Literatur

[1] Spamassassin - ein heuristischer Mailfilter
http://www.spamassassin.org

[2] Vipul's Razor
http://razor.sourceforge.net

[3] Spamnet Outlook Add-In
http://www.spamnet.com

[4] Mail Abuse Prevention System
http://www.mail-abuse.org

[5] Open Relay Database (ORDB)
http://www.ordb.org

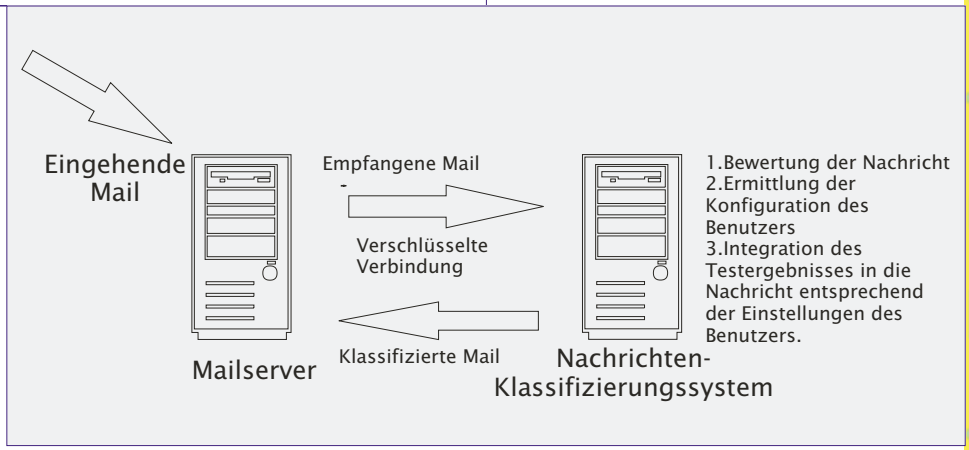

***Abbildung 3**: Integration von Mailklassifikationssystemen*

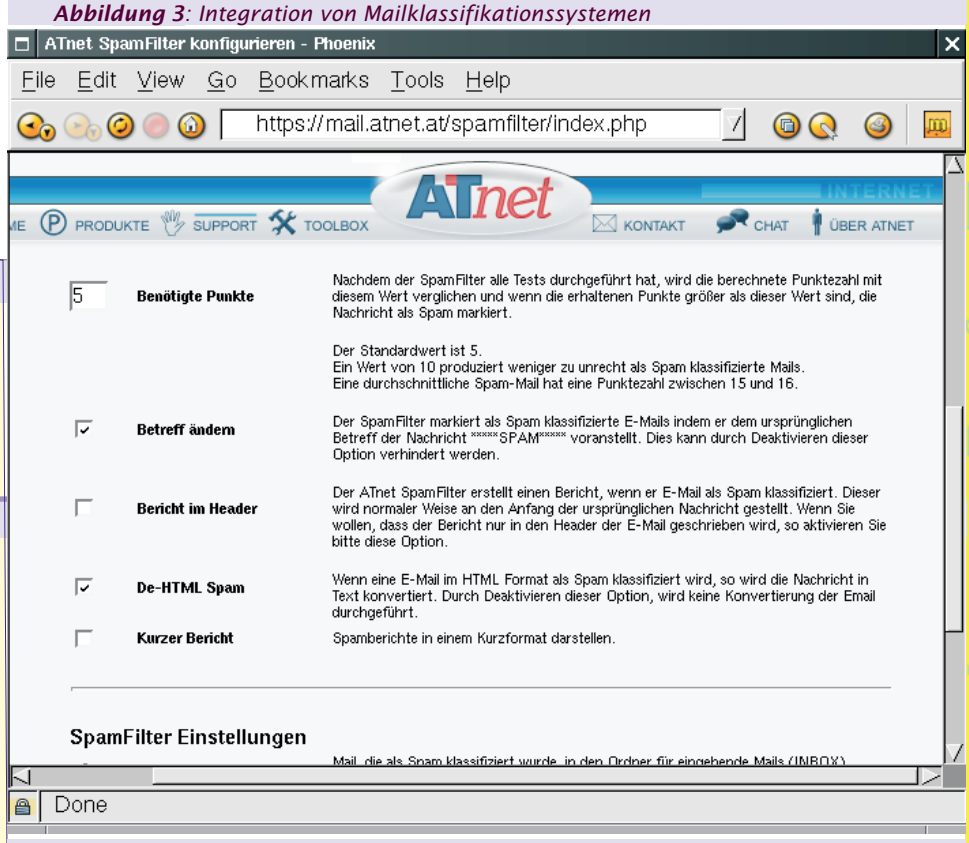

***Abbildung 4:** Spamfilter Konfiguration*

Security

European E-Mail Security End-user Study

Frost & Sullivan

Inhaltsfilterung von E-Mails: Anbieter müssen besser über Vorteile informieren

Potenzielle Kunden wissen noch nicht ausreichend Bescheid über die Möglichkeit der Inhaltsfilterung von E-Mails, weshalb entsprechende Softwaresysteme noch nicht in adäquatem Umfang nachgefragt werden. Eine neue Analyse der Unternehmensberatung Frost & Sullivan geht allerdings davon aus, dass die jüngsten heftigen Diskussionen um den Missbrauch unternehmenseigener E-Mail-Systeme das Bewusstsein für Sicherheitslösungen schärfen und damit einen erhöhten Bedarf generieren werden.

Diese Erkenntnisse beruhen auf ausführlichen Interviews mit mehr als 200 IT-Entscheidungsträgern in mittleren und großen Unternehmen in Großbritannien, Skandinavien, Deutschland und Frankreich, Europas wichtigsten Ländermärkten für Sicherheitssoftware. Gefragt wurde nach Markenbewusstsein sowie nach der qualitativen Einsstufung von Marktakteuren wie Clearswift, Symantec, Trend Micro, Computer Associates, SurfControl, Message Labs, Tumbleweed, Network Associates, Brightmail, Marshal Software, Invisimail und Aladdin.

Ein Fünftel der potenziellen Kunden kennt die Technologie nicht

