

# ComputerPartner

Fakten, Trends und Meinungen für IT-, TK-, CE-Händler und -Dienstleister

Heute mit Sonderheft  
„Digitale Fotografie“

PROJEKTBERICHT DER NETWORKERS AG

## Wie man Spam bekämpft

Unternehmen mit großem E-Mail-Aufkommen erhalten immer mehr unerwünschte Werbebotschaften. Security Appliances mit spezieller Filtersoftware helfen hier weiter.

Von ComputerPartner-Redakteur DR. RONALD WILTSCHECK

Bei einem von der Networkers AG organisierten Arbeitsfrühstück lernte Norbert Schmözl, der Netzwerk-Verantwortliche bei der Augsburgener Allgemeinen, zum ersten Mal die E-Mail-Filter von Borderware kennen. Der Dienstleister aus Hagen konnte den ITler aus dem schwäbischen Verlag sogleich für die E-Mail-Security-Appliance „Mxtreme 200“ begeistern.

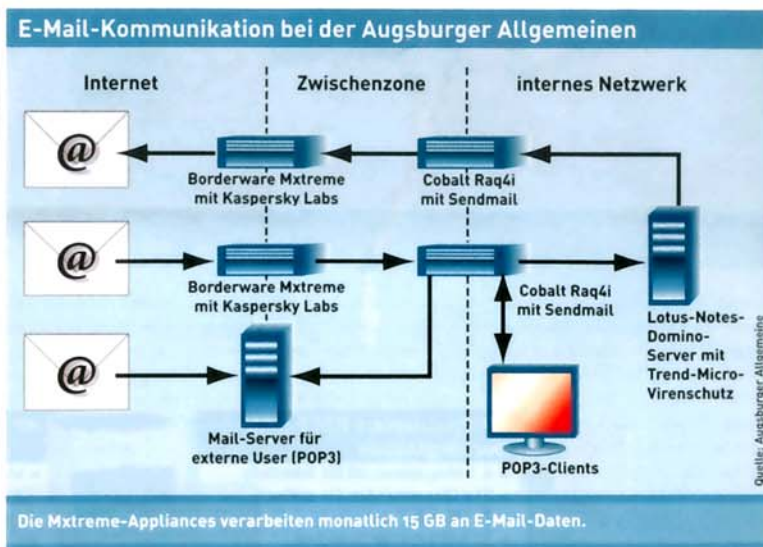
Dies funktionierte so flott, weil die E-Mail-Performance bei der Augsburgener Allgemeinen mittlerweile unerträglich war. Vor einem Jahr hatte das Spam-Volumen ein Ausmaß angenommen, das sich manuell kaum mehr beherrschen ließ. Zum Teil fühlten sich die einzelnen Mitarbeiter gestört und belästigt, zum Teil waren die Inhalte der unerwünschten Mails anstößig oder schlicht böse. Gleichzeitig kostete es erheblichen Aufwand an Zeit und Energie, die Mails zu sichten und zu löschen, inklusive des Risikos, bei dieser Gelegenheit erwünschte und geschäftsrelevante E-Mails zu verwerfen. Alle Hierarchieebenen im Unternehmen waren von dieser Problematik betroffen, sodass das Management entsprechenden Handlungsbedarf im Bereich IT-Security am eigenen Leib erfahren konnte.

Denn bisher stellte sich die Situation folgendermaßen dar: Nachdem im Jahr 2000 die DV-Abteilung der Augsburgener Allgemeinen begonnen hatte, sämtliche Mail-Domains vom damaligen Provider auf eigene Mail-Server zu portieren, sorgte ein externer Mail-Relay, in diesem Falle ein „Cobalt Raq2“ mit Sendmail-Software, für die Annahme aller eingehenden Mails. Insgesamt handelte es sich dabei um 31 zu betreuende Domains mit insgesamt 1.300 E-Mail-Nutzern. Man verzichtete bewusst darauf, separate Mail-User zu definieren. Sollte tatsächlich ein Angriff auf den externen Relay erfolgen, wäre dieser binnen 30 Minuten wieder einsatzbereit.

