

Die Vorteile eines gehosteten Security-Modells

Ein Whitepaper von Osterman Research

Veröffentlicht im Juli 2009

MIT FREUNDLICHER UNTERSTÜTZUNG DURCH

websense®



Osterman Research, Inc. • P.O. Box 1058 • Black Diamond, Washington 98010-1058
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com • www.ostermanresearch.com

Zusammenfassung

Security ist ein absolut wichtiger Bestandteil der E-Mail- und Web-Infrastruktur jedes Unternehmens. Angesichts der zunehmenden Menge von Spams, Viren, Würmern, Trojanern, Blended Threats etc. sowie der immer raffinierteren Attacken von Spammern und anderen Angreifern benötigen Unternehmen eine solide, anpassungsfähige Abwehr, um ihre Netzwerke, Anwender und Daten vor zahlreichen Schwachstellen zu schützen. Rund 90% aller E-Mails sind zum Beispiel Spams, und etwa eine von 100 E-Mails beinhaltet Viren. Da aber die E-Mail-Nutzung jährlich um rund 20% steigt, nimmt gleichzeitig auch die Zahl der Spams, Viren und anderer Malware zu. Als Reaktion auf diese Tendenz sollten Unternehmen eine eigene Messaging-Security-Infrastruktur aufbauen.

Ein drastischer Anstieg ist ebenfalls bei böartigem Web-Content zu beobachten. Dazu zählen E-Mail-Messages, die Links zu gefährlichen Webseiten enthalten, Attachments, die eigentlich nur als Stage-one-Downloader eines anderen Malicious Code aus dem Internet dienen, oder Malware, die einen Kommunikationskanal installiert und ihn dem Angreifer öffnet. In der Regel gelingt es diesen Malware-Seiten, mehr Zombie-Bots zu generieren, die den Teufelskreis von Spams und Viren weiter nähren.

Vor Ort E-Mail- und Web-Security-Funktionen einzurichten, ist allerdings kostspielig und zeitintensiv. Unternehmen müssen viel Geld für Hardware, Software, Training und Wartungsverträge etc. ausgeben, um ihren Schutz aufbauen und aufrechterhalten zu können. Zudem wird in der Malware-Branche enorm viel Geld verdient, so dass Spammer, Phisher und andere die notwendigen Mittel erhalten, um noch raffiniertere und umfangreichere Angriffe zu entwickeln. Unternehmen, die Messaging-Security-Probleme nicht angemessen angehen, müssen mit finanziellen und gesetzlichen Haftungsrisiken rechnen, die sich daraus ergeben können, dass sie den gesetzlichen Anforderungen und anderen Risiken nicht entsprechen.

Unternehmen, die Messaging-Security-Probleme nicht angemessen angehen, müssen mit finanziellen und gesetzlichen Haftungsrisiken rechnen, die sich daraus ergeben können, dass sie den gesetzlichen Anforderungen und anderen Risiken nicht entsprechen.

Dieses, von Websense gesponserte, Whitepaper untersucht, wie Unternehmen heute auf die zunehmende Menge und neue Arten von E-Mail-Bedrohungen reagieren. Zweck der Studie ist es einzuschätzen, wie hoch die tatsächlichen Kosten des Einsatzes einer Messaging-Security-Infrastruktur im Vergleich zu einem gehosteten Modell sind. Ziel war, die tatsächlichen Kostenunterschiede zwischen Modellen verschiedener Größen, Unternehmen und Netzwerk-Topologien zu ermitteln und reale Daten für Best-Practice-Empfehlungen zu sammeln.

Hintergrund und Methodologie

Websense beauftragte Osterman Research, eine weltweite Studie über Messaging-Entscheider durchzuführen, um ihre Management-Kosten für E-Mail-Security-Funktionen zu ermitteln, festzustellen, wie sie die Effizienz ihrer Infrastruktur vor Ort selbst

einschätzen, und andere Fragen zu klären. Insgesamt wurden 818 Umfragen in kleinen, mittleren und großen Unternehmen in Nordamerika, im EMEA-Raum (Europa/Nahost/Afrika) und im asiatisch-pazifischen Wirtschaftsraum (APAC) durchgeführt. Die Umfrage wies folgende Spezifika auf:

- Im Februar und März 2008 wurden Online-Umfragen durchgeführt.
- 364 Umfragen fanden in Nordamerika, 239 im EMEA- und 215 im APAC-Raum statt.
- Die durchschnittliche Zahl der in den Unternehmen befragten Mitarbeiter lag bei 1.500.
- Die durchschnittliche Zahl der in den Unternehmen befragten E-Mail-Nutzer lag bei 1.275.
- Alle Befragten kannten sich gut mit der Messaging-Security-Infrastruktur ihres Unternehmens aus.

