

# **i**Administrator

Das Magazin für professionelle System- und Netzwerkadministration

## **Red Earth Policy Patrol Enterprise 5 Benimmregeln für den Mailverkehr**

**41**

# **Sonderdruck für ProSoft**

**Im Test:** Red Earth Policy Patrol Enterprise 5

# Benimmregeln für den Mailverkehr

von Sandro Lucifora



Das im letzten Jahr in Kraft getretene Gesetz über elektronische Handels-, Genossenschafts- und Unternehmensregister (EHUG) legt fest, dass in gewerblichen E-Mails rechtliche Angaben über das Unternehmen enthalten sein müssen. Eine mögliche Lösung, um die Nachrichtenflut beim Ausgang der E-Mail mit den notwendigen Informationen zu versehen, stellen Mailgateways dar. Policy Patrol von Red Earth Software ist ein solches Tool. Ob es E-Mails rechtskonform bündigt und zugleich vor den Gefahren des Internets schützt, haben wir für Sie in einem Langzeittest herausgefunden.

**U**nter die gesetzliche Regelung zur Absenderkennzeichnung fallen alle E-Letter wie Angebote, Bestellungen, Kündigungen oder Newsletter. Diese unterschiedlichen Formate machen es Administratoren immer schwerer, die Verwaltung des Mailsystems komplikationslos zu bewerkstelligen. Im schlimmsten Fall können Verstöße gegen die Vorgaben Geldstrafen sowie Abmahnungen durch Wettbewerber nach sich ziehen. Der einfachste Weg, unternehmensweite Angaben festzulegen sowie zu gewährleisten, dass diese immer mitgeschickt werden ist es, am zentralen Mailserver, etwa Exchange, die Konfiguration vorzunehmen. Leider verfügen Groupware-Lösungen, auch Microsofts Exchange Server, nur über rudimentäre Möglichkeiten, diese Einstellungen zentral zu tätigen.

Die Verwendung eines Mailgateways ist also die komfortablere Alternative. Die Vorgehensweise von Policy Patrol ist schnell erklärt: Die Software installiert sich auf dem Exchange-Server und klinkt sich in die interne und externe SMTP-

Kommunikation ein. Nach der Installation überwacht das System jeglichen E-Mailverkehr in Exchange, beeinflusst die Grundkonfiguration der Mailstruktur aber nicht. Da auch kein Neustart notwendig ist, kann der Administrator die Software im laufenden Betrieb aufspielen und in Ruhe in Betrieb nehmen. Das Administrations-Tool lässt sich wahlweise zentral oder dezentral verwenden, zum Beispiel auf der eigenen Arbeitsstation, und interagiert per Remote-Zugriff mit Policy Patrol.

## Umfassende E-Mailsicherheit

Policy Patrol 5 ist modular aufgebaut. Je nach Lizenzierung stehen unterschiedliche Funktionen zur Verfügung. Wir haben die Enterprise-Version, die alle verfügbaren Module enthält, getestet. Im Einzelnen sind das die Funktionen Disclaimer/Signatur anfügen, ein Manager für Dateianhänge, Archivierung, ein Spamfilter und eine Antiviren-Engine. Das System beschränkt sich also nicht darauf, ausgehende E-Mails um diverse Angaben zu erweitern, sondern kann nach verschiede-

nen Kriterien auch eingehende E-Mails bearbeiten und prüfen.

Wer das ganze Paket inklusive Reporting und Archivierung nutzen will, benötigt im Netzwerk noch einen MS SQL-Server. Je nach Mailaufkommen könnte jedoch dessen kostenlose Desktop-Version wegen der Größenbegrenzung nicht ausreichen. Insgesamt ist die Einrichtung aber schnell erledigt und der Administrator kann sich im Laufe der Zeit daranmachen, die Regeln, Filter und Funktionen nach und nach zu verfeinern.

