




MDaemon AntiSpam


Whitepaper

 EBERTLANG Distribution GmbH
Garbenheimer Straße 36
D-35578 Wetzlar

Tel. 06441 67 11 80
Fax 06441 67 11 8222

 Tel. 0820 00 10 36

 Tel. 044 58 65 910

 Tel. 022 21 96 170

Allgemeine Informationen zum MDaemon Mailserver finden Sie [hier](#).

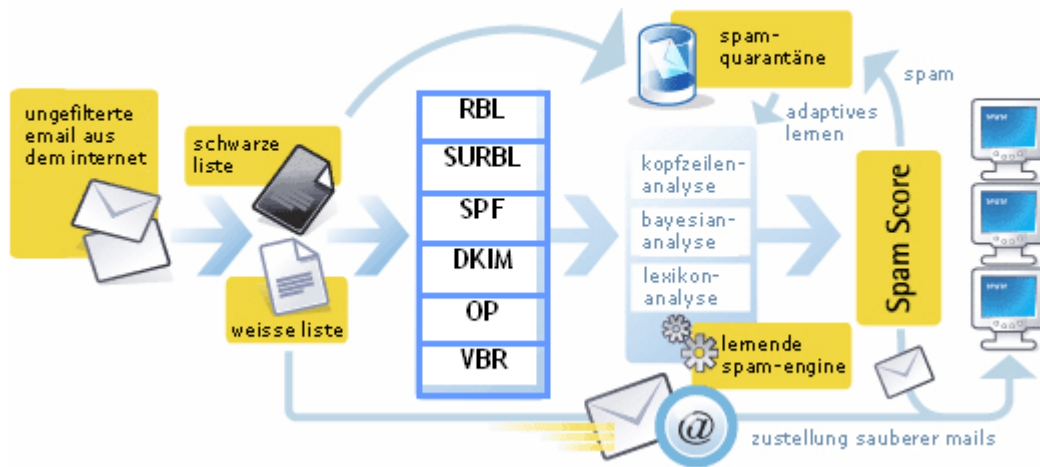
Detaillierte Informationen finden Sie [hier](#):

Eine 30-Tage-Testversion erhalten Sie [hier](#).

Inhaltsverzeichnis

Unerwünschte Werbung identifizieren, klassifizieren, eliminieren	3
Überblick	3
1. Schwarze Listen (Blacklists)	4
Schwarze Listen für DNS (DNS-BL)	4
Schwarze Listen (manuelle Pflege)	5
SURBL	5
2. Weiße Listen (Whitelisting)	6
3. Gefälschte Absender	7
Sender-Policy-Framework	7
DomainKeys und DomainKeys-Identified-Mail	7
Schutz gegen Rückstreuung	8
4. Heuristische Analyse	9
Hinweis bei Updates	12
Besonders wichtig	13
Bayes'sches Lernverfahren für POP3-Benutzer	14
5. Outbreak Protection – Schutz gegen Massenangriffe	16
Einrichten des E-Mail-Clients für den Spam-Filter bzw. das Bayes'sche Lernverfahren	18
Konfiguration bei einem IMAP-Konto	18
IMAP-Account im E-Mailclient erstellen	18
Konfiguration bei einem POP3-Konto	19
Die Wahl des eigenen Schutzes	21
Zusammenfassung	21
Beispiel-Screenshots für erkannte Spam-E-Mails	22

Unerwünschte Werbung identifizieren, klassifizieren, eliminieren



Überblick

Die Menge an Spam (unerwünschten Werbe E-Mails), die täglich in unseren E-Mail-Postfächern landet, hat absurde Größenordnungen angenommen. Glücklicherweise wurden gleichzeitig immer mehr in E-Mail-Server und E-Mail-Clients integrierbare Technologien entwickelt, um dieser Flut Herr zu werden – unglücklicherweise bietet aber keine dieser Lösungen alleine einen Schutz, den man als umfassend bezeichnen könnte. Die Voraussetzungen, die eine umfassende Anti-Spam Lösung erfüllen muss, sind nichts desto trotz sehr hoch. Zum Teil geht es hierbei darum, Spam-E-Mails zu identifizieren, obwohl diese immer stärker an das Erscheinungsbild von Nicht-Werbe E-Mails angelehnt sind, zum Teil geht es aber auch darum, legitime E-Mails nicht versehentlich über eine solche Technologie auszufiltern. Dieser Leitfaden gibt Ihnen einen Einblick in die derzeit zur Spam-Abwehr genutzten Technologien und deren Effizienz.

1. Schwarze Listen (Blacklists)

Die erste Schutztechnologie – das so genannte Blacklisting – wurde schon zu den Anfangszeiten des Internet-Marketings zwischen 1990 und 1997 entwickelt. Zu dieser Zeit war es für Spammer noch recht unüblich sich selbst zu schützen. Dementsprechend bot es sich für die Empfänger von unerwünschten Werbe-E-Mails an, einfach die Absender-E-Mailadressen, einen von Spammern genutzten IP-Adressbereich oder eine gesamte Domain zu blocken. Gegen Ende dieses Zeitraums begann der Boom des Internets und wo Unternehmen und Universitäten auf IT-Administratoren zurückgreifen konnten, die sich des Problems Spam annehmen konnten, waren immer mehr Privatanwender Spams ungeschützt ausgesetzt. Als einzige Gegenmaßnahme gegen die immer weiter wachsende Spamflut wurden die Blacklists ständig erweitert, aber diese Methode als einzige Methode der Spam-Bekämpfung erwies sich bald als relativ schwach, da die Absender von Spam-Nachrichten immer öfter Ihre eigenen E-Mail-Adressen versteckten bzw. über temporäre E-Mail-Adressen oder einfach die Mailserver von Dritten versendeten. Nichts desto trotz sind die schwarzen Listen noch heute eine Säule im Kampf gegen unerwünschte Werbung; diese sorgen dafür, dass sich andere Technologien jetzt nur noch auf die unerwünschten Nachrichten konzentrieren müssen, bei denen sich die Absender auch die Mühe gemacht haben, die Herkunft der E-Mail zu verschleiern.

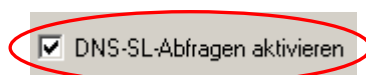
Schwarze Listen für DNS (DNS-BL)

Das System der Schwarzen Listen für DNS (abgekürzt auch DNS-BL genannt) verhindert in den meisten Fällen, dass unverlangt zugesandte Werbe-Post, sog. „Spam“, den Benutzern des eigenen Systems zugestellt werden kann. Diese Funktion kann mit verschiedenen Diensten zusammenarbeiten, die Listen von bekannten Spam- Versendern unterhalten. Diese werden immer dann abgefragt, wenn eine Gegenstelle Post beim Server einliefern will. Wenn die Gegenstelle bei einem der Dienste erfasst ist, wird die Verbindung abgewiesen. Die RBL-Datenbanken leiten ihren Namen aus dem englischen Begriff „Realtime-Blackhole“, „schwarzes Loch in Echtzeitbearbeitung“ ab.

Um den Spam-Blocker von MDAemon zu aktivieren, gehen Sie bitte wie folgt vor:

1. Klicken Sie in MDAemon auf **Sicherheit | SpamFilter**
2. Öffnen Sie das Register **DNS-SL**
3. Aktivieren Sie hier die Option **DNS-SL Abfrage aktivieren**.

Nun fragt MDAemon die MAPS/RBL/ORDB-Server nach gesperrten Gegenstellen ab. Sie können in dem Reiter **Optionen** zusätzlich noch Einstellungen in Bezug auf die Weiterverarbeitung von erkannten Spam-E-Mails vornehmen, wie z.B., dass die Nachrichten nur gekennzeichnet aber angenommen werden oder aber verschiedene Header ausgewertet werden usw.



Hinweis:

Zwar verhindert diese Funktion den Empfang von Spam recht zuverlässig, doch kann es vorkommen, dass Gegenstellen fälschlich gesperrt sind; dies führt zu Problemen, wenn Nachrichten von gesperrten IP-Adressen ohne weitere Prüfung abgewiesen werden.

Schwarze Listen (manuelle Pflege)

Um Blacklists (Schwarze Listen) in MDAemon zu pflegen, gehen Sie bitte wie folgt vor:

1. Klicken Sie in MDAemon auf **Sicherheit | Spam-Filter**
2. Öffnen Sie den Register **Schwarze Liste (nach Absender)**
3. Tragen Sie die unerwünschte Absenderadresse ein. Das Format wird automatisch angepasst.

Ein Eintrag einer Absenderadresse in dieser Schwarzen Liste stellt nicht allein sicher, dass Nachrichten von dieser Adresse immer als Spam behandelt werden. Er bewirkt lediglich, dass zu der Bewertung, die der Spam-Filter für die betreffende Nachricht ermittelt, die auf dem Reiter „Spam-Filter“ festgelegte Punktzahl hinzugerechnet wird.