Die wichtigsten Studien-Ergebnisse

Die oben genannte Studie, die speziell für das vorliegende Whitepaper durchgeführt wurde, lieferte viele interessante Antworten auf die Frage, wie Messaging-Security-Systeme in Unternehmen in aller Welt gemanagt werden. Die Studie zeigte, welche Kosten aus dem Management einer Messaging-Security-Lösung vor Ort resultieren; auf gehostete Messaging-Security geht dieses Whitepaper später ein.

- **Die vor Ort anfallenden Kosten sind beträchtlich**

Die durchschnittliche Zahl der von Antivirus- und Antispam-Servern unterstützten Anwender beträgt 250 bzw. 260. Wenn wir nach vorsichtiger Schätzung annehmen, dass sich die Kosten für Hardware und Security-Software auf insgesamt \$5.000 belaufen, liegen die Kosten nur für den Server bei \$20 pro Anwender bzw., über die typische Lebensdauer üblicher Messaging-Systeme von drei Jahren gerechnet, bei unter \$7 pro Anwender. Antivirus- und Antispam-

Appliances unterstützen eine etwas höhere Zahl von Anwendern: Die mittleren Werte lagen bei 273 bzw. 338. Wenn wir davon ausgehen, dass eine Appliance zur Unterstützung dieser durchschnittlichen Anwenderzahlen \$4.000 kostet, dann liegen die Kosten pro Anwender bei rund \$14 oder bei knapp \$5 pro Anwender und Jahr.

Allerdings ist es wichtig darauf hinzuweisen, dass die Unternehmen aufgrund der steigenden Anzahl von Spams, Web-Bedrohungen und Malware während der Lebensdauer von drei Jahren zusätzliche Hardware für die meisten Infrastrukturelemente einsetzen müssen, so dass sich die oben genannten Zahlen in etwa verdoppeln.

*Die geschätzten Kosten für die Verwaltung von Messaging-Security vor Ort liegen etwa zwischen **\$136 und \$138 pro Anwender und Jahr** oder bei **mehr als \$11 pro Anwender und Monat.***

- **Die IT-Personalkosten für das Security-Management sind beträchtlich**

Im Durchschnitt kann jeder auf IT-Security spezialisierte Mitarbeiter 875 E-Mail-Anwender unterstützen. Wenn wir davon ausgehen, dass das Jahresgehalt einschließlich aller Nebenkosten (Gehalt, Urlaubsgeld, Zusatzleistungen etc.) für einen IT-Mitarbeiter bei \$90.000 liegt, belaufen sich die jährlichen IT-Arbeitskosten auf \$103 pro E-Mail-Anwender.

Die Verwaltung der Security-Infrastruktur umfasst zahlreiche Aufgaben wie den Einsatz von Hardware, Software und Appliances; außerdem muss sichergestellt werden, dass das gesamte System in der Regel zu 100% der Zeit laufen muss; es sind Patches und Upgrades zu installieren sowie die Kapazität zu planen, damit sichergestellt ist, dass die Infrastruktur nicht durch Spam-Spitzen überlastet wird u.v.m.

Interessanterweise ergab unsere Studie, dass die Zahl der von IT-Mitarbeitern unterstützten Anwender in Nordamerika etwas höher liegt als im EMEA- und APAC-Raum, was wir darauf zurückführen, dass der nordamerikanische Markt stärker entwickelt ist, dass die Messaging-Security-Systeme seit längerer Zeit in Gebrauch sind und dass der Wirkungsgrad der IT-Arbeit größer ist.