- Windows 2000 Server oder
- Windows XP Professional oder
- Windows Server 2003.
- Microsoft Exchange Server 2007 oder
- Exchange Server 2003 oder
- Exchange Server 2000 oder
- Exchange Server 5.5 oder
- Windows Small Business Server
- Microsoft .NET Framework 1.1

### Systemanforderungen

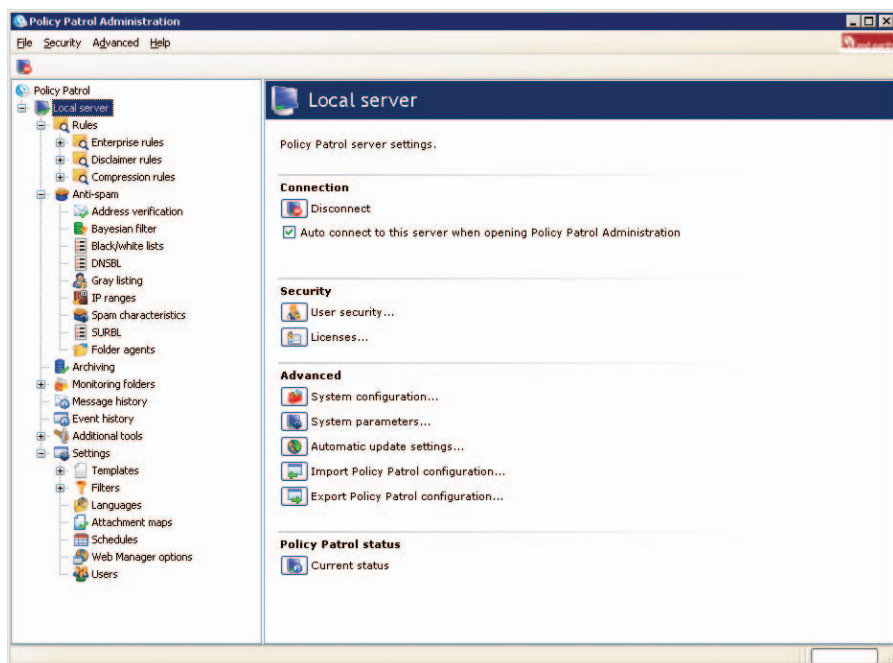


Bild 1: Die zentrale Administration von "Policy Patrol" ist übersichtlich und gut strukturiert

Vor der Einrichtung der einzelnen Module sollten in den Settings einige globale Konfigurationen eingestellt werden. Dieses Vorgehen setzt den Gedanken der zentralen Konfiguration durchgängig um. Unter den Settings werden zum Beispiel die Signaturen, Templates und sämtliche Notifications an zentraler Stelle abgelegt und bei Bedarf nur hier geändert. Das erspart bei etwaigen späteren Anpassungen eine Menge Aufwand.

Im Test haben wir die E-Mails über einen Exchange Server 2003 mit fünf Benutzerkonten über mehrere Wochen mit Policy Patrol überwachen, prüfen und anpassen lassen. Die vorrangige Grundaufgabe des Systems ist es, E-Mails eine gesetzeskonforme Signatur sowie einen Disclaimer anzufügen.

### Disclaimer und Signaturen zentral verwalten

Die Software unterscheidet im entsprechenden Modul zwischen Signatur und Disclaimer. Als Disclaimer wird in diesem Zusammenhang ein Nachspann, meist ein Haftungsausschluss, bezeichnet. Eine Signatur hingegen beinhaltet die persönlichen Kontaktinformationen und die Unternehmensangaben.

### Variablen aus dem Active Directory übernehmen

Beide Anhang-Varianten werden meist unterschiedlich behandelt. So müssen Signaturen nicht unter jeder E-Mail stehen, sondern nur unter solchen, die einen neuen Geschäftskontakt darstellen. In einen E-Maildialog mit einem regelmäßigen Geschäftspartner muss dagegen keine Signatur eingefügt werden.

Den Disclaimer hingegen möchten Unternehmen oft in jede E-Mail einbinden, meist abhängig vom Zweck des Schreibens. So kann der Disclaimer einer normalen E-Mail den Hinweis darauf enthalten, dass die Information vertraulich zu behandeln ist. Eine E-Mail mit einem Angebot oder einer Rechnung verfügt im Regelfall über einen spezifizierten Disclaimer, etwa einen Hinweis auf die AGB, die Verbindlichkeit eines Angebots oder eine Kontoverbindung.

So gestaltete verschachtelte Anforderungen haben wir im Test eingerichtet. Für den Disclaimer hinterlegten wir in den globalen Settings den jeweiligen Text. Hierbei lassen sich Texte für HTML und Plain separat eintragen. In der Praxis fehlte uns hier eine Funktion, die den HTML-Text

auf Knopfdruck in das Plain-Text-Fenster übernimmt. An selber Stelle hinterlegten wir die Signatur. Hier nutzten wir die Funktion zur Einbindung von hinterlegten Variablen und personalisierten damit die Signatur. Dabei konnten wir auf Variablen zurückgreifen, die als Felder im Active Directory hinterlegt sind. Vermisst haben wir aber den Platzhalter für die Internetadresse.