SURBL

Bei SURBL (Spam URI Realtime Blocklists) handelt es sich um ein effektives Anti-Spam System, das das Filtern nicht alleine anhand der Absenderadresse steuert, stattdessen werden auch innerhalb von E-Mails angegebene Hyperlinks in die Analyse mit einbezogen. Absender von Spam-E-Mails ändern sehr oft ihre Absenderadresse, die Adresse zur eigenen Website, die innerhalb der Nachricht beworben wird, wird jedoch nur äußerst selten geändert, da dies meist mit Kosten verbunden ist. SURBL arbeitet hierbei unglaublich effektiv. 40-60% aller Spam-E-Mails werden bei einer Fehlerquote von praktisch 0% automatisch identifiziert. Diese Methode wird nicht ewig so effektiv arbeiten können, aber derzeit und im Hinblick auf die nächsten Jahre ist SURBL eine sehr gute Lösung im Kampf gegen Spam. Das SURBL-Modul wird dabei automatisch von entsprechenden Datenbanken, die permanent von Nutzern aus aller Welt mit neusten Informationen versorgt werden, und so auf dem neusten Stand bleiben, mit Updates versorgt.

Die Technologie ist bereits in MDAemon Mailserver Pro implementiert und muss nicht separat aktiviert werden!

2. Weiße Listen (Whitelisting)

Während bei den schwarzen Listen Regeln und hypothetische Analyse zusammen immer bessere Ergebnisse erzielten, wurde der Bedarf an weißen Listen dringender. Individuen und Unternehmen sollten grundsätzlich das Recht haben, auch Nachrichten empfangen zu können, die von einem Filter als Spam klassifiziert wurden (z.B. Newsletter von Lieferanten etc.). Um diese zu ermöglichen und trotzdem Spam möglichst effizient ausfiltern zu können, wurden weiße Listen eingeführt. E-Mails von Absendern, die auf diesen Listen eingetragen sind, werden grundsätzlich zugestellt, ganz gleich ob das Format eigentlich als Spam identifiziert werden würde oder nicht.

Um White Lists (Weiße Listen) in MDAemon zu pflegen, gehen Sie bitte wie folgt vor:

1. Klicken Sie in MDAemon auf **Sicherheit | Spam-Filter**
2. Öffnen Sie den Register **Weiße Liste (nach Absender)**
3. Tragen Sie die gewünschte Absenderadresse ein. Das Format wird automatisch angepasst.

Nachrichten von den Adressen auf dieser Weißen Liste sind üblicherweise kein Spam.

1. Öffnen Sie den Register **Weiße Liste (nach Empfänger)**
2. Tragen Sie die gewünschte Empfängeradresse ein. Das Format wird automatisch angepasst.

Nachrichten an die Adressen auf dieser Weißen Liste sind üblicherweise kein Spam

1. Öffnen Sie den Register **Weiße Liste (automatisch)**
2. Prüfen Sie, dass die Option **Kontakte und Datei der persönlichen Weiße Liste als Weiße Liste für den Spam-Filter** aktiviert ist

Diese Option bewirkt, dass Einträge in den Standard-Kontaktordner und der persönlichen Weißen Listen aller Benutzer als Weiße Listen für den Spam-Filter verwendet werden. MDAemon kann bei jeder eingehenden Nachricht die Weiße Liste und den Standard-Kontaktspeicher jedes Benutzers nach dem Absender der Nachricht durchsuchen. Wird der Absender bei dieser Suche gefunden, dann wird die Nachricht automatisch als Treffer auf der Weißen Liste gewertet. Falls Sie die Funktionen zur automatisch erstellten Weißen Liste nicht auf jeden einzelnen MDAemon-Benutzer anwenden wollen, können Sie sie für einzelne Benutzerkonten durch Deaktivieren der Einstellung Standard-Kontakte und Kontakte im Ordner Weiße Liste als Weiße Liste für Spam-Filter nutzen im Abschnitt Optionen des Benutzerkonten-Editors deaktivieren.

3. Gefälschte Absender

Spammer fälschen sehr oft die Absenderadressen der von ihnen versendeten Spam-Nachrichten. Diese Taktik macht es zum einen schwer, schwarze Listen zu führen, zum anderen führt es immer wieder dazu, das ganze Domains/Firmen unschuldigerweise auf solchen schwarzen Listen landen, weil die eigene Domain durch Spammer missbraucht wurde. Um das Fälschen von Absendern zu erschweren, wurden mehrere Technologien entwickelt.

Ein wichtiges Prinzip, welches von beiden Ansätzen verfolgt wird, ist, dass der Absender einer E-Mail auch die IP-Adresse des eigenen Mailservers bekannt geben muss. Dies ermöglicht es einem E-Mail-Server, der eine E-Mail von einem anderen E-Mail-Server erhält, welcher dabei vorgibt, von einer bestimmten Domain zu verschicken, die IP-Adresse des Absenders mit der veröffentlichten IP-Adresse zu vergleichen.

Dieses System würde zumindest unschuldige Individuen und Unternehmen davor bewahren, beschuldigt zu werden, Spam zu versenden. Die Tragweite hiervon sollte dabei nicht unterschätzt werden. Ein Großteil aller verschickten Spam-Nachrichten behauptet, den Ursprung bei Yahoo.com oder Hotmail.com zu haben, beide Unternehmen bestätigen jedoch, dass der Großteil dieser Nachrichten eine gefälschte Absenderdomain benutzt.

Sender-Policy-Framework

Für alle Domänen sind MX-Einträge veröffentlicht, in denen die Rechner erfasst sind, die Post für die Domänen empfangen dürfen. Aus diesen Einträgen ergibt sich aber nicht, welche Rechner für diese Domänen Post versenden dürfen. Das Sender-Policy-Framework (SPF) ermöglicht es, für Domänen „umgekehrte MXEinträge“ zu veröffentlichen, aus denen dann die Rechner ersichtlich sind, die für die Domäne Nachrichten versenden dürfen.

DomainKeys und DomainKeys-Identified-Mail

Die Systeme DomainKeys (DK) und DomainKeys Identified Mail (DKIM) prüfen E-Mail-Nachrichten und können die Nutzung gefälschter Absenderdaten (das „Spoofing“) verhindern. Sie können auch benutzt werden, um die Intaktheit eingehender Nachrichten zu prüfen und sicherzustellen, dass der Inhalt einer Nachricht nicht verändert wurde, nachdem sie den Mailserver des Absenders verlassen hat. Um diese Funktionen bereitzustellen, kommen Schlüsselpaare aus je einem öffentlichen und einem geheimen Schlüssel zum Einsatz. Abgehende Nachrichten werden mithilfe eines geheimen Schlüssels signiert, eingehende signierte Nachrichten werden anhand des öffentlichen Schlüssels des Absenders geprüft, der über den DNS-Server des Absenders abrufbar sein muss.

Um den Schutz gegen gefälschte Absender zu aktivieren, gehen Sie bitte wie folgt vor:

1. Klicken Sie im Menü auf **Sicherheit | Sicherheitseinstellungen**
2. Klicken Sie auf den Register **DKIM-Prüfung**
3. Aktivieren Sie die Option **Mithilfe von DomainKeys erstellte Signaturen prüfen** und **Mithilfe von DomainKeys-Identified-Mail (DKIM) erstellte Signaturen prüfen**
4. Klicken Sie auf den Reiter **SPF & Sender-ID**
5. Aktivieren Sie die Option **Host des Absenders über SPF prüfen**

Informationen zum Signieren abgehende Nachrichten über DomainKeys finden Sie hier:

<http://www.altn.com/Support/KnowledgeBase/KnowledgeBaseResults/?Number=KBA-02067>

Schutz gegen Rückstreuung

Als „Rückstreuung“ bezeichnet man Antworten auf E-Mail-Nachrichten, die bei Benutzern des lokalen Systems eingehen, obwohl diese Benutzer die Ursprungsnachrichten gar nicht versendet hatten. Rückstreuung tritt auf, wenn Spam oder durch Viren versandte Nachrichten einen „Antwort-Pfad“ mit gefälschter Absenderadresse enthalten. Wird eine solche Nachricht durch den Server eines Empfängers abgewiesen, oder hat der Empfänger eine Abwesenheitsmeldung aktiviert, so wird die jeweilige Antwortnachricht an die gefälschte Adresse gesandt. Dies kann zu zahlreichen falschen Statusnachrichten und Nachrichten von Auto-Beantwortern führen, die die Postfächer der Benutzer belegen. Spam-Versender und Viren-Programmierer nutzen diesen Umstand bisweilen gezielt aus, um Denial-of-Service-Angriffe gegen E-Mail-Server durchzuführen; sie lösen dazu gezielt eine Flut von Nachrichten aus, die von Servern weltweit ausgeht.

Die Lösung, die MDAemon bietet Um die Rückstreuung zu bekämpfen, enthält MDAemon in Version 9.6 eine Funktion zum Schutz gegen Rückstreuung. Sie bewirkt, dass Statusnachrichten und Nachrichten von Auto-Beantwortern nur dann an die Benutzer weitergeleitet werden, wenn die Benutzer die Ursprungsnachrichten selbst versandt haben. Dazu dient ein Hashverfahren mit geheimem Schlüssel, das einen bestimmten uhrzeitabhängigen Code in den „Antwort-Pfad“ der abgehenden Nachrichten einfügt. Tritt bei der Zustellung einer solchen Nachricht ein Problem auf, und wird sie zurück geleitet, oder geht eine automatisch erzeugte Antwort mit dem Antwort-Pfad `mailerdaemon@...` oder NULL, so erkennt MDAemon den vorher eingefügten Code und stellt dadurch fest, dass es sich um eine legitime Antwort auf eine Nachricht handelt, die tatsächlich von einem lokalen Benutzerkonto aus versandt wurde. Enthält die Adresse den besonderen Code nicht, oder ist der Code mindestens sieben Tage alt, kann MDAemon die Nachricht als ungültig behandeln und abweisen.