Aus Sicherheitsgründen entschied man sich zusätzlich für eine verzögerte Übermittlung von Nachrichten an die internen Mail-Systeme. Die Firewall überprüfte im Anschluss mittels Content Filtering die eingehenden Mails.

Doch bereits 2002 zeichnete sich die grundsätzliche Problematik ab: Bisher wurden die auftretenden Sicherheitslücken mit entsprechenden Hersteller-Patches behoben. Doch die Konfiguration des Cobalt Raq2 als reiner externer Mail-Relay mit verzögerter Verarbeitung wurde nicht mehr unterstützt, und die DV-Abteilung musste von da an die Control-Files manuell bearbeiten.

Installierten Mitarbeiter die aktuellen Patches, überschreiben sie dabei zwangsläufig die



manuellen Einträge. Dadurch waren ständig umfangreiche Nacharbeiten notwendig. Hinzu kam, dass bestimmte Mail-Formate bei der Content-Security-Überprüfung auf der Firewall-Ebene nicht zutreffend erkannt und in der Folge vom Server nicht fehlerfrei bearbeitet werden konnten. Teilweise wurden die Mails nur noch unleserlich den Empfängern zugestellt.

### Security-Appliances erste Wahl

Hinzu kam die zunehmende Spam-Flut, sodass sich die Abteilung Kommunikation & DV der Augsburgener Allgemeinen zum Handeln gezwungen sah. Dabei hatten die Techniker eine sehr klare Vorstellung, wie sie vorgehen wollten: Die bestehenden Systeme sollten durch neue Security-Appliances ersetzt und vom Hersteller jederzeit mit Updates versorgt werden. Für die Lösung im Bereich E-Mail Sicherheit wurde ein differenziertes Anforderungsprofil erstellt. Keinerlei unerwünschte Mails sollten mehr zugestellt werden – das stand ganz oben auf der Wunschliste, sowohl bei Anwendern als auch bei Administratoren.

„Die Content-Filterung sollte vollständig auf dem externen Mail-Relay stattfinden und nicht mehr die Firewall belasten“, lautete die Vorgabe von Norbert T. Schmözl, der in der Gruppe Netzwerkmanagement bei der Abteilung Kommunikation & DV der Augsburgener Allgemeinen unter anderem für die Mail-Systeme verantwortlich zeichnet. Außerdem sollte der gesamte

E-Mail-Verkehr mit mindestens zwei voneinander unabhängigen Methoden auf Spam hin überprüft werden. Zwei externe Mail-Relays sollten ferner redundant ausgelegt werden, damit bei Ausfall eines Gerätes das andere einspringen könnte. „Ein zusätzlicher Vorteil einer Appliance gegenüber einer Softwarelösung ist das standardmäßig gehärtete Betriebssystem“, argumentiert Schmözl weiter.

Mit der Implementierung des Systems beauftragte das Verlagshaus die Networkers AG auch deswegen, weil das Systemhaus aus Hagen eine Niederlassung im 80 Kilometer von Augsburg entfernten Neu-Ulm besitzt. „Außer den Referenzen gaben für uns die detaillierte Beratung im Vorfeld und der gute Kontakt zu Technik und Service den Ausschlag für die Networkers“, begründet Schmözl von der Augsburgener Allgemeinen die Wahl.

Nach intensiven Recherchen und Beratungen entschied man sich gemeinsam für die „Mxtreme-200“-Security-Appliances von Borderware Technologies. Auch zu diesem Hersteller unterhält das Systemhaus aus Hagen enge Kontakte: „Wir sind entsprechend früh und unmittelbar an der Entwicklung von IT-Security-Lösungen beteiligt. Das bedeutet kürzere Produktionszyklen und ist bei der Beratung unserer Kunden ein entscheidender Vorteil“, erläutert Ralf Sander, Marketingleiter bei der Networkers AG, die Entscheidung zugunsten von Borderware.

