

Collax Spamfilter

Howto

Dieses Howto beschreibt die Einrichtung des Spamfilters auf einem Collax Server.

Vorraussetzungen

- Collax Business Server
- Collax Groupware Suite
- Collax Security Gateway
- Collax Platform Server inkl. Collax Modul Mail Security

Ziel

In diesem Howto sollen die verschiedenen Mechanismen zur Abwehr unerwünschter Spam-E-mails gezeigt und erklärt werden.

Wir gehen davon aus, dass der Mailserver bereits eingerichtet ist und möchten möglichst viele unerwünschte E-mails ausfiltern. Bei den eingetragenen Werten in den Screenshots handelt es sich um Erfahrungswerte. Es kann vorkommen, dass man die Werte seinem Umfeld anpassen muss.

Mechanismen

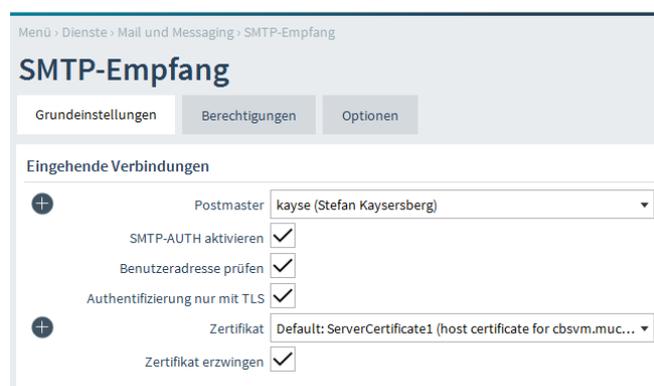
Welche Mechanismen gibt es? Grundsätzlich werden zwei Arten unterschieden.

Mechanismen die beim SMTP Empfang bereits zum Einsatz kommen und welche, die nach dem Eingang der Email filtern sollen. Erstere können nur dann eingesetzt werden, wenn die E-mails aufgrund eines MX Records direkt an den Server zugestellt werden. Werden E-mails vom Providerserver abgeholt, können nicht alle Filtermechanismen eingesetzt werden.

Mechanismen vor der Annahme von E-mails

Bereits bei der ersten Kontaktaufnahme des versendenden Emailservers, können E-mails abgelehnt werden. Das setzt allerdings voraus, dass E-mails direkt empfangen werden. Der MX Record muss auf die externe IP des Servers verweisen. Wenn E-mails vom Provider abgeholt werden, sind diese Filter nicht sinnvoll.

Im Dialog „Dienste → Mail und Messaging → Mail Transport → SMTP-Empfang“ können bereits einfache Mechanismen zur Spamabwehr konfiguriert werden. Wenn „Benutzeradresse prüfen“ aktiviert ist, wird Email nur dann angenommen, wenn der authentifizierte Benutzer auch zu der Absenderadresse gehört. Auch wenn das Passwort eines Mitarbeiters geknackt wurde, können dann keine Mails mit falschem Absender versendet werden.



SMTP-AUTH aktivieren Normalerweise nimmt der SMTP-Dienst nur E-Mails an, die entweder für eine interne Maildomain bestimmt sind oder die von einem System eingeliefert werden, welches die Berechtigung zum „Weiterleiten“ („Relayen“) hat. Letzteres wird üblicherweise nur für IP-Adressen im lokalen Netz erlaubt.

Wird diese Option aktiviert, kann der SMTP-Dienst auch von Systemen bzw. Benutzern in „fremden“ Netzen zum Relayen von E-Mail verwendet werden. Dazu müssen sich diese Benutzer am System authentifizieren.

Benutzeradresse prüfen Ist diese Option aktiviert, wird für authentifizierte Benutzer der Absender überprüft. Nur wenn der Login-Name und die Absenderadresse zusammengehören, wird die E-Mail angenommen.

Wenn dieses System E-Mails von anderen Mailservern annehmen und weiterleiten soll und diese Systeme dazu eine Authentifizierung durchführen müssen, darf diese Option nicht aktiviert sein. Da in diesem Fall die Absenderadressen nicht zu dem Login des anderen Mailserver gehören, wird die Annahme der E-Mails verweigert.