Um den Schutz gegen Rückstreuung zu aktivieren, gehen Sie bitte wie folgt vor:

1. Klicken Sie im Menü auf **Sicherheit | Sicherheitseinstellungen**
2. Wechseln Sie in den Register **Schutz gegen Rückstreuung**
3. Aktivieren Sie die Option **Schutz gegen Rückstreuung aktivieren**

Diese Funktion schützt die Benutzer mithilfe von BATV gegen "Rückstreuung".

Rückstreuung tritt auf, wenn Spam oder durch Viren versandte Nachrichten eine gefälschte Adresse als Absender oder Antwortpfad enthalten. Solche Nachrichten können tausende falsche Nachrichten über Zustellfehler, Abwesenheitsnachrichten, Nachrichten von Auto-Beantwortern und andere auslösen, die den Posteingang blockieren.

Schutz gegen Rückstreuung aktivieren

Der Schutz gegen Rückstreuung implementiert die Technik „Bounce Address Tag Validation“ (kurz BATV, übersetzt Gültigkeitsprüfung von Adressen bei zurücklaufenden Nachrichten durch Tags).

Nähere Informationen über BATV sind verfügbar unter:

<http://www.mipassoc.org/batv>

4. Heuristische Analyse

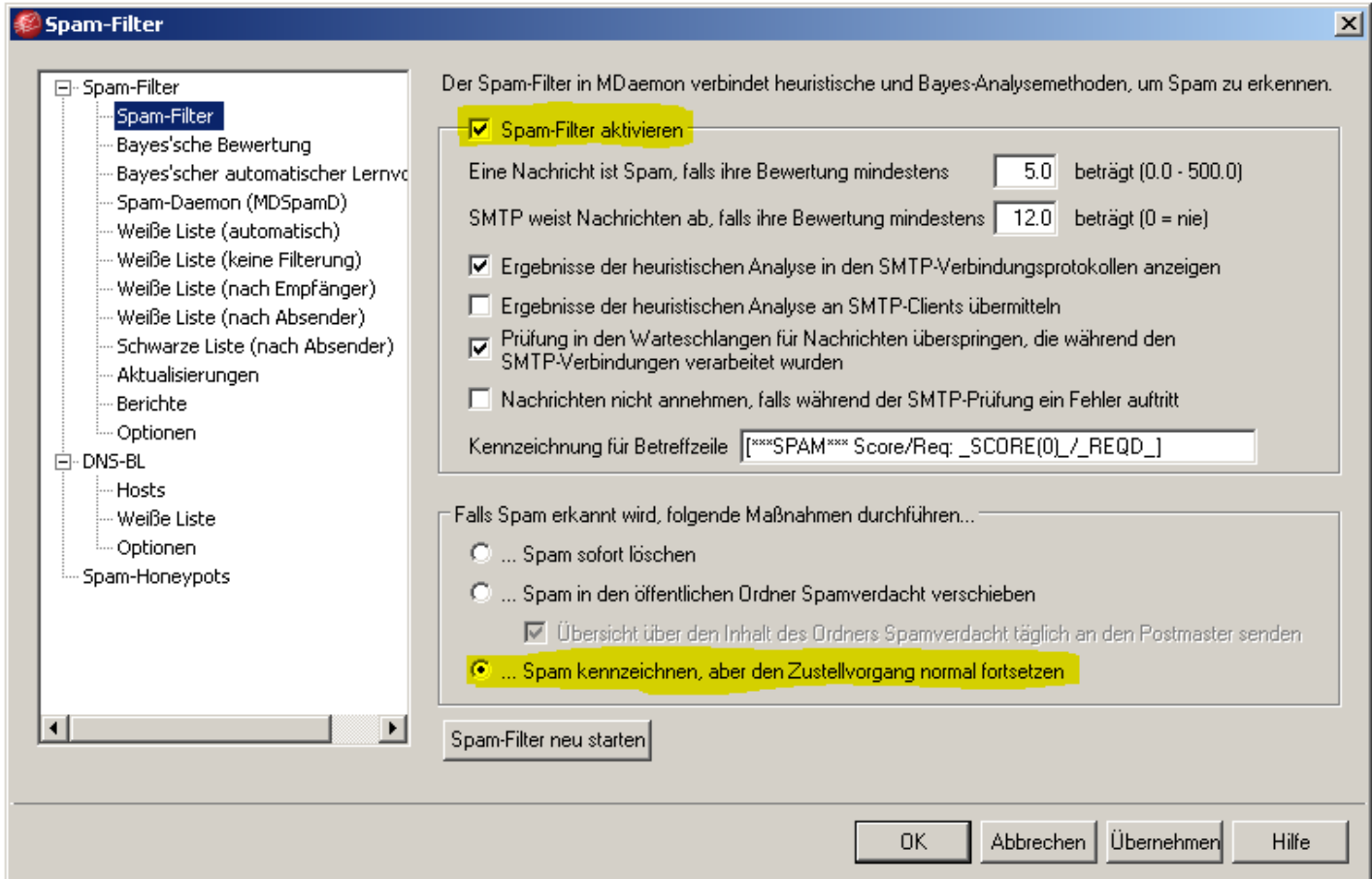
Für einen Menschen ist es recht einfach festzustellen, ob eine unerwünschte Nachricht den regelbasierten Filter passiert hat und es ist umso überraschender festzustellen, dass Computer dies bei weitem nicht so einfach bewerkstelligen können, aber die Entwicklung in diesem Bereich der Informationstechnologie ist lange nicht so zügig fortgeschritten, wie noch in den 80er Jahren prognostiziert. Ungeachtet der intensiven Forschung auf dem Bereich der Interpretation von Text und Sprache, neutralen Netzen oder allgemeiner Statistik sind noch die Ergebnisse der besten Programme noch immer nicht wirklich mit denen eines Menschen vergleichbar.

Die Suche nach einer Möglichkeit, wie ein Mensch ein Gesamtbild einer Nachricht beurteilen zu können, führte zu einer Technik, die nahezu so effektiv – wenn nicht sogar effektiver – ist, als ein Mensch. Eine der wichtigsten Methoden hierbei ist die direkte Implementierung einer statistischen hypothetischen Analyse. Buchstaben, Wörter, Erscheinungsbild, Betreff und alle anderen Komponenten einer E-Mail-Nachricht müssen sich zwischen normalen und unerwünschten E-Mails unterscheiden, wenn es einem Menschen möglich ist, E-Mails entsprechend zu klassifizieren, ohne diese komplett zu lesen. Basierend auf dieser Erkenntnis wurde die so genannte Bayesian Filter-Technologie entwickelt. Werden als solche identifizierte Spam-Nachrichten nach statistischen Gesichtspunkten analysiert, tauchen diverse Merkmale auf, die bei verdächtigen E-Mails statistisch getestet werden können, um dann entscheiden zu können, ob es sich dabei um eine normale oder eine Spam-Nachricht handelt.

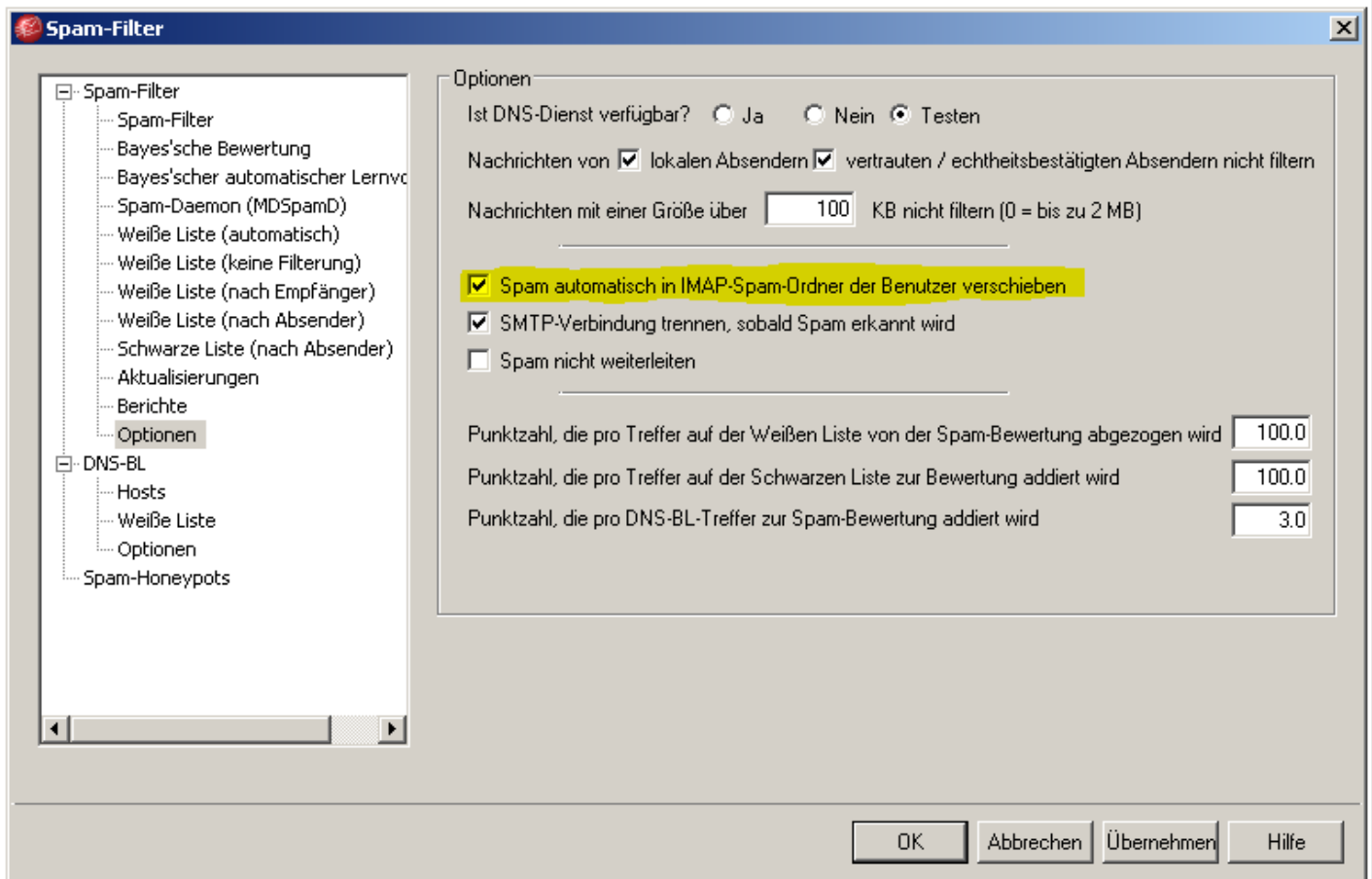
Einer der interessantesten Aspekte dieses statistischen Schutzes ist die Möglichkeit, Feedback zu geben. Erhält man eine Spam-Nachricht, die die Filter passieren konnte, hat man die Möglichkeit, diese als Spam markiert an den Filter zurückzusenden, was dann dazu führt, dass diese Information bei der zukünftigen Beurteilung von Nachrichten durch den Filter berücksichtigt wird. Dieses Verfahren erlaubt es Anti-Spam Lösungen, sich jetzt auch zügig auf neue Arten von Spam einzustellen. Diesen Schutzmechanismus auszuhebeln erfordert nun schon deutlich mehr Mühe.