### Richtschnur zur E-Mailbehandlung

Im nächsten Schritt legten wir die Regeln an, die Policy Patrol dazu veranlassen, diverse Angaben unter die E-Mails zu setzen. Das System unterscheidet wie

#### Die Pflichtangaben gelten für:

- Einzelkaufleute
- Personenhandelsgesellschaften wie OHG, KG oder GmbH & Co. KG
- Gesellschaften mit beschränkter Haftung
- Aktiengesellschaften
- Partnerschaftsgesellschaften
- Genossenschaften

#### Diese Daten müssen ersichtlich sein:

- Der vollständige Firmenname, so wie er im Handelsregister, Partnerschaftsregister oder Genossenschaftsregister eingetragen ist
- Rechtsformzusatz (beispielsweise GmbH, KG, Kommanditgesellschaft, OHG, AG, e.K. et cetera)
- Sitz des Unternehmens (anzugeben ist der satzungsmäßige Hauptsitz, auch wenn die E-Mail von einer Zweigniederlassung aus verschickt wird)
- Registernummer (des Unternehmens, nicht einer etwaigen Zweigniederlassung)
- Registergericht (des Unternehmens, nicht einer etwaigen Zweigniederlassung)

#### Bei GmbHs müssen zusätzlich enthalten sein:

- Alle Geschäftsführer mit ausgeschriebenem Vor- und Zunamen (falls vorhanden) der Aufsichtsratsvorsitzende mit ausgeschriebenem Vor- und Zunamen

#### Bei AGs müssen zusätzlich enthalten sein:

- Alle Vorstandsmitglieder mit ausgeschriebenem Vor- und Zunamen, wobei der Vorstandsvorsitzende als solcher zu bezeichnen ist
- Ausgeschriebener Vor- und Zuname des Aufsichtsratsvorsitzenden

Wir übernehmen keine Gewähr für die Vollständigkeit der Angaben.

**Tipp: Diese Angaben müssen in den Disclaimer**

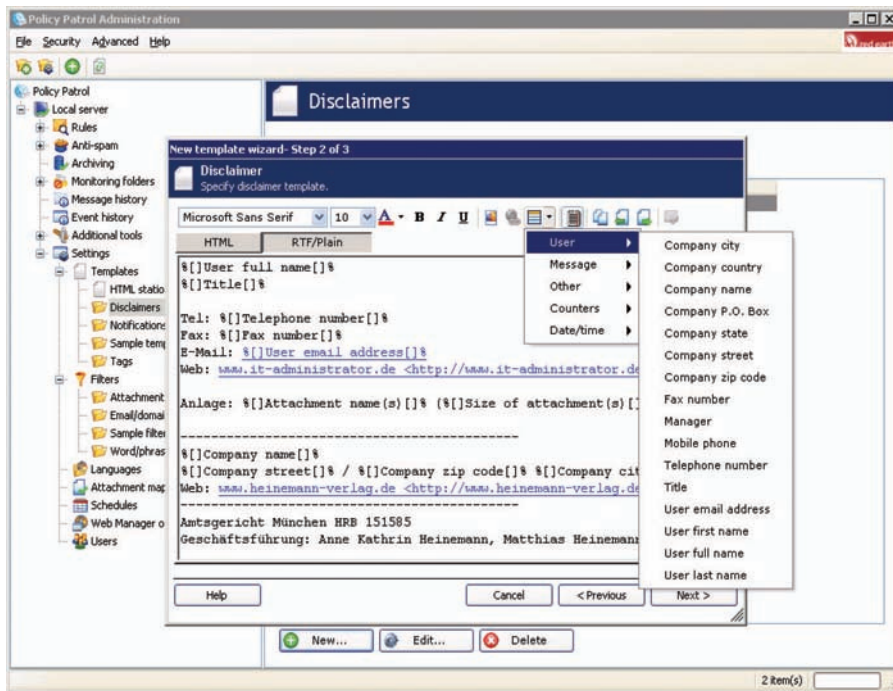


Bild 2: Die Vorlagen für Signaturen werden anhand von Variablen aus dem Active Directory individualisiert

beschrieben zwischen Disclaimer und Signatur. Daher mussten wir auch zwei Regeln einsetzen. Die Vorgehensweisen zum Einrichten sind für den Disclaimer und die Signatur identisch.