Authentifizierung nur mit TLS Grundsätzlich wird bei einer SMTP-Authentifizierung das Passwort im Klartext übermittelt und könnte abgehört werden. Eine sichere, verschlüsselte Übertragung des Passworts ist nur bei der Aktivierung von TLS (Transport Layer Security) gegeben. Mit dieser Option kann sichergestellt werden, daß der SMTP-Dienst eine Authentifizierung nur bei aktiviertem TLS durchführt. Ist TLS mit der Gegenseite nicht möglich, wird der SMTP-Dienst die Zugangsdaten nicht unverschlüsselt senden.

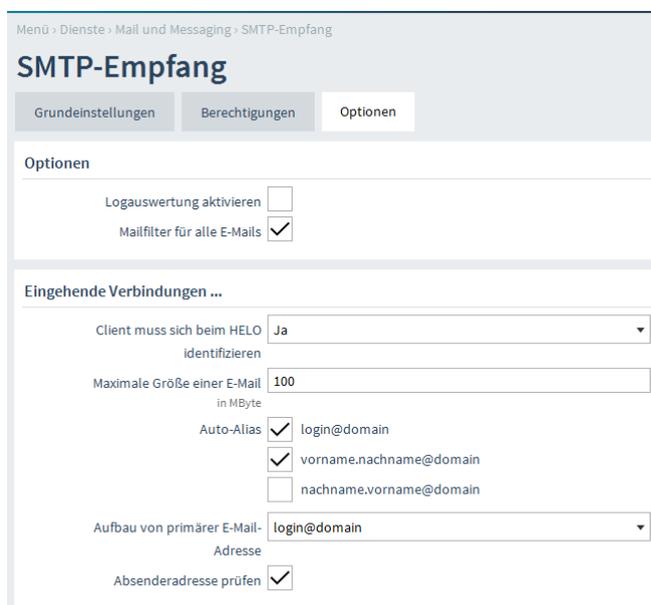
Zertifikat Um TLS zu verwenden, muss für den SMTP-Dienst im Vorfeld ein Zertifikat erstellt oder importiert worden sein. In dieser Liste werden alle geeigneten Zertifikate auf dem System angezeigt. Hier muss das für den Mailserver entsprechende Zertifikat ausgewählt werden.

Wird kein Zertifikat ausgewählt, kann TLS nicht verwendet werden.

Zertifikat erzwingen Eine sichere Anmeldung an einem Mailserver ist nur bei verschlüsseltem Austausch der Zugangsdaten möglich. Dazu muss in jeder SMTP-Verbindung TLS (Transport Layer Security) aktiviert werden. Für eine TLS-Verbindung benötigt jedes der beiden Systeme ein Zertifikat.

Ist diese Option aktiviert, wird bei eingehenden Verbindungen von der Gegenseite immer ein Zertifikat verlangt.

Im Reiter Optionen sollte zunächst der Haken bei „Mailfilter für alle E-Mails“ aktiviert sein.



Client muß sich beim HELO identifizieren Abhängig von diesem Parameter wird die HELO-Meldung bei einkommenden SMTP-Verbindungen untersucht.

Die Einstellung *nein* erlaubt dem Client, beliebige Angaben mit dem HELO zu senden.

Wird die Einstellung *ja* aktiviert, muß der Client einen syntaktisch korrekten Hostnamen schicken. Es wird jedoch nicht anhand der DNS-Datenbank geprüft, ob der Name auch gültig ist.

Mit der Einstellung *strikt* muß der angegebene Name zusätzlich ein FQDN und per DNS auflösbar sein.

Die Einstellungen *ja* und *strikt* können die Kommunikation mit manchen fehlerhaft konfigurierten Gegenstellen unterbinden. Von diesen Systemen werden keine E-Mails angenommen. Dies ist in erster Linie eine wirkungsvolle Maßnahme gegen Spam, kann aber in Einzelfällen zu Problemen führen.

Maximale Größe einer E-Mail Dieser Parameter legt die maximale Größe einer einzelnen E-Mail in Megabyte fest. Folgendes ist bei der Angabe zu berücksichtigen: Da ein- oder ausgehende E-Mails mit Anhängen vom E-Mail-Client kodiert werden, ist die Größe beim Versand oder Empfang um ungefähr ein Drittel größer, als ursprünglich beim Verfassen der E-Mail-Daten auf dem Client.

Absenderadresse prüfen Bei der Aktivierung dieser Option wird geprüft, ob die Maildomain des Absenders in der DNS-Datenbank existiert (A- oder MX-Record). Ist dies nicht der Fall, wird die E-Mail zurückgewiesen.