Der Spam-Filter von MDAemon Pro

1. Wählen Sie im MDAemon-Menü **Sicherheit | Spam-Filter**.
2. Treffen Sie im Register **Spam-Filter** die gewünschte Option wie MDAemon Nachrichten, die als Spam erkannt wurden behandeln soll:



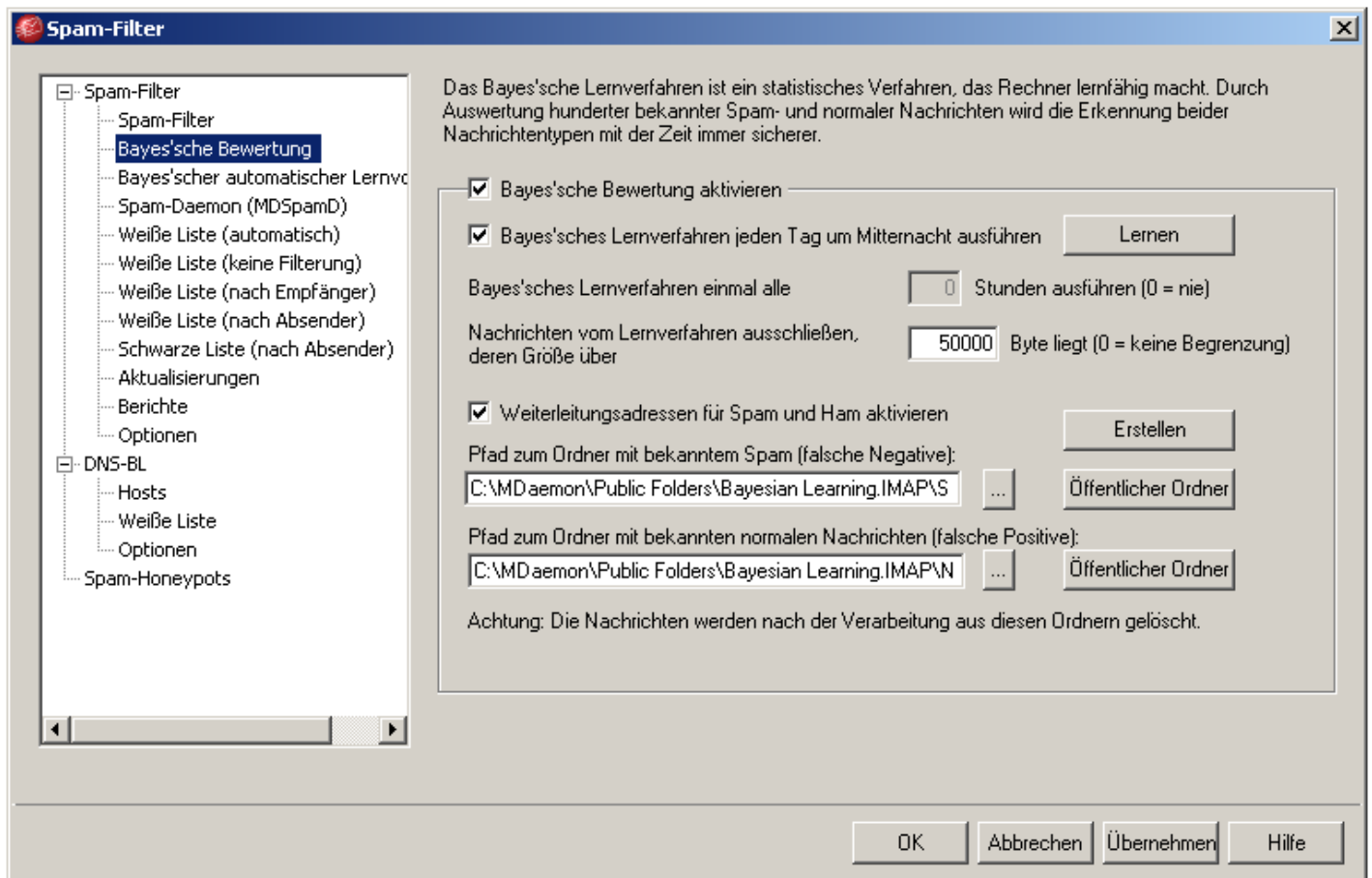
3. Wechseln Sie in den Reiter **Optionen**



Die Option *Spam automatisch in den IMAP-Spam-Ordner des Benutzer verschieben*, aktivieren Sie bitte **nur**, wenn die E-Mail-Clients die Post über **IMAP4** abrufen oder die Benutzer WorldClient verwenden. Die spamverseuchten Nachrichten werden nun automatisch in den Ordner **Junk-E-Mail** verschoben.

Bei Verwendung von **POP3-Konten** sollten Sie diese Option **deaktivieren**.

Im Register **Bayes'sche Bewertung** wird das Bayes'sche Lernverfahren aktiviert:



Wir empfehlen Ihnen die Nutzung des Bayes'schen Lernverfahren, um den Spam-Filter zu trainieren.

Hinweis bei Updates:

Während der Aktualisierung einer früheren Version fragt die Installationsroutine nach, ob das Bayes'sche Lernverfahren automatisch konfiguriert werden soll. Diese Abfrage erfolgt aber nur, falls vorher noch keine Ordner für das Bayes'sche Lernverfahren angelegt worden waren. Wird die Abfrage bejaht, so erzeugt MDaemon eine Standard-Ordnerstruktur aus öffentlichen IMAP-Ordnern und aktiviert das Lernverfahren. Dabei wird nötigenfalls zugleich die Unterstützung für öffentliche IMAP-Ordner aktiviert.

Das Bayes'sche Lernverfahren ist ein mathematisches Verfahren, durch das Rechner in gewissem Umfang lernfähig werden. Software, die nach dem Bayes'schen Verfahren arbeitet, kann Muster erkennen, wenn sie immer wieder Nachrichten verarbeitet, von denen bekannt ist, dass es sich bei ihnen entweder um Spam oder nicht um Spam handelt. Mit der Zeit werden die Bewertungen, die anhand des Bayes'schen Lernverfahrens vergeben werden, immer treffsicherer.

MDaemon führt mehrmals täglich das Lernprogramm SA-Learn aus. Das Programm untersucht die Inhalte je eines Ordners mit als Spam bekannten und als normalen Nachrichten bekannten Elementen. Diese Ordner und ihre Inhalte muss der Systemverwalter selbst bereitstellen. Sobald genug Nachrichten in dieser Weise ausgewertet werden, beginnt der heuristische Programmkernel des Spam-Filters, unter Anwendung des Bayes'schen Verfahrens, mit der Bewertung eingehender Nachrichten.

Da die Ergebnisse, die nach dem Bayes'schen Verfahren ermittelt werden, mit der Zeit immer genauer werden, erreicht das System auch eine immer höhere Treffsicherheit bei der Bewertung der Nachrichten.