- **Auch die personalunabhängigen Kosten sind hoch**

Die Unternehmen investieren in ihre Messaging-Security-Infrastruktur einen erheblichen Betrag für die personalunabhängigen Kosten. Nordamerikanische Unternehmen geben zum Beispiel pro Jahr durchschnittlich fast \$28 pro Anwender für Wartungsverträge, Softwareaktualisierungen, neue Hardware usw. aus. Unternehmen im EMEA-Raum geben knapp über \$29 pro Anwender aus, während Unternehmen im APAC-Raum pro Anwender fast \$19 investieren.

Ausgehend von den oben genannten Kosten und einer Lebensdauer der Messaging-Security-Infrastruktur von drei Jahren, liegen die geschätzten Kosten für die Verwaltung von Messaging-Security vor Ort etwa zwischen \$136 und \$138 pro Anwender und Jahr oder bei mehr als \$11 pro Anwender und Monat.

- **IT-Mitarbeiter benötigen umfangreiches Training**

Der IT-Trainingsbedarf ist ebenfalls beträchtlich; der durchschnittliche IT-Mitarbeiter muss anfangs durchschnittlich 30 Trainingsstunden absolvieren, in jedem Folgejahr durchschnittlich 20 weitere. Für einen Zeitraum von drei Jahren und bei einem Jahresgehalt einschließlich aller Nebenkosten in Höhe von \$90.000 belaufen sich die Kosten für jeden IT-Mitarbeiter umgerechnet auf \$3.076 sowie fast zwei Trainingswochen, um Messaging-Security-Funktionen zu lernen bzw. sich auf den aktuellen Stand zu bringen.

- **Die Bandbreite wird entscheidend durch den Messaging-Traffic beeinflusst**

Die in den befragten Unternehmen verfügbare durchschnittliche Bandbreite liegt bei 592 Mbit/sec; allerdings war die Bandbreite mit 734 Mbit/sec in nordamerikanischen Unternehmen am größten, gefolgt von 534 Mbit/sec im EMEA- und 427 Mbit/sec im APAC-Raum. Wie nicht anders zu erwarten, macht der SMTP-Traffic einen erheblichen Anteil der verfügbaren Bandbreite aus, der im Durchschnitt bei 29% liegt.

Dies wirkt sich massgeblich auf die Gesamtbetriebskosten der Messaging-Security vor Ort aus. Angesichts steigender Spam- und Malware-Zahlen wird auch ein größerer

- **Das Vertrauen in die Messaging-Security vor Ort ist nicht groß**

Viele Unternehmen haben kein großes Vertrauen in die Fähigkeiten ihrer Antispam- und Antivirus-Funktionen. So sagten uns 73% der Unternehmen, dass sie zuversichtlich bzw. sehr zuversichtlich sind, dass ihre Antivirus-Infrastruktur in der Lage ist, alle Viren, Würmer, Trojaner und andere Bedrohungen erfolgreich abzuwehren; nur 61% der Unternehmen waren genauso zuversichtlich, dass ihre Antispam-Infrastruktur in der Lage ist, unerwünschten Content abzuwehren. Das bedeutet, dass die Unternehmen zu einem erheblichen Teil kein Vertrauen in ihre aktuellen Messaging-Security-Schutzmaßnahmen haben.

Diese Daten belegen, dass die Unternehmen ihre Anfälligkeit für die vielfältigen Bedrohungen selbst als hoch einschätzen, was ja auch den Tatsachen entspricht, und lassen erkennen, dass die Unternehmen nicht so gut geschützt sind, wie sie sein sollten.

- **Wie sieht es mit gehosteten Lösungen aus?**

Die meisten Unternehmen dachten noch nicht über einen Wechsel zu einer gehosteten E-Mail-Security-Lösung nach. Viele Unternehmen unterschätzen häufig die Kosten für das Management ihrer Infrastruktur vor Ort und nehmen an, dass es immer kostengünstiger ist, die Messaging-Security intern zu verwalten. Oder sie kennen nicht den hohen Security-Level, den gehostete Lösungen im Vergleich zum unternehmensinternen Management bieten.

Osterman Research stellte fest, dass die Entscheider zunehmend empfänglich für den Gedanken sind, wichtige Anwendungen wie die Messaging-Security zu hosten.

Viele Unternehmen haben kein großes Vertrauen in die Fähigkeiten ihrer Antispam- und Antivirus-Funktionen.

