Antispam-Appliance für den Mittelstand

Abweisend

Lukas Grunwald

Neben dem Quasi-Standard Brightmail, auf dem viele sehr teure Antispam-Produkte basieren, gibt es günstige Alternativen. Mit der Sponts will IKU Mittelständler ansprechen, die keine fünfstelligen Beträge für den Einstand in die Filterung ausgeben wollen.

Sponts ist in zwei Versionen verfügbar: in Form eines kompakten Mini-ITX-PC (570 €) und als 19-Zoll-Einschub, der im Rechenzentrum nur eine Höheneinheit belegt (820 €). An Lizenzkosten sind mindestens rund 400 € jährlich (bis 10 Postfächer, bei bis zu 1000 Postfächern rund 4000 € im ersten Jahr, danach 2000 €) zu veranschlagen (www.iku-ag.de).

Die Installation erfolgt wie bei Appliances üblich über eine serielle Verbindung per Terminal oder Terminal-Emulation zur Festlegung der Betriebsparameter für den späteren Zugriff via Webbrowser. Was bei ähnlichen Produkten oft keine Beachtung findet, ist hier vorbildlich gelungen: Nach dem Erzeugen des SSL-Schlüsselpaares gibt das Gerät den SHA- und MD5-Fingerprint aus, sodass beim ersten Zugriff kein Man-in-the-Middle-Angriff zu befürchten ist und der Administrator sicher sein kann, dass er die richtige Box bedient. Außerden kann er mehreren Anwendern vom Administrator über den Root-User bis zum Datenbank-Benutzer jeweils unterschiedliche Passwörter geben und so die Zugriffsrechte fein granulieren.

Nach dem Terminal-Setup, das auf Dialog-Skripts basiert, lassen sich die übrigen Konfigurationsschritte per Webbrowser vornehmen. Der zeigt per SSL-Verbindung eine Oberfläche für die Ansicht der Log-Dateien, die Zuordnung der Anwender und Postfächer sowie die Konfiguration des E-Mail-Relaying.

Zur Spam-Erkennung und -Abwehr setzt die Sponts mehrere Verfahren ein, darunter Spamassassin, DNS-Lookups sowie einen Timing-Mechanismus, der dem Greylisting-Verfahren (siehe S. 94) ähnelt, jedoch nur eine SMTP-Sitzung pro E-Mail benötigt. Das Gerät wartet ein bestimmtes Zeitintervall von zum Beispiel 60 s ab, bevor es die E-Mail empfängt, ohne dabei die SMTP-Sitzung zu beenden. Da die meisten Spammer oder E-Mail-Würmer nicht auf solche Pausen Rücksicht nehmen und Mails trotzdem während der Zwangspause zu senden versuchen, bricht Sponts die Verbindung in solchen Fällen ab. Leider trifft dieser Trick auch reguläre Absender, die mangelhaft konfigurierte SMTP-Server einsetzen, und Mail-Systeme von Yahoo, die SMTP-Verbindungen nach einer kürzeren Zeitspanne beenden.

Schick's noch einmal

Wenn ein System eine gewisse Menge unerwünschter Mails gesendet hat, kommt es schnell auf eine schwarze Liste, sodass die Appliance von dort keine E-Mails mehr annimmt. Bei erkanntem Spam begeht sie nicht den sonst leider gängigen Fehler, auf die meist gefälschten E-Mails wiederum mit einer Mail zu antworten, sondern lehnt die unerwünschte E-Mail schon im SMTP-Dialog mit dem Fehlercode 550 ab. Das kann aber dazu führen, dass Abonennten von Mailinglisten bei Fehlalarmen sofort ausgetragen werden, sodass dafür eine gesonderte Konfiguration nötig ist.

Da Sponts bearbeitete E-Mails in einem Ringpuffer speichert, lassen sie sich jederzeit neu zustellen (Option „Replay"), was gerade bei der Feinabstimmung von großem Vorteil ist. Der Ringpuffer kann bei Bedarf auch dann E-Mails annehmen, wenn der Haupt-SMTP-Server nicht verfügbar ist. Die Anwender können dann via POP3 auf die Appliance zugreifen, auch wenn der Rest des Mailsystems ausgefallen oder zu Update-Zwecken abgeschaltet sein sollte.

Für die Beobachtung des Betriebs und die Auswertung der Logdaten besteht die Möglichkeit, auf eine interne MySQL-Datenbank zuzugreifen und alle möglichen Parameter auszuwerten und zu dokumentieren. Der Administrator muss dafür selbst SQL-Abfragen bauen, was zwar sehr flexibel ist, dagegen aber auch Know-how und Zeit benötigt. Die Anfertigung von PDF-Reports, wie sie vergleichbare Lösungen beherrschen, sucht man leider vergebens.

Die Appliance unterstützt das Network Time Protocol und optional derzeit H+BEDV Antivir und Sophos Anti-Virus. Im Test hat sie alle EICAR-Strings erkannt, und die Zip-Mailbombe blieb wirkungslos. Beim Dauertest fiel jedoch auf, dass die eingesetzten Netzadapter im Zusammenspiel mit einem Cisco-Catalyst-Switch von Zeit zu Zeit Aussetzer hatten, während sie einwandfrei mit einem 100-Mbps-Switch für 25 Euro zusammenarbeiteten.

An der organisatorischen Abbildbarkeit von IT-Prozessen ist im Vergleich zu vielen anderen Appliances nichts auszusetzen, nur die Antispam-Engine kann mit Brightmail nicht ganz mithalten. Sonst ist es eine runde Lösung für Kunden, die Wert darauf legen, dass der Hersteller im deutschsprachigen Raum angesiedelt ist.

Fazit

Es muss nicht immer Brightmail sein, wenn man die Mühe scheut, selbst einen PC mit Exim und Spamassassin einzurichten. Mindestens derselbe Effekt ist innerhalb weniger Minuten mit der Sponts-Appliance erreichbar, die jedoch manchmal etwas zu radikal filtert. (un)

LUKAS GRUNWALD

arbeitet als Consultant bei der DN Systems GmbH in Hildesheim und ist in diverse freie Softwareprojekte involviert.