MDaemon erzeugt folgende Struktur von öffentlichen IMAP-Ordnern und konfiguriert MDAemon so, dass die Ordner genutzt werden:

<Bayesian Learning> - IMAP-Hauptordner
<Bayesian Learning\\Spam> - Ordner für falsche negative Treffer
<Bayesian Learning\\Non-Spam> - Ordner für falsche positive Treffer

Die Berechtigungen für diese Ordner werden grundsätzlich so eingerichtet, dass nur lokale Benutzer lokaler Domänen auf sie zugreifen können, und dass ihre Rechte außerdem auf das Durchsuchen und Erstellen ("Lookup" und "Insert") beschränkt sind. Der Postmaster erhält die Rechte Durchsuchen, Lesen, Erstellen und Löschen ("Lookup", "Read", "Insert" und "Delete").

Besonders wichtig:

Das Lernprogramm hängt von dem Urteil des Systemverwalters ab. SA-Learn verlässt sich darauf, dass der Systemverwalter das Programm nur mit Nachrichten versorgt, die tatsächlich Spam und normale Nachrichten sind, und dass er diese Nachrichten nach den beiden Kategorien richtig einteilt. Er prüft diese Entscheidung des Systemverwalters nicht, sondern handelt nur danach.

Der Systemverwalter sollte die Benutzer veranlassen, Kopien aller bei ihnen eingegangenen falschen negativen und falschen positiven Nachrichten in diese Ordner zu kopieren. MDAemon verarbeitet diese mithilfe des Lernprogramms und löscht die Nachrichten anschließend.

Die dauerhafte Versorgung des Bayes'schen Systems mit normalen Nachrichten ("HAM"), die das System in den Lernvorgang einbeziehen kann, stellt oft ein Problem dar. Vielen Benutzern ist es nicht bewusst, dass es für das Lernverfahren genauso wichtig ist, neben Spam-Nachrichten auch immer Muster legitimer Nachrichten zu erhalten.

Aus diesem Grund wurde der Reiter Weiße Liste (autom.) im Menü des Spam-Filters um eine Einstellung erweitert, welche die Versorgung des Bayes'schen Systems mit als legitim bekannten Nachrichten automatisieren soll. Die Einstellung "Bayes-Datenbank durch Kopien von Nachrichten auf der Weißen Liste aktualisieren" bewirkt, dass MDAemon Kopien aller Nachrichten, die bestimmten Kriterien entsprechen, in den Lernordner für HAM (normale Post) kopiert.

Eine Nachricht erfüllt diese Kriterien entweder, wenn sie als eingehende Nachricht an einen lokalen Benutzer gerichtet ist und von einem Absender stammt, der im WorldClient-Adressbuch des Empfängers erfasst ist, oder wenn sie als abgehende Nachricht von einem lokalen Benutzer an einen Empfänger gerichtet ist, der im WorldClient-Adressbuch des Absenders enthalten ist. Da diese Kriterien nur geprüft werden können, wenn das Adressbuch als Quelle für die Weiße Liste eingerichtet ist, muss auch die zugehörige Einstellung aktiv sein, damit die geschilderte Vereinfachung wirksam wird.

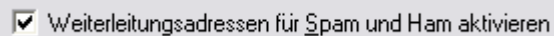
Falls Nachrichten von lokalen Absendern nicht von diesem automatischen Prozess erfasst werden sollen, kann dies durch Bearbeiten des folgenden Eintrags in der Datei MDAemon.ini erreicht werden:

```
[SpamFilter]
UpdateHamFolderOutbound=No (Nein, Vorgabe ist "Yes", Ja)
```

Erfüllt eine Nachricht die dargestellten Kriterien, so wird sie automatisch in den Lernordner für HAM kopiert, und zwar auch dann, wenn das Bayes'sche automatische Lernverfahren selbst deaktiviert ist. So ist sicher gestellt, dass das Lernverfahren, wenn es aktiviert wird, oder wenn ein Lernvorgang von Hand ausgelöst wird, immer eine ausreichend große Datenbasis normaler Nachrichten zur Verfügung hat.

Bayes'sches Lernverfahren für POP3-Benutzer

Der Konfigurationsdialog für das Bayes'sche Lernverfahren im Menü des Spam-Filters wurde um eine Option erweitert. Sie gestattet den **POP3-Benutzern** die Weiterleitung von Nachrichten an **Spam-** und **Ham-Ordner** zum Zwecke des automatischen Lernens.



Ist diese Option aktiv, so verarbeitet MDAemon Post an die Adressen SpamLearn@domaene.de und HamLearn@domaene.de

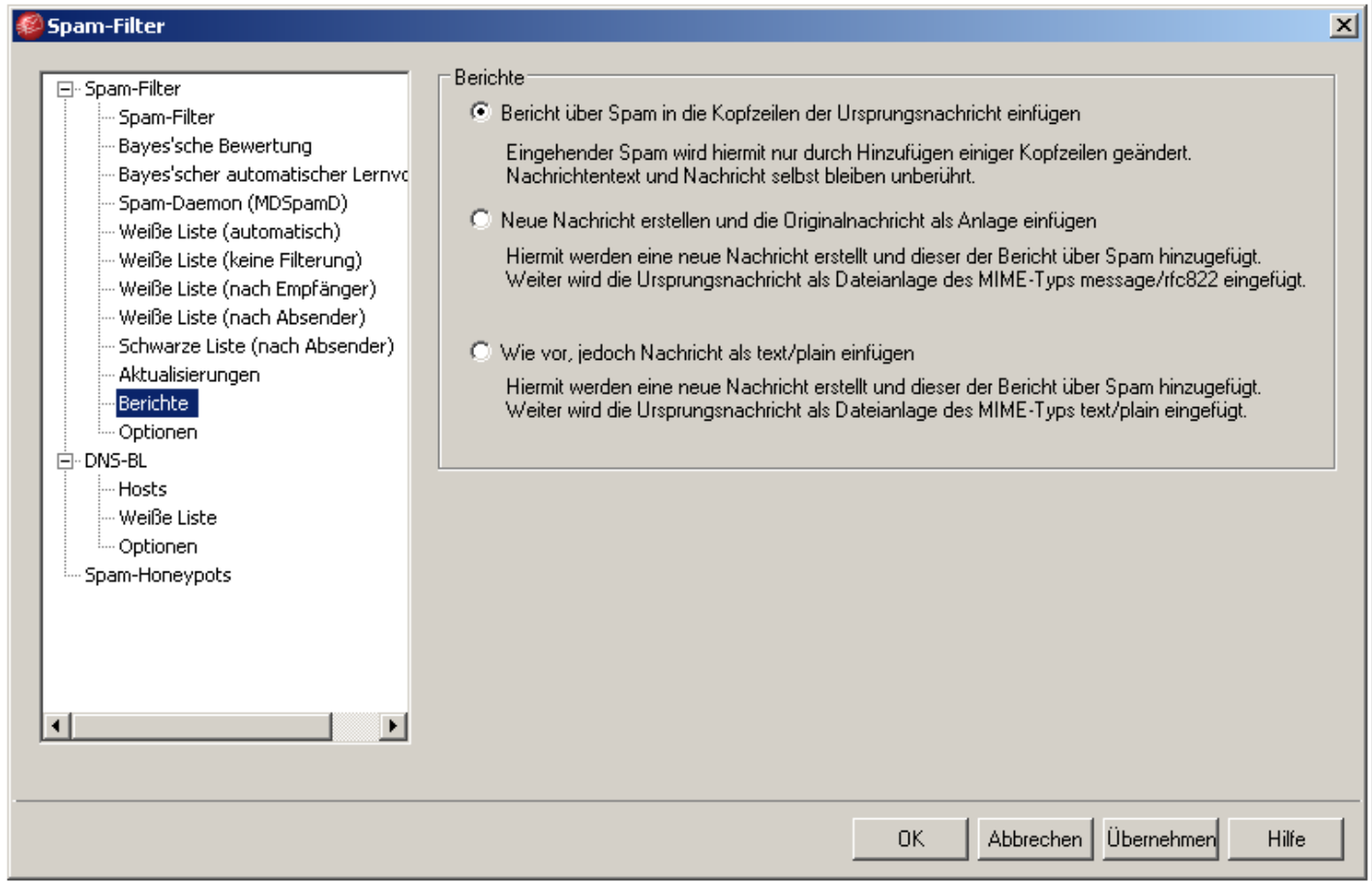
Nachrichten an diese Adressen dürfen **nur durch SMTP-Verbindungen** mit Echtheitsbestätigung über **SMTP-AUTH** übertragen werden. MDAemon erwartet die weitergeleiteten Nachrichten außerdem **als Dateianlage** des MIME-Typs message/rfc822. MDAemon verarbeitet nur solche Nachrichten an die beiden Adressen, die beiden genannten Kriterien erfüllen.

Die Zieladressen können durch Bearbeiten des folgenden Eintrags in der Datei CFILTER.INI geändert werden:

```
[SpamFilter]
SpamLearnAddress=SpamLearn@
HamLearnAddress=HamLearn@
```

Beachten Sie bitte, dass das letzte Zeichen des Eintrags ein at-Zeichen "@" sein muss!

