Warum Sie gehostete Messaging-Sicherheit in Erwägung ziehen sollten

Ein Osterman Research Whitepaper

Veröffentlicht: Februar 2009

GESPONSERT VON

TREND MICRO™

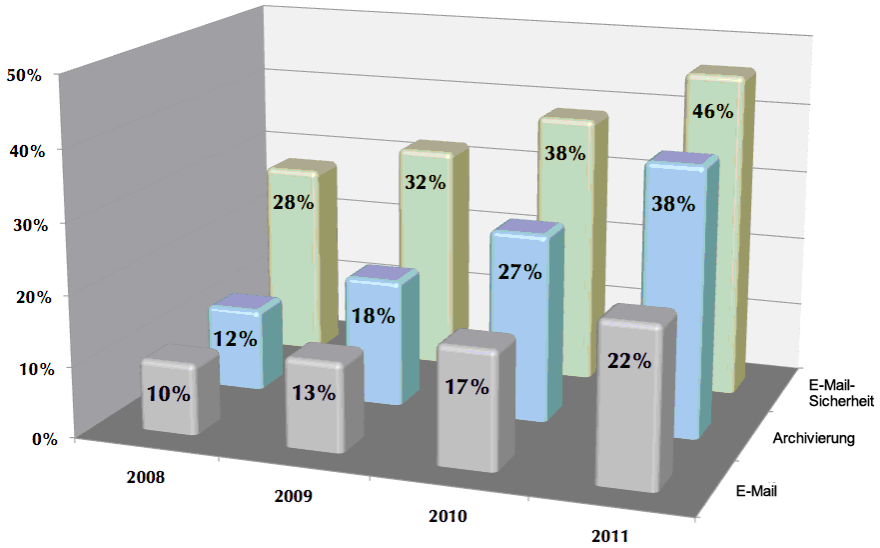
Osterman Research, Inc. • P.O. Box 1058 • Black Diamond, Washington 98010-1058
Tel.: +1 253 630 5839 • Fax: +1 866 842 3274 • info@ostermanresearch.com • www.ostermanresearch.com

Kosteneinsparungen bei gleichzeitiger Verbesserung der E-Mail-Sicherheit

Gehostete (d. h. webbasierte) Lösungen für Messaging-Sicherheit finden bei Unternehmen aller Größen immer mehr Anklang. Einige haben sich bereits für gehostete Services entschieden, während andere sich langsam mit der Idee anfreunden und nun eher Services von Dritten zur Verwaltung ihrer Sicherheitsinfrastruktur nutzen als noch vor einem Jahr. Entscheidungsträger erkennen gerade jetzt im Zuge der aktuellen Wirtschaftskrise, dass gehostete Lösungen für E-Mail-Sicherheit eine kostengünstige Alternative darstellen und gleichzeitig die Sicherheit erhöhen.

Verschiedenen Umfragen zufolge prognostiziert Osterman Research eine stetige Zunahme der verschiedenen Arten gehosteter Messaging-Services (siehe nachstehende Abbildung). Auf dem Markt webbasierter Services wird im Bereich E-Mail-Sicherheit das stärkste Wachstum erwartet. Dieser Markt wird nach allgemeinen Einschätzungen in den nächsten Jahren eine führende Rolle bei den Kategorien ausgelagerter Services übernehmen. Nach einer 2008 von Osterman Research groß angelegten Marktstudie für gehostete Services haben sich Spam- und Virenschutz als die beiden Lösungen herauskristallisiert, um die Unternehmen nach eigener Aussage ihre intern verwaltete Infrastruktur wahrscheinlich oder tatsächlich ergänzen wollen. Obwohl einige Unternehmen das Hosting ihrer gesamten E-Mail-Infrastruktur einem externen Anbieter übertragen, ist der Wert einer dedizierten gehosteten Lösung für E-Mail-Sicherheit eines Anbieters, der sich auf Content-Sicherheit spezialisiert hat, nicht von der Hand zuweisen.

Prognose für ausgelagertes Messaging in Nordamerika
Lizenzen in mittelständischen und Großunternehmen
2008-2011
(% der abgedeckten E-Mail-Benutzer im Unternehmen)



WELCHE FAKTOREN TRAGEN DAZU BEI, EINE GEHOSTETE E-MAIL-SICHERHEITSLÖSUNG ZU VERWENDEN?

Unter welchen Umständen ziehen Entscheidungsträger eine gehostete Lösung für E-Mail-Sicherheit in Erwägung? In einer speziell für dieses Whitepaper unter 117 Entscheidungsträgern im Bereich E-Mail-Sicherheit durchgeführten Umfrage gaben die Befragten an, dass es folgende Hauptkriterien sind, sich wahrscheinlich oder sehr wahrscheinlich für eine gehostete E-Mail-Sicherheit zu entscheiden: Kosteneinsparung, Datenschutz und ein etablierter Hersteller für lokal installierte Sicherheitslösungen.