Für lokale Absender wird zusätzlich geprüft, ob die Absenderadresse auf dem Collax Server existiert. Ist dies nicht der Fall, wird die E-Mail zurückgewiesen.

Weitere Einstellungen zum Spam-SMTP-Filter können unter „Dienste → Mail und Messaging → Mail Security → Spam“ vorgenommen werden.

Die Defaultwerte kann man so belassen, es sei denn man hat Probleme beim Empfang bestimmter Emails. Dann kann man die Werte seinen Bedürfnissen entsprechend anpassen.

Menü > Dienste > Mail und Messaging > Spamfilter

Spamfilter

Spam-Inhalts-Filter Heuristik (Bayes) Reputationsdienste Spam-SMTP-Filter

Greylisting

Greylisting verwenden

Verzögerungsdauer (in Sekunden)

Maximales Alter der Einträge (in Tagen)

Zeitfenster für erneuten Versuch (in Stunden)

Anzahl der E-Mails für automatische Whitelist

Nachricht

Teergrube

Teergrube emulieren

Verzögerung Stufe 1 in Sekunden

Verzögerung Stufe 2 in Sekunden

Greylisting verwenden Durch Aktivieren dieser Option wird Greylisting aktiviert. Dabei wird jede per SMTP neu eingelieferte E-Mail von Systemen, die nicht die Berechtigung Mail Relay haben, zunächst mit einer temporären Fehlermeldung abgewiesen. Nach Ablauf einer bestimmten Sperrfrist wird die E-Mail angenommen. Damit wird verhindert, daß E-Mail von Programmen angenommen wird, die über keine Mailqueue verfügen (und damit keine richtigen Mailserver sind).

Teergrube emulieren Mit dieser Option wird die Funktion Teergrube zur zusätzlichen Abwehr von Spam-E-Mails und der Verbreitung von Würmern eingeschaltet. Durch die Aktivierung wird die Kommunikation innerhalb von zwei Verbindungsstufen, zwischen dem Collax Server und dem verbindenden SMTP-Server, verzögert.

Es ist zu beachten, daß durch diese Option der eingehende E-Mail-Server für den Zeitraum der Verzögerung von Stufe 1 und Stufe 2 blockiert wird.

Mechanismen nach der Annahme von Emails

Dieser Dialog befindet sich unter „Dienste → Mail und Messaging → Mail Security → Spam“

Spam-Inhalts-Filter

Aktivieren Sie den Spam-Inhalts-Filter

Menü > Dienste > Mail und Messaging > Spamfilter

Spamfilter

Spam-Inhalts-Filter Heuristik (Bayes) Reputationsdienste Spam-SMTP-Filter

Spam-Inhalts-Filter

Aktivieren

Automatische Aktualisierung
einschalten

Vertrauenswürdige Mail-Relays

E-Mail ist wahrscheinlich Spam

ab Schwellenwert
3: restriktiv, 8: großzügig

Markierung im Betreff der E-Mail

E-Mail ist sicher Spam

ab Schwellenwert

Aktion

Quarantäneverfahren

Automatische Aktualisierung Diese Option aktualisiert regelmäßig die Spam-Regeln für den Spam-Inhalts-Filter.

Vertrauenswürdige Mail-Relays Hier sollten die IP-Adressen der Mailserver angegeben werden, die für die eigene Domain E-Mails annehmen. Für bestimmte Tests („Received“-Zeilen im Mailheader) wird eine Liste aller Netze und Rechner benötigt, die als „vertrauenswürdig“ betrachtet werden sollen. „Vertrauenswürdig“ bedeutet dabei, daß diese Rechner nicht der Ausgangspunkt von Spam sind – es kann jedoch durchaus sein, daß diese Rechner Spam weiterleiten.

Die Liste enthält automatisch alle Rechner und Netze, die über die Gruppenrichtlinien E-Mails über dieses System weiterleiten dürfen (Berechtigung: Mail-Relay ohne Authentifizierung).

Zusätzlich müssen hier die Mailserver angegeben werden, die als MX („Mail-Exchanger“) für die Domain zuständig sind. Diese sind per DNS ermittelbar, meist sind es ein oder mehrere Mailserver beim eigenen Provider.