Treffen Sie in dem Reiter Berichte die gewünschte Option zu den **Berichten** des Spam-Filters:



5. Outbreak Protection – Schutz gegen Massenangriffe

Der Schutz gegen Massenangriffe ist eine bahnbrechende Technik, die eine durch MDAemon versorgte E-Mail-Infrastruktur automatisch und binnen Minuten nach Beginn eines Massenangriffs gegen Spam, Viren, und Phishing automatisch und vorausschauend schützen kann. Diese Schutzfunktion benötigt keine Heuristik-Regeln, keine Inhaltsfilterung, und keine Aktualisierungen für Signaturen. Stattdessen stützt sie sich auf die Analyse bestimmter Schemata, die in Zusammenhang mit E-Mail-Übermittlungen erkannt und mit Vergleichsdaten abgeglichen werden. Diese Vergleichsdaten stammen aus der Analyse von Millionen von E-Mail-Nachrichten, die täglich von Tausenden Spam-Fallen weltweit gesammelt und ausgewertet werden. Die Analyse, die aufgrund dieses Abgleichs erstellt wird, kann Massenangriffe fast gleich zum Zeitpunkt ihres Beginns und damit wesentlich schneller erkennen, als es traditionelle Filter und Signatur-gestützte Lösungen könnten.

Diese Schutzfunktion von SecurityPlus nimmt die Nachrichteninhalte überhaupt nicht zur Kenntnis; sie stützt sich stattdessen auf eine mathematische Auswertung der Nachrichtenstruktur und der Eigenheiten der Nachrichtenzustellung über SMTP. Eine streng regelgebundene Auswertung des Nachrichteninhalts findet nicht statt. Die Technik kann daher auch nicht durch Seed-Texte, gut durchdachte absichtlich verfälschte Schreibweisen, Taktiken der Sozialkonstruktion (des "Social Engineerings"), Sprachbarrieren oder Abweichungen aufgrund verschiedener Kodierungen umgangen werden.

Der Schutz wird in Echtzeit gewährleistet, und er wird innerhalb von Minuten, oft sogar Sekunden, nach dem Beginn eines neuen Massenangriffs wirksam. Gerade bei Viren ist dieses Schutzniveau von entscheidender Bedeutung, da die Hersteller herkömmlicher AntiVirus-Software nach einem neuen Massenangriff oftmals mehrere Stunden brauchen, um aktualisierte Signaturen zu prüfen und zu verteilen, und da es oft noch länger dauert, bis dann die Aktualisierungen auch im Wirkbetrieb eingesetzt werden.

Während dieser Zeit sind MDAemon-Nutzer ohne SecurityPlus gefährdet. Bei Spam-Nachrichten bietet sich ein ähnliches Bild – es dauert oft einige Zeit und kostet einigen Aufwand, bis Spam analysiert ist und aus dem Analyseergebnis wirksame Filterregeln für herkömmliche heuristische Systeme entwickelt sind.

Die Schutzfunktion ergänzt die bestehenden signaturgestützten AntiVirus-Funktionen, die auf Kaspersky-Technik basieren. Sie stellen so eine weitere Schutzschicht für den Schutz gegen Viren bereit. Darüber hinaus umfasst die Schutzfunktion Anti-Spam- und Anti-Phishing-Funktionen, die ebenfalls in Echtzeit arbeiten. SecurityPlus ist nahtlos in die Benutzeroberfläche und die SMTP-Verarbeitung von MDAemon eingebunden und nutzt dazu die SDK- und Plugin-Schnittstellen.

Um die neue Technologie zu nutzen, muss MDAemon SecurityPlus 3.x installiert werden.

Um den Schutz gegen Massenangriffe zu aktivieren, gehen Sie bitte wie folgt vor:

1. Klicken Sie in MDAemon auf **Sicherheit | Outbreak Protection**
2. Aktivieren Sie die Option **Outbreak Protection aktivieren**

Wir empfehlen folgende Einstellung zu treffen:

Outbreak Protection ✖

Outbreak Protection, der Schutz gegen Ausbrüche und Massenangriffe (kurz "OP"), ist eine Technik für die Erkennung von Ausbrüchen und Massenangriffen in Echtzeit. Sie kann Viren, Spam und bestimmte anstößige sowie rechtswidrige Inhalte innerhalb der ersten Minuten eines Ausbruchs erkennen und abweisen.

Outbreak Protection aktivieren

Viren werden in Echtzeit abgewiesen in Quarantäne gegeben
 Nachrichten in Quarantäne werden im Quarantäne-Ordner von SecurityPlus abgelegt.

Spam wird in Echtzeit abgewiesen angenommen und später gefiltert Bewertung
 Durch IWF erfasste Inhalte werden in Echtzeit abgewiesen angenommen und später gefiltert Bewertung

Beim Abweisen von Spam auch Nachrichten abweisen, die als "Massensendungen" eingestuft wurden

Verbindungen zur Nachrichtenübermittlung trennen, nachdem Viren, Spam oder durch IWF erfasste Inhalte abgewiesen wurden

OP-Aktivität im Plugin-Protokoll von MDaemon protokollieren

Ausnahmen

Echtheitsbestätigte SMTP-Verbindungen sind von OP-Verarbeitung ausgenommen

SMTP-Verbindungen von vertrauten IPs sind von OP-Verarbeitung ausgenommen

Durch SPF/Sender-ID/DK/DKIM erfolgreich geprüfte Nachrichten sind von OP-Verarbeitung ausgenommen

Adressen der Spam-Fallen und Adressen aus der Weißen Liste des Spam-Filters sind von OP-Verarbeitung ausgenommen

Für die Weiße Liste der OP werden statt der Daten aus den Kopfzeilen der Nachricht die Daten aus dem SMTP-Umschlag genutzt.

Falsche positive & falsche negative Treffer

Die Erkennungs- und Einstufungsverfahren werden ständig verfeinert.

Sie können irrtümlich als Spam erkannte Nachrichten an spamfp@altn.com und irrtümlich nicht als Spam erkannte Nachrichten an spamfn@altn.com senden. Sie können irrtümlich als vireniniziert erkannte Nachrichten an virusfp@altn.com und irrtümlich nicht als vireniniziert erkannte Nachrichten an virusfn@altn.com senden.

Bitte senden Sie dabei die Ursprungsnachrichten als MIME-Dateianlagen. Leiten Sie die Nachrichten nicht einfach weiter, weil dadurch wichtige Daten aus den Kopfzeilen verloren gehen.

Einrichten des E-Mail-Clients für den Spam-Filter bzw. das Bayes'sche Lernverfahren

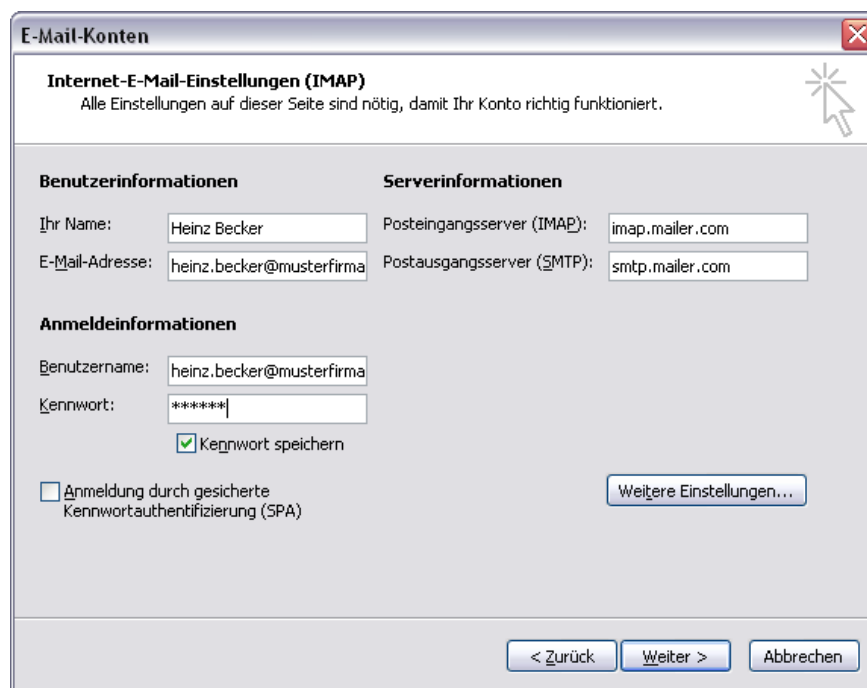
Konfiguration bei einem IMAP-Konto

Nachfolgend wird beschrieben, wie Ihr E-Mailclient für die Verwendung des Spam-Filters bzw. des Bayes'schen Lernverfahrens konfiguriert werden muss. In diesem Beispiel wird ein IMAP4-Account verwendet und die falsch negativen E-Mails (Nachrichten, die als Spam hätten erkannt werden müssen aber nicht erkannt wurden) und die falsch positiven E-Mails (Nachrichten, die fälschlich als Spam gekennzeichnet wurden und normale, gute E-Mails) müssen manuell von den Benutzern in die entsprechenden Lernordner verschoben werden.

IMAP-Account im E-Mailclient erstellen

Falls noch nicht geschehen, müssen Sie zunächst ein IMAP-Account in dem E-Mail-Client einrichten. Als Beispiel wird hier Outlook 2003 verwendet und das Benutzerkonto existiert bereits im MDAemon Mailserver.

Klicken Sie in Outlook auf **Extras | E-Mail-Konten**. Wählen Sie die Option **Ein neues E-Mail-Konto hinzufügen** und klicken Sie auf **Weiter**. Wählen Sie als Servertyp **IMAP** aus und klicken Sie auf **Weiter**. Tragen Sie in der folgenden Maske die **Benutzer-, Server- und Anmeldeinformationen** ein.