In diesem Sinne glauben die meisten Entscheider, dass gehostete Messaging-Security-Angebote zahlreiche Vorteile bieten können wie zum Beispiel geringere Kosten für die IT-Arbeit und Upgrades, verbesserte Erkennungsraten bei Spams, Viren und anderen Bedrohungen sowie eine größere Flexibilität.

- **Die Konzentration auf einen Anbieter wird als Vorteil gesehen**

Rund die Hälfte der Entscheider in den Unternehmen glaubt, dass es sinnvoll bzw. sehr sinnvoll wäre, die Internet-Security, die Datensicherheit, die E-Mail-Security und andere damit zusammenhängende Funktionen auf einen einzigen Anbieter zu konzentrieren. Interessanterweise ging von sechs Unternehmen nur eines davon aus, dass ihm eine solche Konzentration keinen Wert bietet.

Die Vorteile des gehosteten Security-Modells

Gehostete E-Mail- und Internet-Security können Unternehmen jeder Größe zahlreiche Vorteile bieten wie z.B. geringere Betriebskosten im Vergleich zu Vor-Ort-Lösungen, einfacheres Management von Security-Funktionen und bestmöglichen Schutz vor Bedrohungen.

REDUKTION DER GESAMTBETRIEBSKOSTEN

Viele Entscheider glauben, dass es weniger kostspielig ist, E-Mail- und Internet-Security intern zu verwalten als die Funktionen gehosteter Modelle zu nutzen. Für größere Unternehmen (über 1.500 Arbeitsplätze) kann diese Einschätzung richtig sein, häufig ist sie es aber nicht. Oft berücksichtigen die Entscheider zum Beispiel nicht die Gesamtkosten, die anfallen, wenn sie ihren Mitarbeitern E-Mail-Security und andere Funktionen zur Verfügung stellen. Oftmals unterschätzen sie den Gesamtumfang der Arbeiten, die für das Management des Systems erforderlich sind, das Störpotenzial von Ausfällen und anderen unvorhergesehenen Ereignissen bei sonstigen IT-Aktivitäten, die wahren und vollständigen Kosten für Kapitalaufwendungen, die unerwarteten Kosten für das unternehmensinterne Management eines Systems, den Strom- und Kühlbedarf im Zusammenhang mit dem Hardware-Management vor Ort und so weiter.

Außerdem kennen die meisten Entscheider die tatsächlichen Kosten für die Bereitstellung von E-Mail- und anderen Dienstleistungen nicht. 2007 fragte Osterman Research zum Beispiel Entscheider im Messaging-Bereich, wie genau sie die Kosten der Bereitstellung von Messaging-Dienstleistungen für ihre Anwender im Blick haben. Die Umfrage ergab, dass 8 % der Befragten genau wussten, wie hoch diese Kosten waren. 25% nahmen Schätzungen vor, die um plus oder minus 10% von den tatsächlichen Kosten abwichen. Das bedeutet, dass zwei Drittel der Entscheider im Messaging-Bereich die tatsächlichen Kosten für die Bereitstellung von Messaging-Dienstleistungen in ihren Unternehmen nicht kannten.

Da viele Entscheider die vollständigen Kostenauswirkungen des Infrastrukturmanagements vor Ort unterschätzen und die meisten die Kosten für Einsatz und Management nicht genau kalkulieren können, ist vielen nicht klar, dass es oft kostengünstiger ist, die E-Mail-Security-Funktionen an einen externen Anbieter zu vergeben. Dies gilt für die Fixkosten – also die Kosten, die für das Unternehmen direkte Kosten sind – ebenso wie für die Opportunitätskosten. Für letztere gilt: Da durch einen gehosteten Anbieter IT-Mitarbeiter für andere Arbeiten freigestellt werden können, kann dies für das Unternehmen wertvoller sein, als wenn sie das interne Management der E-Mail-Security-Infrastruktur übernehmen.