Als Erstes legten wir fest, für welchen User die Regel gilt. In unserem Fall wollten wir exemplarisch einen Disclaimer für den Rechnungsausgang einbinden. Da jeder Benutzer Rechnungen verschicken kann, legten wir die Regel ohne Ausnahme fest. Im nächsten Schritt bestimmten wir, dass diese Regel lediglich bei extern ausgehenden E-Mails fällig ist. Nun bestimmten wir noch, wann der Disclaimer hinzugefügt wird. Dafür konnten wir auf mehrere Ereignisse filtern. Um den Zusatz zu erhalten, musste die E-Mail digital signiert sein, einen definierten Absender haben, im Betreff musste "Rechnung" stehen und es musste ein Anhang beigefügt sein.

Der nächste Dialog erlaubte uns, zusätzliche Ausschlüsse zu hinterlegen. Dazu erweiterten wir die Regel um den Filter, dass der Betreff keine Wort-Phrase wie "AW:", "Re:" und "WG:" enthalten darf. Die Sammlung dieser Phrasen hatten

wir bereits in den zentralen Settings hinterlegt; dort lassen sie sich jederzeit ergänzen. Treffen all diese Ereignisse zu, soll die E-Mail ausgeliefert und dieser zuvor der Disclaimer für Rechnungen hinzugefügt werden.

Um die von uns zuvor definierte Signatur hinzuzufügen, riefen wir den Assistenten im Menüpunkt "Signatures" auf und konfigurierten die passende Regel nach dem bekannten Vorgehen. Auch hier sollte die Regel für alle User gelten, die externe Nachrichten versenden. Den Ausschlussfilter auf die Wort-Phrasen konnten wir uns hier sparen, da Policy Patrol von Haus aus keine Signaturen an Antwort-E-Mails hängt. Die Auswahl des Signatur-Templates war nur noch eine Fleißübung, bevor die Regel in Betrieb ging.

### Domainabhängige Absenderangaben

Im Test haben wir mit verschiedenen Absender-Domains kommuniziert. Um jeweils die passende Signatur hinzuzufügen, konnten wir die Konfiguration für E-Mailbedingungen verwenden. Hier kam die Abfrage hinzu, dass der Absender eine bestimmte Domain enthalten muss. Je nach Domain-Gruppe wird eine eigene

Regel angelegt, die dann die jeweilige Signatur einsetzt. Die Domain-Gruppen werden wiederum in den globalen Settings deklariert. So können Unternehmensgruppen, die über einen gemeinsamen Exchange-Server arbeiten, den unterschiedlichen Angaben in den Signaturen Rechnung tragen.

## Kontrolle und Bearbeitung von Attachments

Anhänge verschiedenster Art sind Alltag beim E-Mailversand. Doch bei solchen Anhängseln ist Vorsicht geboten, nicht nur was den Schutz vor Viren angeht. Vielfach wollen Unternehmen vermehrt kontrollieren, welche Art von Anhängen Anwender überhaupt versenden und empfangen dürfen. Um diese Regeln einzuhalten, verfügt Policy Patrol über Funktionen, die sich gezielt auf die Anhänge beziehen.

### Verfahrensregeln für bestimmte Dateitypen

Unter den Enterprise-Regeln findet sich der Wizard für Anhänge. Der Filter prüft auf die reine Existenz, die Größe, den Namen und den Typ sowie auf Wort-Phrasen im Dateinamen und die Anzahl von Anhängen. In einem Unternehmen kann es zum Beispiel nicht erwünscht sein, dass Anwender MP3-Dateien versenden. Um dies generell zu verhindern, wird an dieser Stelle der Filter auf den Dateityp gelegt und im Fall des MP3-Versands die Nachricht in einen bestimmten Ordner umgeleitet und eine E-Mail- oder Netzwerknachricht an einen beliebigen Empfänger gesendet. Ein Sicherheitsbeauftragter kann die ausgehende Datei vor dem Versand dann noch einmal prüfen. So lässt sich verhindern, dass vertrauliche Daten aus dem Unternehmen geschleust werden.