Fortsetzung auf Seite 32 →

→ Fortsetzung vom Seite 30

Doch die Verantwortlichen bei der Augsburgener Allgemeinen wollten nicht die Katze im Sack kaufen. An einen ersten einwöchigen Test schloss sich die einmonatige Evaluierungsphase in der endgültigen Konfiguration an. Die eigentliche Inbetriebnahme nahm anschließend nur zwei Arbeitstage in Anspruch, danach stand die Lösung einsatzbereit. „Unsere Anforderungen wurden hiermit erfüllt, auch hinsichtlich der Kosten-Nutzen-Relation“, beurteilt Scholz das Projekt. So haben die beiden Borderware-Security-Appliances zusammen weniger als 15.000 Euro gekostet. Etwas mehr als 2.600 Euro gab der Kunde für die Arbeit des Dienstleisters aus.

Dafür konnte der Mail-Bastion-Host vor der Firewall außer Betrieb genommen werden. Ursprünglich war er dafür vorgesehen, Mail-Angriffe abzufangen und Überlastungen abzufedern. Diese Arbeit übernahmen nun die zwei Mxtreme-Systeme. Die Lastverteilung auf die beiden E-Mail-Firewalls erfolgt jetzt via DNS-Round-Robin, das heißt die Borderware-Appliances werden im laufenden Betrieb abwechselnd angesprochen. Die geplante 50-zu-50-Verteilung ist bereits Realität.

**Anti-Spam-Richtlinien**

Damit ein Spam-Filter einwandfrei seine Arbeit verrichten kann, muss er ständig an die sich fortwährend ändernde E-Mail-Werbeflut angepasst werden. Dabei werden verschiedene Methoden eingesetzt. Mittels des so genannten „Source Adress Filtering“ (SAF) listet beispielsweise die Firewall alle als vertrauenswürdig eingestuft internen Mailserver auf. Diese Server sind entsprechend autorisiert, Mails an beliebige Ziele bei m Kunden zu senden. Als nächster Schritt kommen White- und Blacklisting-

Verfahren (WBL) zum Zuge. Mit dieser Filtermethode können Benutzer selbstständig ihr persönliches Spam-Muster definieren, indem sie Mails mit bestimmten Header- oder Textinhalten als Werbemüll beschreiben. So konnten die User selbst gleich mehrere hundert Domains bestimmen, von denen in Zukunft keinerlei Mails mehr angenommen werden.

Hinzu kommen statistische Auswertungen der eingehenden elektronischen Briefe. So ermittelt beispielsweise das Distributed-Checksum-Clearinghouse (DCC)-Verfahren über eine Prüfsumme, ob eine Massen-Mail via pure Häufigkeit als Spam klassifiziert werden kann. Diese Methode haben die Spezialisten bei der Augsburgener Allgemeinen als die nächste Hierarchiestufe in der Spam-Erkennungs-Skala definiert. So werden alle eingehende Mails, die bei der DCC-Prüfung über einem gewissen Schwellenwert liegen, automatisch mit dem Vermerk „Spam“ in der Betreffzeile gekennzeichnet. Daraufhin kann jeder Empfänger selbst entscheiden, was mit dieser Mail passieren soll.

Als weitere Spam-Erkennungsverfahren kommt die so genannte Statistical-Token-Analyse (STA) zum Zuge. Diese Methode basiert auf bayesischen Filterregeln, die Spam anhand bestimmter dort vorkommender Wörter und Satzteile erkennen und unternehmensspezifisch kategorisieren können. Gemäß den Empfehlungen des Herstellers betrieb die Augsburgener Allgemeine ihre Mail-Firewall in den ersten zwei Wochen in einem Trainingsmodus. Dabei bestimmten die Anwender selbst, welche E-Mails sich als nützlich und welche als Müll erwiesen. Gleichzeitig definiert sie die Ausdrücke in der Betreffzeile und im Body-Text, die auf Spam hindeuten. Anhand die-

ser Kriterien erzeugt die STA-Prüfung einen Wert zwischen 0 (kein Spam) und 99 (definitiv Spam). Mittels der frei definierbaren Schwellenwerte können die unterschiedlichen Verfahren (DCC, WBL, STA) die eingehenden Mails den Kategorien „Ham“ (definitiv kein Spam), „vielleicht Spam“ und „ganz sicher Spam“ zuordnen.