Laut Analyse müssen sich die Anbieter von Filtersystemen in der nächsten Zukunft hinsichtlich Kundenbewusstsein und Nutzung von Software zur Inhaltsüberwachung zentralen Herausforderungen stellen. So gaben nahezu 20 Prozent der Befragten an, über das Angebot entsprechender Lösungen nicht informiert zu sein, und ein weiterer Prozentsatz wusste nur bedingt über die erhältlichen Produkte Bescheid. Von den Befragten, die die angebotenen Lösungen kennen, setzen allerdings knapp 53 Prozent sie nicht ein. Die große Mehrheit hatte der Installation solcher Sicherheitssysteme zudem innerhalb ihres Unternehmens niedrige Priorität eingeräumt.

Nutzwert muss besser kommuniziert werden

Grund zum Optimismus gibt es dennoch, meint Jose Lopez, Sicherheitsexperte bei Frost & Sullivan: "Es muss den Anbietern nur gelingen, die Zielgruppe vom hohen Nutzen der Inhaltsfilterung zu überzeugen. Dabei werden die zunehmende Anzahl von Negativmeldungen über die unerlaubte Nutzung bzw. Belastung von Firmen-E-Mail-Systemen und die sich daraus ergebenden Sicherheitsprobleme sicherlich als wichtige Argumente dienen."

Um Kaufinteresse zu wecken, sollten die angebotenen Lösungen aus der Perspektive der potenziellen Endnutzer vor allem drei Aspekte abdecken: erstens die Bedrohung durch Viren und unautorisierte Weitergabe unternehmensinterner Informationen, zweitens die unnötige Belastung der Systeme durch Spam oder Junk Mails (Massenmails wie Werbung, Kettenbriefe, Pyramidenspiele etc.) und drittens E-Mails mit beleidigendem oder pornographischem Inhalt.

Virenabwehr ist Hauptgrund für Einsatz

"An erster Stelle geht es den Firmen immer noch um die Viren," kommentiert Lopez, "doch gibt es in Bezug auf E-Mail-Sicherheit noch andere Probleme, die nicht einfach durch Installation einer Anti-Virus-Software gelöst werden können. Da gibt es beispielsweise vertrauliche Informationen, die über undichte Stellen an die Konkurrenz gelangen könnten. Das ist vor allem in der Finanzbranche oder in der Luftfahrt- und Verteidigungsindustrie relevant, aber im Prinzip ist jedes Unternehmen betroffen, das Forschung betreibt. Das sind die Punkte, an denen die Anbieter von E-Mail-Inhaltsfilterung ansetzen müssen."