REDUKTION DER KOMPLEXITÄT UND DER UNSICHERHEIT

Die E-Mail-Security stellt ein zunehmend komplexes Gebiet dar. Die Komplexität und Menge an neuen Bedrohungen sowie Spitzen im Malware-Traffic können zu zahlreichen Problemen führen. In Unternehmen, die ihre eigene Security-Infrastruktur betreiben, kann dies eine Auslastung der internen Kapazitäten oder eine Kompromittierung der Systeme und daraus resultierend eine Leistungsverminderung oder den kompletten Absturz des internen Netzwerk zur Folge haben. Aufgrund des enormen Anstiegs von Spam zwischen Mai und November 2006, der von Botnets und Bilder-Spams ausgelöst wurde, stießen zum Beispiel viele Vor-Ort-Lösungen an ihre maximalen Kapazitätsgrenzen. In vielen Unternehmen mussten IT-Mitarbeiter schnell neue Server

und Appliances integrieren und sich den von der unvorhergesehenen Spam-Flut verursachten Problemen widmen.

Eine gehostete Lösung kann die Komplexität und Unsicherheit erheblich reduzieren, die aus neuen Bedrohungen und einer steigenden Zahl von Spams und Spyware etc. resultieren. Da die Anbieter gehosteter Lösungen die Hauptlast dieser Probleme zu tragen haben und über leistungsfähigere Funktionen verfügen, als sich die meisten Unternehmen leisten können, sind ihre Kunden vor den wachsenden Problemen, mit denen sie konfrontiert sind, geschützt.

BEREITSTELLUNG VON MAXIMALEM SCHUTZ

Die Anbieter gehosteter Security führen in der Regel Updates nahezu in Echtzeit aus. So wird beispielsweise ein Anbieter von Antivirus- und Antispam-Filtering-Dienstleistungen ständig Updates der Signaturen vornehmen. Die Anbieter haben meistens Zugang zu den neuesten Bedrohungssignaturen, bevor diese an die Öffentlichkeit gelangen, und sind stets auf dem aktuellsten Stand über die Entwicklung neuer Bedrohungen. Darüber hinaus setzen die Anbieter gehosteter Lösungen in der Regel ein breiteres Spektrum von Technologien zum Schutz vor Bedrohungen ein und verfügen über Fachwissen, das für ihre Kunden, und speziell für ihre kleineren Kunden, sonst nicht verfügbar oder erschwinglich wäre.

Zudem nutzen die führenden Anbieter gehosteter Lösungen zahlreiche Antivirus-Scanner und URL-Filter, um Phishing-Attacken zu erkennen, sowie Reputationsanalyse-Funktionen, um festzustellen ob eine IP-Adresse die Quelle von echtem oder fragwürdigem Content ist. Und sie analysieren globale Traffic-Muster in Echtzeit. Das alles sind Funktionen, deren internen Einsatz und Management sich die meisten Unternehmen – vor allem die kleineren – nicht leisten können.

Die meisten Entscheider kennen nicht die tatsächlichen Kosten für die Bereitstellung von E-Mail- und anderen Services – Osterman Research stellte fest, dass zwei Drittel der Entscheider im Messaging-Bereich die tatsächlichen Kosten für die Bereitstellung von Messaging-Dienstleistungen in ihrem Unternehmen nicht wissen.

Anbieter von gehosteten Lösungen sind in der Regel in der Lage mehr Mittel in ihre Infrastruktur zu investieren als einzelne Unternehmen, und bieten ein extrem hohes Niveau an Zuverlässigkeit. Da die meisten Anbieter gehosteter Lösungen sehr leistungsfähige Datenzentren unterhalten, bieten sie normalerweise auch ein sehr hohes Niveau an Zuverlässigkeit sowie günstige Service Level Agreements (SLAs), wie sie mit intern gemanagten Systemen nur schwer zu erreichen wären. Dadurch können sich die Kunden darauf konzentrieren, Dienstleistungen bereitzustellen, die für sie von größerem Wert sind; gleichzeitig haben sie die Gewissheit, dass die Messaging-Funktionen praktisch zu 100% der Zeit zur Verfügung stehen. Es ist auch wichtig darauf hinzuweisen, dass die Datenzentren der Anbieter von gehosteten Lösungen rund um die Uhr besetzt sind und dass im Falle des Vorhandenseins eines SLA für die gesamte Betriebszeit die Funktionen und der Security-Level kontinuierlich überwacht werden. Das bedeutet, dass Probleme schneller gelöst werden können, als es den meisten Unternehmen möglich wäre, die ihre eigene Security-Infrastruktur betreiben.