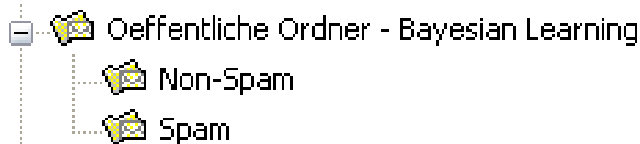
The screenshot shows the 'E-Mail-Konten' dialog box in Outlook 2003. The title bar reads 'E-Mail-Konten'. Below the title bar, there is a section titled 'Internet-E-Mail-Einstellungen (IMAP)' with a sub-note: 'Alle Einstellungen auf dieser Seite sind nötig, damit Ihr Konto richtig funktioniert.' The dialog is divided into three main sections: 'Benutzerinformationen', 'Serverinformationen', and 'Anmeldeinformationen'. In 'Benutzerinformationen', 'Ihr Name' is 'Heinz Becker' and 'E-Mail-Adresse' is 'heinz.becker@musterfirma'. In 'Serverinformationen', 'Posteingangsserver (IMAP)' is 'imap.mailer.com' and 'Postausgangsserver (SMTP)' is 'smtp.mailer.com'. In 'Anmeldeinformationen', 'Benutzername' is 'heinz.becker@musterfirma' and 'Kennwort' is masked with '*****'. There is a checked checkbox for 'Kennwort speichern' and an unchecked checkbox for 'Anmeldung durch gesicherte Kennwortauthentifizierung (SPA)'. A 'Weitere Einstellungen...' button is located to the right of the 'Anmeldung...' checkbox. At the bottom of the dialog, there are three buttons: '< Zurück', 'Weiter >', and 'Abbrechen'.

Klicken Sie anschliessend auf **Weiter** und **Fertigstellen**. Das neue Konto erscheint dann automatisch in Outlook. Überprüfen Sie bitte, ob der Empfang und Versand korrekt funktioniert.

Um nun die beiden Lern-Ordner des Bayes-Verfahren in Outlook zu abonnieren gehen Sie wie folgt vor:

1. Klicken Sie in Outlook **Extras | IMAP-Ordner**.
2. Klicken Sie den Button **Abfrage**.
3. **Markieren** Sie die Lernordner und klicken Sie **Abonnieren**.
4. Klicken Sie anschließend **Übernehmen** und **OK**.

Nun sind die beiden Lernordner sichtbar und der Benutzer kann die entsprechenden E-Mails per Drag&Drop verschieben.



Konfiguration bei einem POP3-Konto

Nachfolgend wird beschrieben, wie Ihr E-Mailclient für die Verwendung des Spam-Filters bzw. des Bayes'schen Lernverfahrens konfiguriert werden muss. In diesem Beispiel wird ein POP3-Account verwendet und die falsch negativen E-Mails (Nachrichten, die als Spam hätten erkannt werden müssen aber nicht erkannt wurden) und die falsch positiven E-Mails (Nachrichten, die fälschlich als Spam gekennzeichnet wurden und normale, gute E-Mails) müssen wie in diesem Beispiel beschrieben an das jeweilige MDAemon-Konto **SpamLearn@** bzw. **HamLearn@** gesendet werden.

POP3-Account im E-Mailclient erstellen:

Falls noch nicht geschehen, müssen Sie zunächst ein POP3-Account in dem E-Mail-Client einrichten. Als Beispiel wird hier Outlook 2003 verwendet und das Benutzerkonto existiert bereits im MDAemon Mailserver.

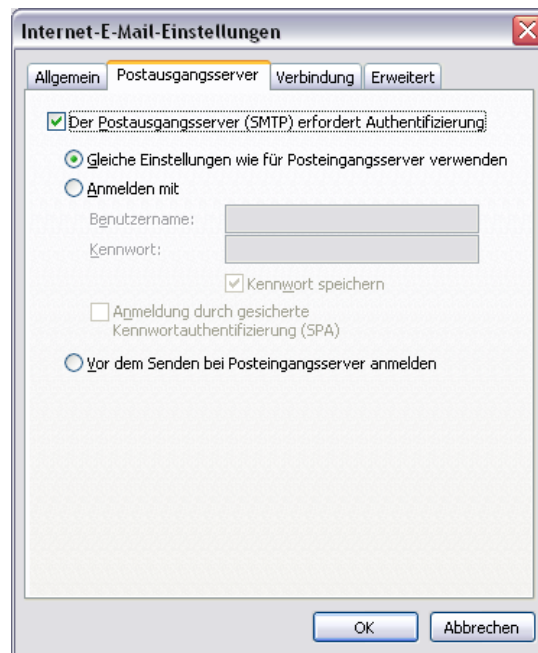
Klicken Sie in Outlook auf **Extras | E-Mail-Konten...** Wählen Sie die Option **Ein neues E-Mail-Konto hinzufügen** und klicken Sie auf **Weiter**. Wählen Sie als Servertyp **POP3** aus und klicken Sie auf **Weiter**. Tragen Sie in der folgenden Maske die **Benutzer**, **Server-** und **Anmeldeinformationen** ein.

Beispiel:

The screenshot shows the 'E-Mail-Konten' dialog box with the following fields and options:

- Internet-E-Mail-Einstellungen (POP3)**: Alle Einstellungen auf dieser Seite sind nötig, damit Ihr Konto richtig funktioniert.
- Benutzerinformationen**:
 - Ihr Name:
 - E-Mail-Adresse:
- Serverinformationen**:
 - Posteingangsserver (POP3):
 - Postausgangsserver (SMTP):
- Anmeldeinformationen**:
 - Benutzername:
 - Kennwort:
 - Kennwort speichern
 - Anmeldung durch gesicherte Kennwortauthentifizierung (SPA)
- Einstellungen testen**:
 - Wir empfehlen Ihnen, das neue Konto nach dem Eingeben aller Informationen in diesem Fenster zu testen, indem Sie auf die Schaltfläche unten klicken (Netzwerkverbindung erforderlich).
 -
 -
- Navigation:

Klicken Sie auf den Button **Weitere Einstellungen** und aktivieren Sie im Reiter **Postausgangsserver** die SMTP-Authentifizierung am Postausgangsserver. Klicken Sie **OK**.



Klicken Sie nun auf **Weiter** und **Fertigstellen**. Das neue Konto erscheint dann automatisch in Outlook. Überprüfen Sie bitte, ob der Empfang und Versand korrekt funktioniert.

Um das Bayes'sche Lernverfahren zu trainieren müssen die Benutzer nun die falsch negativen E-Mails (Nachrichten, die als Spam hätten erkannt werden müssen aber nicht erkannt wurden) an die E-Mailadresse **SpamLearn@** senden.

Die falsch positiven E-Mails (Nachrichten, die fälschlich als Spam gekennzeichnet wurden und normale, gute E-Mails) werden an die E-Mailadresse **HamLearn@** gesendet.

Beispiele:

Sie haben eine E-Mail erhalten, die definitiv Spam ist, aber nicht als solche erkannt wurde. Senden Sie nun die E-Mail als Dateianlage.

1. Klicken Sie in Outlook auf **Neu**, um eine neue E-Mail zu erstellen.
2. Verschieben Sie nun die **betroffene E-Mail** z.B. vom Posteingang per **Drag&Drop** in die neue E-Mail.
3. Geben Sie als Empfänger das Konto SpamLearn@IhreDomain.de an.
4. **Versenden** Sie die E-Mail und das Bayes'sche Lernverfahren wird diese E-Mail in der nächsten Lern-Phase mit einbeziehen.

Sie können genauso aber auch **mehrere E-Mails** gleichzeitig als Dateianlage an ein solches Konto versenden.

1. **Markieren** Sie in Outlook die entsprechenden **E-Mails**.
2. Klicken Sie nun mit **rechter Maustaste** auf eine solche E-Mail.
3. Wählen Sie aus dem Kontextmenü **Elemente weiterleiten**.
4. Geben Sie im **An:-**Feld die entsprechende **Lernadresse** ein.

Die Wahl des eigenen Schutzes

Bei der Wahl eines Spam-Schutzes für das eigene Unternehmen kann primär zwischen zwei Lösungen gewählt werden: einem Client-seitigen oder einem Server-seitigen Schutz. Betreibt das Unternehmen einen eigenen E-Mail-Server ist es das einfachste, den Schutz direkt dort zu implementieren. Um sicher zu gehen, die richtige Entscheidung getroffen zu haben, sollten die Leistungsmerkmale der einzelnen Lösungen genau unter die Lupe genommen werden. Jeder einzelne der oben beschriebenen Mechanismen alleine ist nicht wirklich effektiv genug. Die optimale Lösung vereint deshalb sowohl schwarze als auch weiße Listen, Regeln, die statistische hypothetische Analyse und im besten Fall auch DKIM.

Die Integration beim Endanwender ist ein Bereich, der oftmals übersehen wird. Es ist wichtig, dass der einzelne Anwender oder zumindest der Administrator überwachen kann, was von den Filtern aussortiert wurde um gegebenenfalls fälschlicherweise aussortierte legitime E-Mails wieder herzustellen. Des Weiteren sollten Anwender die Möglichkeit haben, Feedback an die hypothetische Analyse zu geben, um deren Effizienz nach und nach zu optimieren.

