung und sollten ebenfalls so früh wie möglich aussortiert werden. Auch bei der Suche nach Viren können „übereifrige“ Filter eine erwünschte E-Mail irrtümlich entfernen. Die meisten Produkte löschen solche E-Mails, ohne den Empfänger oder Absender zu informieren. Die Problematik ist hier vergleichbar mit einem Quarantäneverzeichnis einer herkömmlichen Lösung. NoSpamProxy arbeitet anders.
Die Action „Dateibasierter Virenscanner“ speichert alle Dateianhänge von durchkommenden E-Mails „probehalber“ in ein internes Verzeichnis. Der VirenScanner wird einen lesenden Zugriff auf eventuell verseuchte Anhänge verweigern. NoSpamProxy prüft nach Ablage der Anhänge in das Verzeichnis, ob ein Zugriff noch möglich ist oder nicht. Anhänge, auf die zugegriffen werden kann, werden als virenfrei angesehen. NoSpamProxy kann mit jedem beliebigen Virenscanner zusammen arbeiten, der in Echtzeit Dateizugriffe überwacht. Diese Scanmethode ist auf sehr vielen Dateiservern bereits installiert, sehr performant und zuverlässig. Gute Virenscanner für Serverbetrieb sind allerdings kostenpflichtig. Wir setzen gegenwärtig aktuelle Produkte von Avira ein.
Sie können selbst einstellen, ob verseuchte Anhänge nur gelöscht werden oder ob die zugehörige E-Mail insgesamt abgelehnt werden soll.
Wenn Sie diese Art von E-Mails ablehnen, dann wird, wie bei einer erkannten Spam-E-Mail, der einliefernde Mailserver eine Unzustellbarkeitsnachricht an den Absender generieren. Das Risiko bei einer Falscherkennung entfällt.

E-Mail-Archivierung

Die Action “E-Mail Archivierung” speichert die verarbeiteten E-Mails auf Wunsch als EML-Datei auf unserem NoSpamProxy-Server ab. Das bietet Ihnen u.a. die Möglichkeit, diese Dateien in Ihr vorhandenes Archivierungssystem zu importieren.
Mit „Zu archivierende E-Mail-Typen“ stellen Sie zunächst ein, welche E-Mails Sie überhaupt archivieren möchten. Sie können nur zugestellte E-Mails archivieren (empfohlen) oder nur temporär abgewiesene oder nur permanent abgewiesene E-Mails. Sie haben aber auch die Möglichkeit, die drei Typen zu kombinieren.
Bei gewünschter Zusatzoption „E-Mail-Archivierung mit Backup“ werden wir Ihr E-Mail-Archivierungsverzeichnis täglich (ggf. in separat zu vereinbarenden kürzeren Zeitabständen) auf einen Dateiserver außerhalb unseres Rechenzentrums inkrementell sichern und bei Bedarf eine Rücksicherung veranlassen. Sie erhalten von uns einen FTP-Zugang mit Leserechten zu Ihrem E-Mail-Archivierungsverzeichnis. Ein direkter Kundenzugriff auf die Backupdaten ist nicht vorgesehen. Auf dem NoSpamProxy- und ggf. Backup-Server werden Ihre Mails bis zum 15. Dezember eines jeden Jahres gespeichert. Alle E-Mails bis zu diesem Zeitpunkt werden von uns auf WORM-Medien geschrieben und zu unserer Entlastung an Sie per Post oder Paketdienst versandt. Nach Ihrer Empfangsbestätigung werden wir die betreffenden Mails auf unserem Server endgültig löschen und ggf. ein neues Backup initialisieren.

Greylisting

Das Greylisting ist eine Vorsichtsmaßnahme gegen „verdächtige“ E-Mails. Bleibt eine E-Mail knapp unter dem von Ihnen definierten Spam-Schwellenwert, würde diese E-Mail ohne Greylisting als ausreichend gut bewertet werden. Die Greylisting-Action lässt nun diese E-Mail nicht gleich durch, sondern lehnt sie temporär ab. Der einliefernde Mailserver bekommt eine Fehlermeldung, die ihn dazu bewegt, die E-Mail nach einiger Zeit erneut zu senden. Die Action erstellt einen Level of Trust-Eintrag, der den Absender und Empfänger enthält und der dann mit einer gewissen Verzögerung gültig wird. Die Verzögerung können Sie nach Ihrem Bedarf ändern.
Hinter dieser Action steht folgendes Prinzip: Ein direkt sendender Spammer scheut in der Regel die Mühe, die E-Mail ein zweites Mal zu senden. Ein normaler Absender-Mailserver hingegen wird nach einiger Zeit erneut die Zustellung versuchen. Bei dem zweiten Versuch wird nun diese Verbindung durch den Level of Trust-Filter besser bewertet, so dass die E-Mail passieren kann.
Den Schwellenwert, ab wie vielen Malus-Punkten eine eigentlich passierende E-Mail als „verdächtig“ eingestuft wird, können Sie individuell einstellen. Ebenso können Sie die Verzögerungszeit einstellen, nach der der Level of Trust-Eintrag erfolgen soll.

Statistisches Training (Bayes)

Der schon früher beschriebene Bayes-Filter nutzt eine Datenbank zur Klassifizierung von E-Mails. Diese Datenbank muss durch E-Mails trainiert werden. Diese Aufgabe übernimmt das Statistische Training, das Sie in den Regeln von NoSpamProxy entsprechend einbinden können. Mit dieser Action ist NoSpamProxy in der Lage, während des Betriebs selbstständig zu „lernen“.
Ausgehende E-Mails werden dabei durch das Statistische Training immer als „gute“ E-Mail gelernt. Dabei muss die Action in die ausgehende Regel von NoSpamProxy eingebunden werden.
Eingehende E-Mails werden in Abhängigkeit der Bewertung wie folgt gelernt:
E-Mails, die eine Bewertung kleiner gleich „ein fester Wert zwischen -9..-1“ bekommen haben werden als „gute“ E-Mails gelernt.
E-Mails mit einem Ergebnis größer gleich „ein fester Wert zwischen 1..9“ werden als „schlechte“ E-Mails aufgenommen.
E-Mails, die zwischen diesen Werten bewertet werden, werden als „neutral“ betrachtet und es findet kein Lernvorgang statt.