### Der Anwender spart sich das Entpacken

Eine weitere Funktion ist das Packen und Entpacken von Anhängen. Im Test realisierten wir damit verschiedene Regeln. Zum einen sollten alle nach extern versandten E-Mailanhänge, die in der Sum-

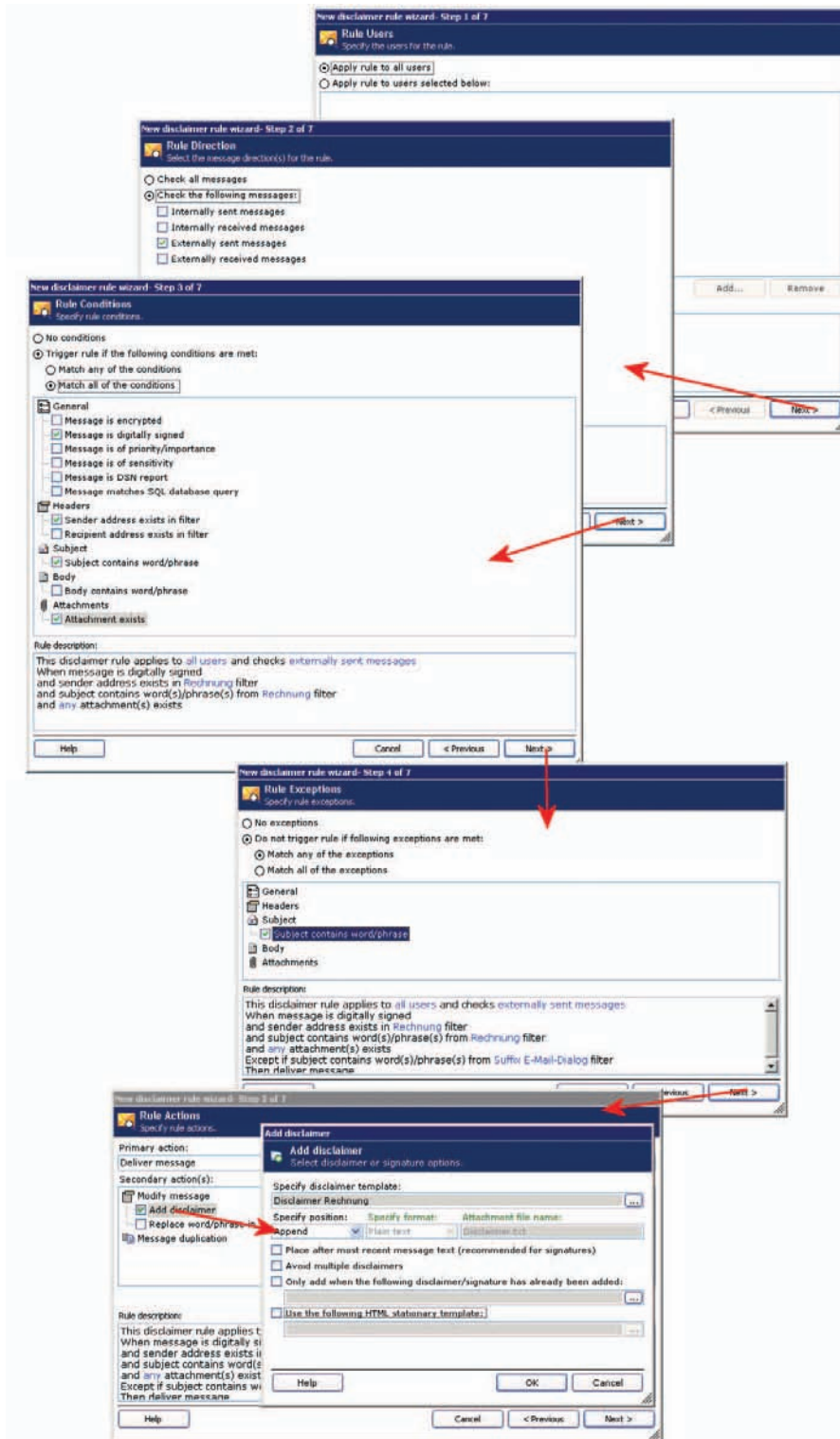


Bild 3: Die Regel-Definition für Disclaimer und Signaturen lässt sich in wenigen Schritten individuell einrichten

me größer als 1 MByte pro E-Mail waren, gepackt werden. Im Gegenzug sollte das System alle Anhänge, die hineinkommen und gepackt sind, schon auf dem Exchange-Server auspacken. Das erspart den