E-Mail ist wahrscheinlich Spam ab Schwellenwert Jede E-Mail wird nach verschiedenen Kriterien bewertet. Für jedes zutreffende Kriterium erhält die E-Mail eine Anzahl Punkte, die aufsummiert werden. Mit diesem Parameter wird festgelegt, ab welcher Punktzahl eine E-Mail als Spam behandelt wird. Ein Wert von „5“ ist die normale Einstellung. Bei diesem Wert ist die Negativerkennung schon extrem gering, die Effizienz beim Erkennen von Spam allerdings auch nicht optimal. Zunächst sollte mit einem hohen Grenzwert gestartet werden, der nach und nach heruntergesetzt wird. Durch die Auto Whitelist-Funktion verringert sich die Negativerkennung mit der Zeit zudem.

Markierung im Betreff der E-Mail Der Spamfilter legt in den Kopfzeilen einer E-Mail („Header“) einen Report über die erreichte Punktezahl und die zutreffenden Regeln ab. Durch das Ablegen im Header der Mail sieht die Mail auf den ersten Blick für den Benutzer unverändert aus. Mit Hilfe dieses Reports kann nachvollzogen werden, wie das System funktioniert und wie Grenzwerte angepaßt werden sollten (indem bei jeder fälschlich als Spam markierten E-Mail untersucht wird, welche Punktezahl sie erhalten hat).

Wird diese Option aktiviert, wird zusätzlich eine Markierung im Betreff der E-Mail eingefügt.

E-Mail ist sicher Spam ab Schwellenwert Hier wird eingestellt, was mit E-Mails geschehen soll, die als Spam erkannt wurden. Spam kann gelöscht, in einem eigenen Ordner gespeichert oder angehalten werden („Quarantäne“). In diesem Feld wird ein ganzzahliger Wert als Grenzwert eingetragen. Bleibt dieses Feld leer, werden Spam-E-Mails nicht gesondert behandelt, sondern ganz normal in das entsprechende Postfach zugestellt.

Aktion Mit der Option mit Warnung an Empfänger senden wird die E-Mail als einfacher Text zugestellt. Diese Einstellung ist notwendig, wenn verhindert werden soll, daß Benutzer oder die Mail-Applikationen die Anhänge öffnen und eventuelle Inhalte ausführen.

Durch die Aktion in Quarantäne verschieben kann die E-Mail mit weiteren Aktionen weiterverarbeitet werden.

Bei der Aktion Verwerfen wird die E-Mail sofort gelöscht, dem absendenden Mailserver wird jedoch bestätigt, daß die E-Mail zugestellt wurde. Für den Absender sieht es so aus, als ob die E-Mail zugestellt wurde.

Diese Aktion birgt die Gefahr, daß fälschlich auch erwünschte E-Mails einen hohen Punktwert bekommen und gelöscht werden („false positive“). Sie sollte daher erst aktiviert werden, wenn die festgelegten Punktgrenzen in der Praxis einige Zeit erfolgreich getestet wurden.

Quarantäneverfahren Die Aktion in der Mail-Queue behalten hält die E-Mail in der Warteschlange an. Sie muß vom Administrator explizit gelöscht oder freigegeben werden. Dazu kann er sie in der Mailqueue näher untersuchen.

Die Aktion in admin.spam IMAP-Ordner legen funktioniert ähnlich. Hier wird die E-Mail allerdings in einem Postfach gespeichert, welches von Zeit zu Zeit auf False Positives durchgesehen werden kann.

Die Aktion Weiterleitung an Postfach funktioniert so, daß die E-Mail an ein externes Postfach zur weiteren administrativen Bearbeitung zugestellt wird.

Die Aktion Zarafa Ordner funktioniert ähnlich. Hier wird die E-Mail an den Public Folder admin.spam in der Zarafa Groupware zur weiteren administrativen Bearbeitung zugestellt.

E-Mail-Adresse Hier wird der Ort der Quarantäne angegeben. Dies geschieht in Form einer E-Mail-Adresse. Diese Adresse kann einem Benutzerpostfach, einem IMAP-Ordner, oder einem IMAP-Administrationsordner auf einem E-Mail-Server zugewiesen werden kann.

Ein administrativer IMAP-Ordner für die Quarantäne kann als öffentlicher Ordner definiert werden, die Lese- und Schreibberechtigungen sollten jedoch stark eingeschränkt sein. Zusätzlich sollte dieser Ordner direkt per E-Mail erreichbar sein.