Für 2009 prognostiziert Osterman Research, dass die Unternehmen planen, für viele ihrer Messaging-Funktionen gehostete Dienstleistungen in Anspruch zu nehmen, wie die folgende Tabelle zeigt. Während einige gehostete Dienstleistungen nur schwache bis mäßige Zuwächse verzeichnen werden, wird die Messaging-Security in den nächsten Jahren erheblich wachsen.

Prozentsatz der Unternehmen, die eine gehostete oder eine gemanagte Lösung nutzen

Messaging-Funktion	2007	2008	2009
Antivirus- und Antispam	22%	29%	32%
Gehostete und gemanagte E-Mail-Dienstleistungen	13%	14%	19%
E-Mail-Speicherung und -Archivierung	14%	24%	31%
Wireless/Mobility-Services	21%	21%	27%

WEITERE VORTEILE DES GEHOSTETEN MODELLS

Gehostete E-Mail- und Web-Security bietet darüber hinaus noch weitere Vorteile:

- Wenn gehostete Lösungen genutzt werden, ist häufig eine wesentlich geringere interne Netzwerk-Bandbreite erforderlich als im Falle einer Vor-Ort-Infrastruktur, da nach dem Filtern von Spams und anderer Malware sehr viel weniger Content in das interne Netzwerk gelangt. Dies bedeutet, dass eine Aufrüstung der Bandbreite später erfolgen kann, was zu erheblichen Kosteneinsparungen führt.
- Die meisten führenden Anbieter von gehosteten Security-Dienstleistungen verfügen über sehr sichere Einrichtungen, nutzen Videoüberwachung und zahlreiche Zugangspunkte, die sich auf die Technologie der Zwei-Faktor-Authentifizierung sowie auf Tracking- und Monitoring-Tools und andere Systeme stützen, welche die Daten der Kunden vor Kompromittierungen schützen. Sehen Sie sich nach Anbietern um, die nach externen Normen, wie ISO 27001, zertifiziert sind.
- Wenn man einen Anbieter von gehosteten oder gemanagten Dienstleistungen in Anspruch nimmt, wird der Kunde weniger abhängig von der Technologie eines bestimmten Herstellers. Dies verhindert, dass z.B. ein Altsystem zukünftige Entscheidungen für eine Technologie oder einen Hersteller beeinflusst.
- Anbieter gehosteter Lösungen verfügen in der Regel über eine wesentlich höhere Mail-Kapazität als ein Unternehmen, das seine eigene E-Mail-Infrastruktur vor Ort betreibt. Das liegt einfach daran, dass es für Unternehmen ökonomisch nicht sinnvoll ist, ausreichende Kapazitäten vorzuhalten, um den Betrieb beispielsweise auch im Falle einer gravierenden, umfangreichen Spam-Attacke aufrecht erhalten zu können.

Wenn gehostete Lösungen genutzt werden, ist häufig eine wesentlich geringere interne Netzwerk-Bandbreite erforderlich als im Falle einer Vor-Ort-Infrastruktur.

IST GEHOSTETE E-MAIL-SECURITY NUR ETWAS FÜR KMUs (KLEINE UND MITTLERE UNTERNEHMEN)?

Die Ansicht ist weit verbreitet, dass Anbieter einer gehosteten Security den Unternehmen, die nicht über die Mittel für eine Bereitstellung eigener Funktionen vor Ort verfügen, Kosten- und technische Vorteile bieten können. Dass es jedoch für große Unternehmen günstiger und effizienter sei, eigene Security-Funktionen einzusetzen. Osterman Research stellte jedoch fest, dass selbst sehr große Unternehmen technische und Kostenvorteile erzielen können, wenn sie gehostete Security-Lösungen in Anspruch nehmen.