Im Falle der Augsburgener Allgemeinen wurde der obere Schwellenwert mit 80, der untere mit 50 beziffert. Wird der obere Schwellenwert überschritten, wird die Mail eindeutig als Spam qualifiziert. Lediglich in der 30-tägigen Test- und Trainingsphase wurden die Mails noch mit dem Text-String „sehr wahrscheinlich Spam“ gekennzeichnet. Danach wurden sie umgehend gelöscht.

Bei der Konfiguration von Mxtreme legten die Networkers-Techniker auch die Größe der eingehenden Mails auf einen Maximalwert fest. Auch elektronische Briefe, die Unregelmäßigkeiten aufweisen, werden potenziell als so genannte „Malformed Messages“ gekennzeichnet und automatisch in die Quarantäne verschoben. Empfänger und Administrator erhalten zeitgleich eine E-Mail, die sie dar-

**Rechenbeispiel aus der Praxis**

Um die Amortisation einer Spam-Filter-Lösung nachvollziehbar zu machen, hat die interne Datenverarbeitung der Augsburgener Allgemeinen eine entsprechende Statistik in der Praxis erstellt. Man ging von einem täglichen Volumen von ungefähr 7.000 Mails aus. Das entsprach dem Durchschnitt der zurückliegenden drei Monate. Der Anteil eingehender elektronischer Briefe daran belief sich auf 60 Prozent, jener der ausgehenden Mails auf 40 Prozent. Tag für Tag kommen also etwa 4.800 E-Mails an – mit insgesamt 1.300 Nutzern ist dies eine noch sehr konservative Schätzung. Bei einer angenommenen Spam-Quote von 25 Prozent am Gesamtmailaufkommen ergibt das zirka 1.000 unerwünschte Botschaften pro Tag – eine Zahl, die sich im Übrigen mit der über die Mxtreme-Appliance geführten Statistik deckt.

Daraus zieht der E-Mail-Verantwortliche bei der Augsburgener Allgemeinen folgende Schlüsse: „Wenn man annimmt, dass ein User fünf Spam-Mails in der Minute aufmachen, quer lesen, klassifizieren und gegebenenfalls löschen kann, errechnet sich schon daraus ein Wert von 3,5 vergeudeteten Arbeitsstunden täglich. Und dies gilt für alle Tage im Jahr, Spam hält sich nämlich nicht an Wochenenden und Urlaubszeiten. Insgesamt ergibt sich daraus jährlich ein Verlust von 31.000 Euro pro Jahr (1.250 Stunden à 25 Euro).“

Das gesamte Projekt – inklusive aller Dienstleistungen – kostete den Kunden aber nur etwa 17.500 Euro. Sicherlich, nun kommt noch der Aufwand für die Administration der Borderware-Appliances hinzu. Dieser beläuft sich laut Schmölg aber auf maximal 20 Stunden monatlich. Bei einem Stundensatz von 25 Euro ergibt sich also hier eine Amortisationszeit von weniger als 8,5 Monaten. **RW**

über informiert. Für den Bereich „Attachment Filtering“ erstellte der Dienstleister gemeinsam mit dem Kunden eine Liste von erlaubten anzuhängenden Dateitypen. Treffen nicht zugelassene Dokumente ein, kommen sie ebenfalls in Quarantäne. Ausgehende Mails mit nicht zugelassenen Anhängen landen unmittelbar im Müllkorb.

**Sicherer E-Mail-Zugang**

Ziel des Projekts bei der Augsburgener Allgemeinen war es, künftig E-Mails sicher und schneller zuzustellen. Bisher hatte man eine Verzögerung von zirka fünf Minuten in Kauf genommen. Dabei war es bis dato nur eingeschränkt möglich, eingehende Mails in Quarantäne zu schicken. Sie mussten entweder gleich verworfen oder in das interne Netzwerk weitergeleitet werden. Nur mit manuellen Eingriffen in die Konfiguration ließ sich eine Mail vor den LAN-Toren „festhalten“. „Das wollten wir deutlich komfortabler haben“, erzählt Schmölg. „Ein Knopfdruck, und keine Mail gelangt mehr nach innen. Schließlich ist die Ursache einer plötzlich auftretenden Mail-Flut nicht immer sofort ersichtlich. Jetzt haben wir die Möglichkeit, in Ruhe zu analysieren, was im Netzwerk vor sich geht und können entsprechend geeignete Gegenmaßnahmen umsetzen.“