Die Adresse für die direkte Zuordnung in einen IMAP-Ordner eines Benutzers kann die Form *Userid+Ordner@domain.tld* haben. Die Voraussetzung für das Sub-Addressing mit address extensions ist, daß der Mail-Server RFC 3598 unterstützt. Auf diesem Mailserver muß zudem das p-Flag für den Ordner gesetzt sein.

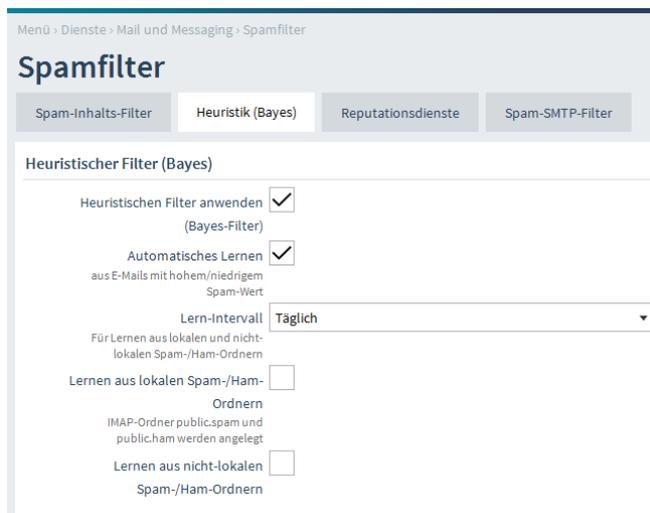
Automatisch löschen nach (Tage) Im administrativen Ordner abgelegte Dateien können nach Ablauf von den angegebenen Tagen automatisch gelöscht werden.

Administrative Rechte für IMAP-Ordner admin.spam Hier werden die Gruppen angegeben, die ausgefilterte Spam-E-Mails begutachten und verwalten sollen.

Heuristik (Bayes)

Obwohl die Bewertungen des Spamfilters recht zuverlässig sind, kann es dennoch vorkommen, daß E-Mails falsch klassifiziert werden. Ein anderer Ansatz zur Spamerkennung verwendet keinen festen Regelsatz mit einem Punktesystem, sondern versucht, über eine Wissensdatenbank eine Entscheidung zu treffen. Zum Aufbau dieser Datenbank muß der Benutzer jeweils eine bestimmte Menge an unerwünschten („Spam“) und erwünschten („Ham“) E-Mails bereitstellen. Der Vorteil dieses Verfahrens liegt darin, daß sich ein solches System den individuellen Anforderungen des Benutzers anpaßt. Der Nachteil ist, daß für die Bereitstellung der Spam/Ham-Ordner eine gewisse Disziplin erforderlich ist.

Mit dieser Option wird über den wahrscheinlichkeitsbasierten Filter eine Erkennung vorgenommen.



Automatisches Lernen Abhängig von der Bayes-Datenbank werden die E-Mails automatisch nach „Ham“ oder „Spam“ klassifiziert und in der Datenbank des Spam-Filters hinterlegt.

Lern-Intervall Hier wird das Zeitintervall für das automatische Trainieren ausgewählt. Diese Einstellung gilt für das Trainieren aus lokalen und entfernten Spam-/Ham-Ordern.

Lernen aus lokalen Spam-/Ham-Ordern Durch das Aktivieren dieser Option werden die gemeinsam nutzbaren Ordner zur Ablage von Spam- und Ham-E-Mails angelegt. In diese Ordner sollen durch Benutzer qualifizierte E-Mails abgelegt werden. Der Spamfilter lernt aus diesen Ordnern dann automatisch.

Schreibrechte für Spam/Ham-Ordner Hier werden die Gruppen angegeben, die ausgefilterte Spam-E-Mails begutachten und verwalten sollen.

Lernen aus nicht-lokalen Spam-/Ham-Ordern Mit dieser Option kann der Spamfilter mit Hilfe eines externen IMAP-Postfachs trainiert werden. Das Postfach sollte hierzu auf einem Mailserver definiert sein und zwei Ordner enthalten, die jeweils mit Ham- und mit Spam-E-Mails bestückt werden können. Der Lernvorgang geschieht durch Auslesen der E-Mails im Postfach, getrennt für Ham und Spam.