Die Vorteile eines Security-Modells aus einer Hand

Noch vor einigen Jahren war es relativ einfach, das Netzwerk eines Unternehmens vor der vergleichsweise geringen Zahl von Bedrohungen durch Viren- und Würmer von Programmieren, deren Bestreben es war, bekannt zu werden, sowie der geringen Menge von Spams zu schützen, die über das Internet verschickt wurden. Aber angesichts der zunehmenden Vielfalt der Bedrohungen, ihres rasant ansteigenden Umfangs und der Vielfalt der Probleme, die heutzutage negative Auswirkungen auf ein Unternehmen haben können, müssen selbst kleine Unternehmen zahlreiche Funktionen einsetzen. Dazu zählen Funktionen, die ein Unternehmen vor Viren, Würmern, Trojanern, Spyware, textbasierten Spams, Bilderspams, PDF-Spams, bösartigen Webseiten und vielen anderen Problemen schützen.

Immer mehr Hersteller stellen spezielle Funktionen zur Filterung und zur Behebung einiger dieser Probleme zur Verfügung und einige wenige Hersteller bieten holistische Lösungen zur Behebung all dieser Probleme.

Osterman Research ist davon überzeugt, dass die Implementierung von Lösungen, die das gesamte Spektrum der E-Mail-, Web- und anderen Bedrohungen abdecken, die Einfluss auf die Unternehmensnetzwerke haben können, der beste Ansatz ist. Unter anderen sind dafür folgende Gründe zu nennen:

- Für einzelne Lösungen von verschiedenen Anbietern muss mehr IT-Mitarbeiterzeit investiert werden als für die holistische Lösung eines einzigen Anbieters, die von einem zentralisierten Interface verwaltet werden kann. Das Management einer größeren Zahl von Einzellösungen kann die Kosten für das IT-Management bisweilen in astronomische Höhen treiben.
- Jeder Anbieter hat seine eigenen Upgrade- und Patch-Managementzyklen, so dass mehr IT-Zeit investiert werden muss, um die einzelnen Lösungen zu upgraden, wobei zwischen ihnen möglicherweise auch Inkompatibilitäten auftreten können.

In den meisten Fällen können die Arbeitszeit der IT-Mitarbeiter minimiert und die Gesamtkosten gesenkt werden, wenn ein Anbieter in Anspruch genommen wird, der alle Security-Funktionen bereitstellt, die zum Schutz eines Unternehmens vor E-Mail- und Web-basierten Bedrohungen erforderlich sind.

- Der Einsatz mehrerer Einzellösungen unterschiedlicher Anbieter wird in den meisten Fällen teurer als der Einsatz einer Lösung eines einzigen Anbieters mit gleichem Funktionsumfang
- Für IT-Entscheider, die Einkaufs-, Finanz- und anderen Abteilungen ist es schwieriger und aufwändiger, mit verschiedenen Anbietern zu arbeiten als nur mit einem einzigen.

Kurz gesagt: Durch die Entscheidung für einen einzigen Anbieter, der alle Security-Funktionen bereitstellt, die zum Schutz eines Unternehmens vor E-Mail- und Web-basierten Bedrohungen erforderlich sind, können sowohl die Arbeitszeiten als auch die Gesamtkosten in den meisten Fällen gesenkt werden.

Resümee

Gehostete Security stellt für Unternehmen jeder Größe eine rentable Lösung dar und wird zunehmend eingesetzt, um die Security zu verbessern und die Kosten zu senken. Eine gehostete Lösung bietet zahlreiche Vorteile. Einer der wichtigsten ist, dass die Kunden eine Infrastruktur nutzen können, die eigens dafür ausgelegt ist, einen sehr hohen Datendurchsatz zu ermöglichen und den größtmöglichen Schutz vor Bedrohungen zu bieten – eine Infrastruktur zu reproduzieren, die von einem Anbieter gehosteter Lösungen bereitgestellt werden kann, wäre für die meisten Unternehmen einfach unerschwinglich. Gehostete Security kann, wie folgende Tabelle zeigt, in vielen Unternehmen zu Kostensenkungen führen.