Mit Hilfe des „iNotes Proxy“ der Mxtreme-Appliance können ausgewählte Benutzergruppen mit „iNotes Web Access“ via Web direkt auf den Notes-Server zugreifen. Die jeweiligen Benutzer werden direkt auf der Maschine angelegt. „Wir arbeiten in einer Notes-Domino-Umgebung, sodass diese Funktion für uns ein richtiger

Mehrwert ist. Jetzt können ausgewählte Nutzer von Browser aus auf unser Kommunikationssystem zugreifen“, so Schmölg. Die zusätzlich installierte Antiviren-Option von Kaspersky Labs soll das System vor Würmern schützen.

„Die Networkers hatten ganz Recht mit ihrer Prognose, dass wir die Borderware-Geräte nach dem Test nicht mehr zurückgeben“, zieht Schmölg sein persönliches Resümee. Die Inbetriebnahme der Appliances führte in dem Verlags-haus zu einer deutlichen Entspannung in der internen Hotline- und User-Help-Desk-Abteilung. Auch die Mitarbeiter reagierten positiv auf das Ausbleiben der Werbebotschaften. Schließlich waren zuvor mehr als ein Viertel aller Mails definitiv Spam. „Unsere Anforderungen sind erfüllt. Auch die Wünsche nach zusätzlichen Komfort-Features hat die Networkers AG schnell aufgenommen und Verbesserungen bei kleineren technischen Problemen zeitnah realisiert. Wir hatten den Eindruck, dass der Hersteller auf solche Rückmeldungen aus der Praxis wartet, um das Produkt nach den Anwenderbedürfnissen weiter zu entwickeln“, so das Fazit des E-Mail-Verantwortlichen bei der Augsburgener Allgemeinen.

**Meinung des Redakteurs**

Der Kampf gegen Spam ist zwar eine Last für den Anwender, doch gerade hier liegen noch Umsatzpotenziale für Systemhäuser brach. Entweder sie installieren die entsprechenden Security-Appliances direkt beim Kunden, oder sie übernehmen die Filterung gleich selbst.

SOLUTION SNAPSHOT	
<b>Kunde</b>	Augsburger Allgemeine, www.augsburger-allgemeine.de
<b>Problemstellung</b>	exponentieller Anstieg von Spam; bestehende Mail-Relay-Lösung nur manuell konfigurierbar; Firewall mit Content-Filter überlastet
<b>Lösung</b>	zwei geclusterte „Mxtreme 200“-Mail-Firewall-Systeme mit Antivirensoftware von Kaspersky Labs
<b>Dienstleister</b>	Networkers AG, www.networkers.de
<b>Technologielieferant</b>	Borderware Technologies, www.borderware.de
<b>Kontaktaufnahme</b>	Empfehlungen in der Region; Kontakt auf einem Roundtable des Dienstleisters zum Thema IT-Sicherheit
<b>Verhandlungsdauer</b>	Entscheidung über eine Evaluierung der Borderware-Produkte bereits auf dem Roundtable getroffen
<b>unerwartete Schwierigkeiten</b>	kleinere technische Probleme während der Implementierung; Berücksichtigung zusätzlicher Kundenwünsche
<b>Projektverlauf</b>	Vorbereitung: eine Woche; Evaluierung: ein Monat; Implementierung: zwei Tage
<b>Kostenumfang des Projekts</b>	etwa 15.000 Euro für die zwei Mxtreme-200-Einheiten von Borderware mit Kaspersky-Antivirus-Lizenzen
<b>Kostenaufteilung</b>	85 Prozent für die Appliances, 15 Prozent für Dienstleistung
<b>Benefit für Kunden</b>	Lösung in acht Monaten amortisiert; Spam weitgehend beseitigt; Entlastung von User-Help-Desk und Hotline; geringer Administrationsaufwand; sicherer E-Mail-Zugriff; Antivirenlösung integriert
<b>Benefit für den Dienstleister</b>	wichtigen Referenzkunden gewonnen