Reputationsdienste

Ein weiterer Ansatz zur Spamerkennung verwendet Reputationsdienste um dynamisch Inhalte und Absender einer Email zur Klassifizierung heranzuziehen. Die weltweit größte Reputationsdatenbank „SenderBase“ analysiert dabei den Internetverkehr in Echtzeit und liefert stets aktuelle Infos zu Gefahren aus dem Netz. Zu dem von Cisco ins Leben gerufenen Dienst, finden Sie unter www.senderbase.org weitere Informationen. Collax implementiert „SenderBase“ und kombiniert darüberhinaus eine Vielzahl an weiteren Diensten zur Vermeidung von Spam E-Mails.

Menü » Dienste » Mail und Messaging » Spamfilter

Spamfilter

Spam-Inhalts-Filter Heuristik (Bayes) Reputationsdienste Spam-SMTP-Filter

Online-Blacklists für SMTP-Reject

Blacklist verwenden
blockiert die Annahme während des SMTP-Dialogs

Vordefinierte Blacklists verwenden [DNSBL- NIX Spam](#)
 [SCBL - SpamCop Blocking List](#)

Manuell Blacklists eintragen

Online-Blacklists für Inhaltsbewertung

Blacklist verwenden
wirkt sich auf die Punktzahl aus

Verwendete Listen: [DNSBL-SPAMCOP](#)

SenderBase verwenden
Gewichtung für SenderBase-Eintrag: 50
in Prozent, zw. 10% und 200%

NIX-Spamfilter verwenden
NIX Spam-Wert: 1

Razor verwenden

DomainKeys Identified Mail (DKIM)

DKIM E-Mail-Überprüfung verwenden

Bonuspunkte für Absender in der DKIM-Whitelist: 8

Bonuspunkte für E-Mails mit einer gültigen DKIM-Signatur: 3

Sender Policy Framework (SPF)

SPF verwenden

Blacklists verwenden Wird diese Option aktiviert, prüft das System bei jeder einkommenden E-Mail, ob die einliefernde IP-Nummer in einer dieser schwarzen Listen erfaßt ist.

Vordefinierte Blacklists verwenden In dieser Liste werden die Blacklist-Server eingetragen, die abgefragt werden sollen. Die Grundkonfiguration enthält eine Liste von frei zugänglichen DNS-Blacklists. Eine Anmeldung o. ä. ist nicht notwendig, um diese Listen nutzen zu dürfen.

Manuell Blacklists eintragen Hier können weitere Blacklists manuell eingetragen werden. Bestimmte Anbieter bieten kommerzielle Blacklists oder dynamische online Blacklists, die eine Anmeldung erfordern.

Blacklists Verwenden Diese Option aktiviert die Abfrage von Spam-Block-Listen, die im DNS-System abgelegt sind. Diese Tests können die Erkennungsrate von Spam deutlich erhöhen – auf Kosten zusätzlicher Netzwerkanfragen.

Wird diese Option aktiviert, werden die „Received“-Zeilen im Mailheader ausgewertet. Für jede Station auf diesem Weg wird ermittelt, ob diese als mögliche Quelle für Spam-E-Mails bekannt ist.

Diese Option ähnelt derjenigen im Abschnitt Online-Blacklists für SMTP-Reject. Während dort allerdings die Annahme einer E-Mail verweigert wird, wird hier nur eine zusätzliche Bewertungsmöglichkeit zur Bestimmung der Spam-Punktzahl aktiviert. Dadurch wird eine E-Mail nicht zwangsläufig abgelehnt, wenn der einliefernde Mailserver auf einer Blacklist erfaßt ist.

Wenn der SMTP-Server oder der Provider bereits DNS-Blocklists auswerten, kann diese Option ohne den Verlust der Bewertungsmöglichkeit deaktiviert werden.

Die voreingestellten Blocklisten umfassen verschiedene unentgeltlich verwendbare Dienste. Diese Liste und die zugehörige Bewertung kann nicht geändert werden.

SenderBase verwenden SenderBase® ist ein weltweites Überwachungsnetzwerk für E-Mail, durch das Spam-E-Mails zuverlässig identifiziert werden können.

Gewichtung für SenderBase-Eintrag Hier kann zusätzlich eine Gewichtung zwischen 10% und 200% für den Wert eingegeben werden, welchen die E-Mail durch SenderBase® erhalten hat.