**Kosten für das Management einer
Messaging-Security-Infrastruktur vor Ort für drei Jahre
(Gemäß den in der Umfrage ermittelten Daten)**

Kostenkomponente	VOR ORT		HOSTED	
	Kosten pro Anwender	Kosten pro Anwender für drei Jahre	Kosten pro Anwender	Kosten pro Anwender für drei Jahre
Personal 875 Anwender pro Administrator (Vollzeitkraft) Jahresgehalt einschließlich aller Nebenkosten/Verwaltung: 65000 € 5% Lohnsteigerung pro Jahr	73,50 € (pro Jahr)	231,6 €	3,38 € (pro Jahr)	3,38 €
Antivirus-Server-/Appliances 250 Anwender pro Server/Appliance Appliance-Kosten: 3 571 €	3,38 € (Anfangskosten)	4,76 €	0 €	0 €
Antispam-Server-/Appliances 250 Anwender pro Server/Appliance Appliance-Kosten: 3 571 €	13,73 € (Anfangskosten)	4,57 €	0 €	0 €
Auf Messaging entfallende Bandbreite 2 142 € pro Monat/1.000 Anwender 20% entfallen auf den Messaging-Traffic Spams/Malware machen 90% des Messaging-Traffic aus	0,38 € (pro Monat)	13,88 €	0,04 € (pro Monat)	1,44 €
GESAMTKOSTEN FÜR DREI JAHRE	254,81 €		11,58 €	
DURCHSCHNITTLICHE KOSTEN PRO JAHR	84,93 €		3,86 €	
DURCHSCHNITTLICHE KOSTEN PRO MONAT	7,07 €		0,32 €	

Anmerkung: Lizenz- und Abonnementsgebühren sind in diesen Zahlen nicht enthalten.

Außerdem kann durch integrierte Lösungen, die gehostete Web- und E-Mail-Security bieten, sichergestellt werden, dass die Unternehmen bestmöglich vor den sich schnell verändernden Bedrohungen geschützt sind, die sich über diese beiden am meisten genutzten Kommunikationskanäle ausbreiten.

Über Websense

Websense, Inc. (NASDAQ: WBSN), ist ein führendes Unternehmen im Bereich des integrierten Web-, Messaging- und Data-Schutzes, das weltweit über 42 Millionen Mitarbeiter in mehr als 50.000 Unternehmen mit Essential Information Protection(TM) versorgt. Die über ein globales Netz von Vertriebspartnern vertriebenen Websense Software- und Hosted-Security-Lösungen helfen Unternehmen, Malicious Code zu blockieren. Sie verhindern den Verlust vertraulicher Informationen und setzen Internetnutzungs- und Messaging-Security-Richtlinien um. Weitere Informationen erhalten Sie unter www.websense.com.

© 2008-2009 Osterman Research, Inc. Alle Rechte vorbehalten.

Ohne Genehmigung von Osterman Research, Inc. darf dieses Dokument, oder Teile des Dokuments, nicht vervielfältigt oder verteilt werden. Auch der Verkauf oder die Verbreitung durch jemand anderem als Osterman Research ist ohne vorherige schriftliche Genehmigung von Osterman Research, Inc. nicht gestattet.

Osterman Research, Inc. erteilt keine Rechtsberatung. Kein Teil dieses Dokuments stellt eine Rechtsberatung dar, und dieses Dokument oder ein hier erwähntes Softwareprodukt oder sonstiges Angebot kann nicht als Ersatz dafür dienen, dass der Leser die Gesetze einhält, auf die in diesem Dokument verwiesen wird (unter anderem Gesetze, Gesetzesbestimmungen, Vorschriften, Regelungen, Richtlinien, Verordnungen, Verfügungen usw., die hier kollektiv als "Gesetze" bezeichnet werden). Bei Bedarf sollte der Leser kompetenten juristischen Rat zu den hier angesprochenen Gesetzen einholen. Osterman Research, Inc. übernimmt keine Verantwortung oder Garantie für die Vollständigkeit oder Richtigkeit der in diesem Dokument enthaltenen Informationen.

DIESES DOKUMENT WIRD OHNE JEGliche GEWÄHRLEISTUNG ZUR VERFÜGUNG GESTELLT. AUSDRÜCKLICHE ODER KONKLUDENTE ZUSICHERUNGEN, BEDINGUNGEN UND GEWÄHRLEISTUNGEN, EINSCHLIESSLICH DER KONKLUDENTEN GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT ODER DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, WERDEN AUSGESCHLOSSEN, AUSSER IN DEM UMFANG, IN DEM EIN SOLCHER AUSSCHLUSS ALS UNZULÄSSIG GILT.