Zusammenfassung

Ein wirksamer Schutz gegen Spam kombiniert mehrere Techniken. SURBL in Verbindung mit schwarzen Listen bekannter Spammer bietet einen guten Basisschutz. Als Ergänzung hierzu sollte das System eine Form statistisch hypothetischer Analyse bieten, um fortschrittlicheren Spammern die Stirn bieten zu können. Es gibt Anti-Spam Lösungen für Server und Clients, grundsätzlich ist es jedoch sinnvoll, unerwünschte Werbung schon direkt seitens des Mailservers abzufangen. Auf diese Weise ist das System an sich transparenter und der Administrator hat bessere Möglichkeiten, dieses zu kontrollieren.

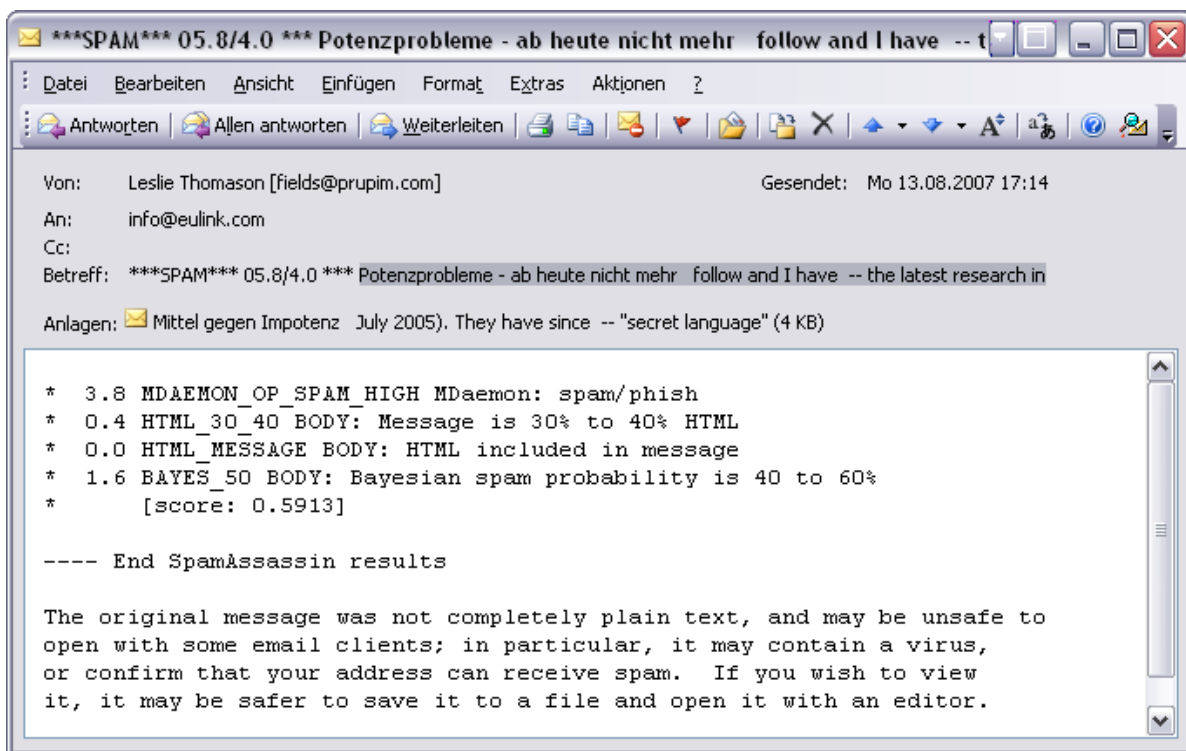
Beispiel-Screenshots für erkannte Spam-E-Mails

Diese Screenshots beziehen sich auf einen aktiven Spam-Filter / Bayes und einer Punktebewertung durch die Heuristik. Die Spam-Einstellungen sind so konfiguriert, dass erkannte Spam-Nachrichten mit der Kennzeichnung *****SPAM*****. in der Betreffzeile versehen werden. Alternativ könnten Sie auch noch die erreichte Punktzahl in der Betreffzeile anzeigen lassen.

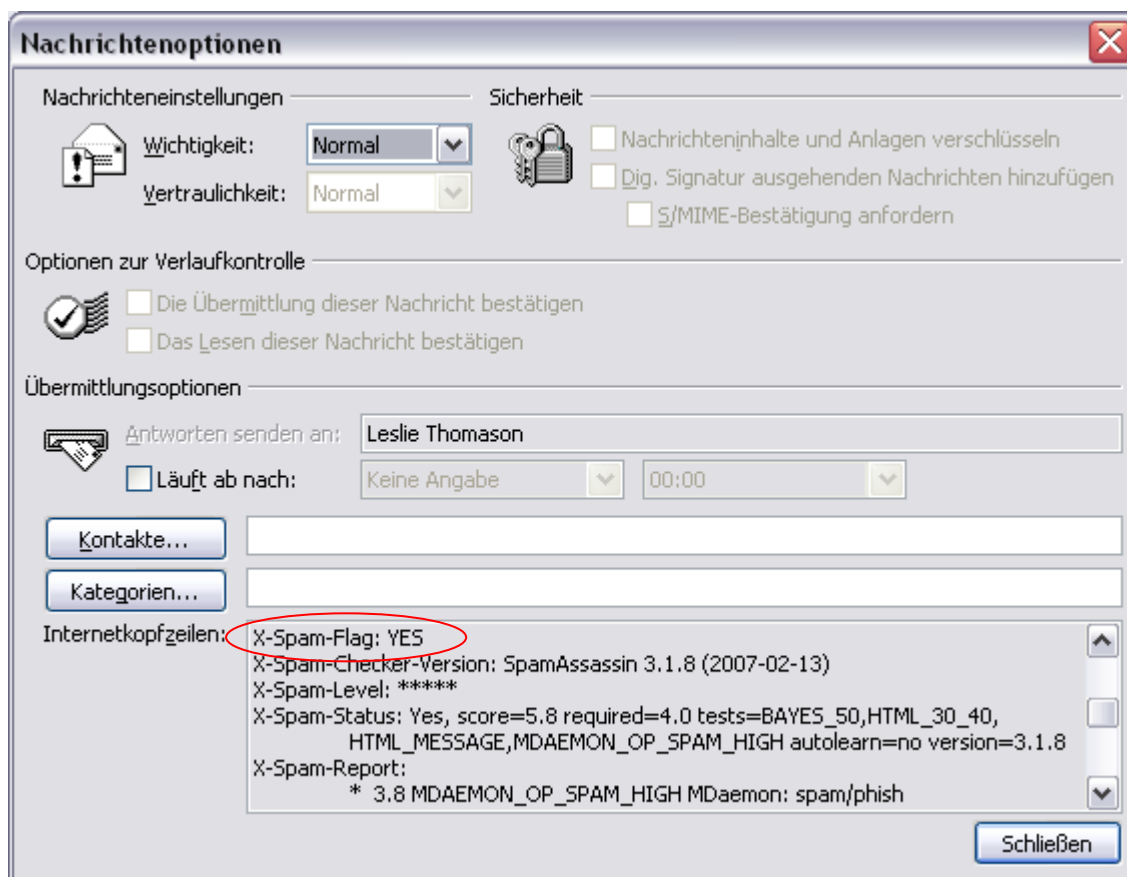
Eine als Spam erkannte E-Mail wurde mit der Betreffzeile *****SPAM*****. gekennzeichnet:

Von	Betreff	Erhalten	Größe
Carson Glenn	***SPAM*** 05.5/4.0 *** Re[79]: Sie leben nur einmal - oder ?	Mo 13.08.2007 15:09	4 KB

Beim Öffnen einer solchen E-Mail erhalten Sie Information über die Punktebewertung der Heuristik. In der Anlage befindet sich die ursprüngliche E-Mail.



Die positiven Nachrichten erhalten von MDaemon den Header **X-Spam-Flag: YES**



In den Protokolldateien können Sie die Bewertungen ebenfalls einsehen.
Wechseln Sie in das Verzeichnis `\MDaemon\Logs`

Öffnen Sie die Protokolldatei `AntiSpam.log`

```

Mon 2008-08-13 16:16:52: Spam Filter processing c:\mdaemon\queues\local\md50000743771.msg...
Mon 2008-08-13 16:16:52: > Message return-path: fields@prupim.com
Mon 2008-08-13 16:16:52: > Message from: fields@prupim.com
Mon 2008-08-13 16:16:52: > Message to: info@ebertlang.com
Mon 2008-08-13 16:16:52: > Message subject: Potenzprobleme - ab heute nicht mehr
Mon 2008-08-13 16:16:52: > Message ID: <01c7ddb4$3215f4e0$cd48b554@fields>
Mon 2008-08-13 16:16:52: Start SpamAssassin results
Mon 2008-08-13 16:16:52: 5.80 points, 4.00 required
Mon 2008-08-13 16:16:52: * 3.8 MDAEMON_OP_SPAM_HIGH MDaemon: spam/phish
Mon 2008-08-13 16:16:52: * 0.4 HTML_30_40 BODY: Message is 30% to 40% HTML
Mon 2008-08-13 16:16:52: * 0.0 HTML_MESSAGE BODY: HTML included in message
Mon 2008-08-13 16:16:52: * 1.6 BAYES_50 BODY: Bayesian spam probability is 40 to 60%
Mon 2008-08-13 16:16:52: * [score: 0.5001]
Mon 2008-08-13 16:16:52: End SpamAssassin results
    
```