Empfängern Arbeit. Zusätzlich sollten eingehende gepackte Anhänge, die durch ein Kennwort geschützt sind, in einen Delay-Ordner gelangen, den eine berechtigte Person sichten muss. Eine weitere "Com-

pression"-Regel sorgte dafür, dass Policy Patrol die Anhänge ausgehender E-Mails, die im Betreff mit "[Nicht packen]" markiert sind, unverändert durchwinkte und diese Wortkombination im Betreff wieder löschte. Durch solche Filter lässt sich im Laufe der Zeit eine sehr individuelle Steuerung realisieren, die auch in umgekehrter Form zur Anwendung kommen kann: Nur die Anhänge mit dem Vermerk "[Packen]" werden komprimiert, andere bleiben unverändert. Solche und ähnliche Steuerfunktionen lassen sich in alle Arten der Filterregeln implementieren.

### Spam- und Virenschutz ohne Makel

Schon die zuvor beschriebenen Regeln sind mächtige Werkzeuge. Mit den Modulen "Anti-Spam" und "Anti-Virus" wertet Red Earth Software Policy Patrol noch um wichtige Sicherheitsfunktionen auf, die den Einsatz zusätzlicher Software für diesen Bereich überflüssig machen.

Anti-Spam bedient sich der mittlerweile zum Standard gehörenden Filterfunktionen, darunter die konfigurierbare Adressenprüfung wie die Klassiker der MX-Prüfung und SMTP-Verifizierung. Ein bayesscher Filter, eine eigene Black-White-Liste und die Befragung einer DNS-Blacklist sorgen weiterhin für eine Befreiung von unerwünschten E-Mails. Greylisting sorgt dafür, dass das System die erste E-Nachricht von unbekanntem Absender temporär abweist und erst nach einem zweiten Zustellversuch annimmt.

In der Konfiguration stellten wir ein, dass erkannter Spam direkt gelöscht und vermuteter Spam in einen dafür vorgesehenen Ordner verschoben wird. Je nach Einstellung – bei uns morgens um acht – sendet Policy Patrol jedem User eine E-Mail mit der Liste von gefilterten Spammessages. Der Benutzer erhält damit Zugriff auf ein Web-Interface, über das er die Nachrichten endgültig löschen oder aber abfragen kann. An diesem Punkt kann er auch die Black- und Whitelist per Mausklick mit den jeweiligen Absenderangaben erweitern.

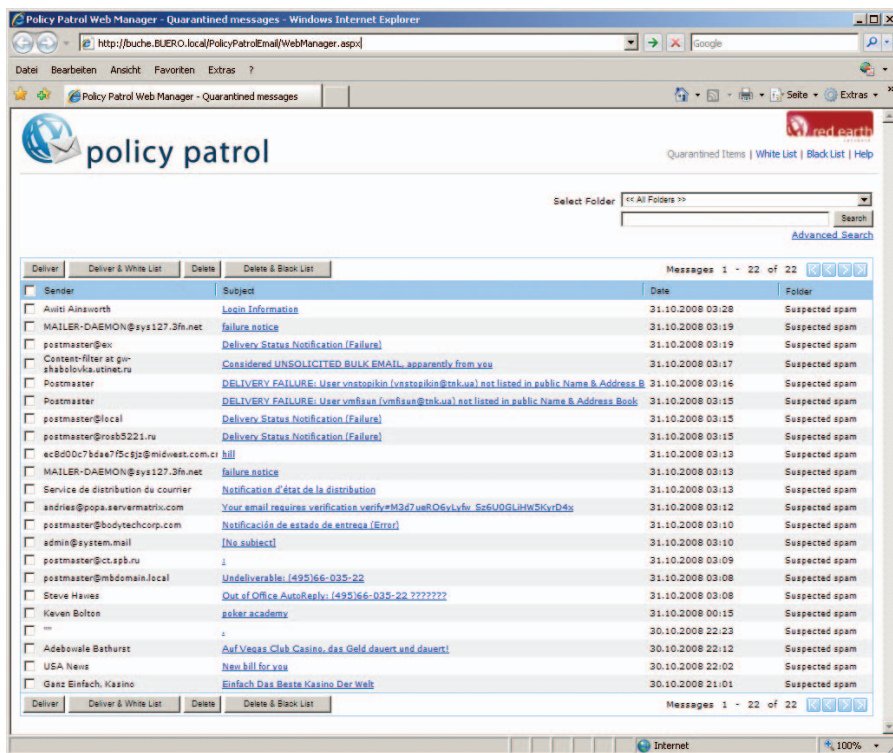


Bild 4: Über das Web-Interface werden die Spammails endgültig gelöscht oder fehlerhaft aussortierte Nachrichten zugestellt