NiX-Spamfilter verwenden NiX Spam ist ein Spamfilter-Projekt der Zeitschrift iX. Es bildet Prüfsummen über den E-Mail-Body inklusive Anhänge und vergleicht diese Prüfsummen in einer laufend aktualisierten, per DNS abfragbaren Blacklist (DNSBL).

Mit dieser Option werden eingehende E-Mails per DNS auf die Platzierung innerhalb des NiX-Spamfilter geprüft.

NiX Spam-Wert Ist eine Absender-IP-Adresse einer E-Mail in der NiX Spamfilter-Datenbank gelistet, wird der hier eingetragene Wert zur Spambewertung addiert.

Razor verwenden Durch Aktivieren dieser Option wird jede E-Mail anhand der Signaturen des Razor-Onlinechecks untersucht. Eine durch Razor als Spam klassifizierte E-Mail bekommt in der SpamAssassin-Auswertung mehr Punkte.

DomainKeys Identified Mail (DKIM) DomainKeys Identified Mail (DKIM) ist ein von Yahoo entwickeltes Verfahren, E-Mails mit einer Signatur zu versehen, die es dem Empfänger ermöglicht, eindeutig festzustellen, ob eine E-Mail wirklich vom angeblichen Absender kommt. Bei der Verwendung von DKIM signiert der Absender seine E-Mails und stellt den öffentlichen Schlüssel über den TXT-Record der gleichen Domain bereit. Der Empfänger kann anschließend beim Empfang der E-Mails über die Signatur und den Schlüssel im DNS die Echtheit der E-Mail verifizieren.

DKIM E-Mail-Überprüfung verwenden Eingehende E-Mails können auf eine DKIM-Signature getestet werden.

Bonuspunkte für Absender in der DKIM-Whitelist Falls der Absender in der Whitelist vorhanden ist, werden die angegebenen Punkte von der Spam-Bewertung abgezogen.

Bonuspunkte für E-Mails mit einer gültigen DKIM-Signatur Falls die eingehende E-Mail eine gültige DKIM-Signatur enthält, werden die hier angegebenen Punkte von der Spam-Bewertung abgezogen.

Ausgehende E-Mail mit DKIM signieren Um die Vertrauenswürdigkeit der eigenen E-Mails zu erhöhen, können E-Mails mit dieser Option mit einer DKIM-Signatur ausgestattet werden.

Sender Policy Framework (SPF) verwenden Durch Aktivieren dieser Option wird bei jeder E-Mail eine Sender Policy Framework-Überprüfung durchgeführt, die das Fälschen des Absenders einer E-Mail auf SMTP-Ebene erschwert.

Spam White/Blacklist – DKIM Whitelist

Dieser Dialog befindet sich unter „Dienste → Mail und Messaging → Mail Security → Spam White-/Blacklist“

In diesem Dialog wird eine Liste von Absenderadressen verwaltet, für die keine Spamfilterung durchgeführt wird. Technisch wird zwar eine Filterung durchgeführt, der Absender erhält jedoch einen so hohen Bonus für die Spam-Bewertung, daß seine E-Mails nie als Spam klassifiziert werden.

Analog zur Whitelist wird hier eine Liste von Absenderadressen verwaltet, deren E-Mails durch eine hohe Spam-Punktezahl immer als Spam klassifiziert werden.

Ebenso wird in diesem Dialog eine Liste von Absenderadressen für DKIM verwaltet, für die keine Spamfilterung durchgeführt wird. Technisch wird zwar eine Filterung durchgeführt, der Absender erhält jedoch einen so hohen Bonus für die Spam-Bewertung, daß seine E-Mails nie als Spam klassifiziert werden.

Menü · Dienste · Mail und Messaging · Spam White/Blacklist

Spam White/Blacklist

Spamfilter-Whitelist Spamfilter-Blacklist DKIM-Whitelist

Spamfilter-Blacklist

Adressen *@spam.de

In diesem Eingabefeld werden die Absenderadressen eingetragen. Die einzelnen Adressen werden mit Leerzeichen, Zeilenumbruch oder Komma getrennt. Die beiden Teile der Adresse (Empfänger und Domain) werden als Muster verwendet. Es ist möglich, *Wildcards* zu verwenden: Ein Fragezeichen steht für ein einzelnes und ein Stern (*) für beliebig viele beliebige Zeichen (hier werden keine regulären Ausdrücke eingesetzt).