Für die Virenabwehr bedient sich Red Earth Software der bekannten Engine von Kaspersky. In der Anti-Virus- und Enterprise-Lizenz ist die Aktualisierung der Kaspersky-Virensignaturen für jeweils ein Jahr enthalten. Im Test konnten wir bei den Schutzfunktionen keine Aussetzer feststellen. Lediglich beim Spamfilter war es notwendig, für die Anhänge noch eine Regel für das Erkennen von Spoofing-Attachments einzubauen, um diese lästigen Nachrichten herauszufiltern. Spoofing-Anhänge sind zum Beispiel solche, die doppelte Endungen wie “.pdf.zip” oder “.wps.exe” haben.

### Kleine Geschenke erhalten die Freundschaft

Seine Funktionalität rundet Policy Patrol noch mit zwei nennenswerten Dreingaben ab: “Auto-Reply” und “POP3 Downloader”. Über Auto-Reply liefert Policy Patrol für definierte Empfängeradressen automatische Antworten an den Absender.

Der POP3-Downloader ist für Unternehmen interessant, die aus unterschiedlichen Quellen ihre E-Mails von externen Mail-

servern via POP3 abholen müssen. Die Gründe dafür können sein, dass der eigene Exchange-Server – aus Sicherheitsgründen – keine SMTP-Verbindung von außerhalb annimmt oder dass zusätzlich einige Konten von Fremd-Domains abgefragt werden müssen. Auch wenn das kleinste Intervall des POP3-Connectors von Exchange, nämlich 15 Minuten, zu lang ist, leistet das Werkzeug gute Dienste.

Policy Patrol setzt die zentrale Konfiguration sehr stringent um. Das gilt ebenso für die Definition von Zeitplänen, die sich mit einzelnen Regeln verknüpfen lassen. Der POP3-Downloader hat jedoch keinen Zugriff auf diese zeitliche Definition. Hier wird nur ein festes Abholintervall hinterlegt, was die vom Produkt sonst bekannte Flexibilität unnötig einschränkt.

### Fazit

Im mehrwöchigen Test hat Policy Patrol mehr als 5.000 E-Mails überwacht und entsprechend den Regeln behandelt. Die Konfiguration war schnell erledigt und hat danach ohne Nacharbeiten gut

funktioniert. Lediglich die Notwendigkeit eines MS SQL-Servers für die Nutzung von Report und Archivierung ist von Nachteil, da die kostenlose Version durch die Größenbeschränkung der Datenbank bei entsprechendem Mailaufkommen nicht ausreichen wird. Wer durch ein Mailgateway seine Disclaimer und Signaturen sowie Anhänge in den Griff bekommen möchte und dies im Paket mit Viren- und Spamschutz tun will, ist mit Policy Patrol Enterprise 5 gut bedient. (In)



**Produkt**  
Mailgateway, das den Postverkehr nach Gefahren durchsucht und mit variablen Textanhängen versieht.

**Hersteller**  
Red Earth Software  
[www.policypatrol.de](http://www.policypatrol.de)

**Preis**  
Policy Patrol Enterprise 5 ist für zehn User ab 402 Euro inklusive einem Jahr Update- und Supportvertrag zu haben. Einzelne Module sind ab 102 Euro für zehn User inklusive Update- und Supportvertrag erhältlich.

**Technische Daten**  
[www.it-administrator.de/downloads/datenblaetter](http://www.it-administrator.de/downloads/datenblaetter)

**So urteilt IT-Administrator (max. 10 Punkte)**

Zuverlässigkeit	9
Konfiguration	9
Erkennungsrate des Spamfilters	8
Aktualität der Virensignaturen	9
Laufender Administrationsaufwand	9

**Dieses Produkt eignet sich**

- optimal für Unternehmen mit einem Exchange-Server ab fünf bis zehn Accounts; auch für Firmengruppen mit mehreren Domains und unterschiedlichen Signatur- und Disclaimer-Vorgaben.
- teilweise für Unternehmen mit einem Small Business Server.
- nicht für Umgebungen ohne Exchange-Server.

**Policy Patrol Enterprise 5**