Frage: „In welchem Maße beeinflussen folgende Faktoren die Wahrscheinlichkeit, dass Entscheidungsträger eine gehostete Lösung für E-Mail-Sicherheit in Betracht ziehen?“ Im Folgenden sehen Sie die Antworten der Befragten, die wahrscheinlich oder sehr wahrscheinlich von folgenden Punkten beeinflusst würden:

Antwort	%
Nachweis, dass eine gehostete Lösung für E-Mail-Sicherheit zu einer 50 %igen Kostensenkung bei der E-Mail-Sicherheit führt	71 %
Garantierter Datenschutz im Service Level Agreement zugesagt	61 %
Nachweis, dass eine gehostete Lösung für E-Mail-Sicherheit zu einer 20 %igen Kostensenkung bei der E-Mail-Sicherheit führt	59 %
Nachweis, dass eine gehostete Lösung für E-Mail-Sicherheit zu einer deutlichen Senkung der IT-Kosten für E-Mail-Sicherheit führt	58 %
Eine gehostete E-Mail-Sicherheitslösungen von einem führenden Anbieter lokal installierter E-Mail-Sicherheitslösungen	47 %

Besonders auffallend ist der Prozentsatz von Unternehmen, die eine gehostete Lösung für E-Mail-Sicherheit in Betracht ziehen würden, wenn sie dadurch Kosten einsparen könnten. Fast 60 % der Befragten wären bereit, eine gehostete Lösung zu erwägen, wenn sie dadurch 20 % an Kosten einsparen könnten, während über 70 % eine solche Lösung ins Auge fassen würden, wenn die Kosteneinsparung 50 % betragen würde.

Dieses Whitepaper zeigt die Bewertung der Kosten einer lokal installierten Lösung im Vergleich zu gehosteten Systemen für E-Mail-Sicherheit auf, einschließlich Hybridsystemen, die lokal installierte und webbasierte Funktionen vereinen. Das vorliegende Dokument basiert auf Daten aus einer speziell durchgeführten Umfrage sowie auf einer einfachen Kostenanalyse, die die Kosten von lokal installierten Systemen darstellt.

DIE KOSTEN LOKAL INSTALLIERTER E-MAIL-SICHERHEIT

Viele Entscheidungsträger sind der Meinung, dass mit einer lokal installierten Infrastruktur weniger Kosten verbunden sind als mit gehosteten Services, denn sie berücksichtigen nicht alle Kosten des intern verwalteten Systems. Die Ergebnisse der speziell für dieses Whitepaper durchgeführten Umfrage zeigen, dass 48 % der Befragten der Aussage, dass gehostete E-Mail-Sicherheit teurer ist als eine lokal installierte Gateway-E-Mail-Sicherheitslösung, weitgehend oder vollständig zustimmen. In einer 2008 durchgeführten Studie gaben 66 % kleine und 57 % Großunternehmen an, dass sie keine webbasierten Services verwenden, da die interne Verwaltung ihrer Ansicht nach kostengünstiger ist als eine Auslagerung. Ausführliche von Osterman Research entwickelte Kostenmodelle zeigen jedoch, dass die Kosten von webbasierten Sicherheitsservices – auch für Großunternehmen – deutlich geringer sind als für lokal installierte Installationen.

Die Kosten von Messaging-Sicherheitslösungen variieren je nach Unternehmensgröße, der Anzahl der abgedeckten Benutzer, der geografischen Verteilung des Unternehmens, der Anzahl der Niederlassungen und diversen anderen Faktoren sehr stark. Bei unserer Untersuchung stellte sich heraus, dass Unternehmen durchschnittlich pro E-Mail-Benutzer zur Aufrechterhaltung ihrer Infrastruktur für E-Mail-Sicherheit jährlich 63 Dollar für Hardware, Software, Lizenzverträge, physischen Speicher und sonstige anfallenden Kosten aufwenden.

Darüber hinaus zeigten die Ergebnisse, dass sowohl der Mittelwert als auch der Medianwert (Zentralwert) darauf schließen lassen, dass die zur Verwaltung der Infrastruktur für E-Mail-Sicherheit für jeweils 1000 E-Mail-Benutzer aufgebrachte Arbeitszeit einem Vollzeit beschäftigten IT-Mitarbeiter entspricht. Wenn wir davon ausgehen, dass die finanzielle Belastung des Unternehmens für diesen dedizierten IT-Mitarbeiter jährlich 80.000 Dollar beträgt, dann kostet die Bereitstellung der Verwaltung der E-Mail-Sicherheit für jeweils 1000 Benutzer 80.000 Dollar pro Jahr. Wenn man den sich hieraus ergebenden Betrag von 80 Dollar pro Benutzer zu den Kosten für Hardware, Software und sonstige lokal installierte Infrastruktur hinzuaddiert, betragen die Gesamtkosten für die interne Installation von E-Mail-Sicherheit 143 Dollar pro Benutzer pro Jahr. Das sind monatlich für jeden Benutzer fast 12 Dollar.

Benutzer	Infrastrukturkosten lokal installierter E-Mail-Sicherheit	Verwaltungskosten für E-Mail-Sicherheit	Gesamtkosten lokal installierter E-Mail-Sicherheit
1.000	63.000 $	80.000 $	143.000 $
5.000	315.000 $	400.000 $	715.000 $
10.000	630.000 $	800.000 $	1.430.000 $

Die oben aufgeführten Ergebnisse müssen relativiert werden. Osterman Research hat durch zahlreiche Studien herausgefunden, dass viele Entscheidungsträger die Bereitstellungskosten für Messaging- und ähnliche Services für Benutzer unterschätzen. Es kann außerdem nicht oft genug darauf hingewiesen werden, dass die Kosten die hier angegebenen Kosten *weit* übersteigen können. Dies gilt vor allem für kleinere Unternehmen, Unternehmen mit stark verteilten Netzwerken und Unternehmen, die in Großstädten ansässig sind und höhere Personalkosten haben.

IN WELCHEM BEZUG STEHEN DIE KOSTEN LOKAL INSTALLIERTER UND GEHOSTETER LÖSUNGEN?

Selbst wenn nur die Infrastrukturkosten berücksichtigt werden, liegen die Kosten gehosteter Lösungen für E-Mail-Sicherheit diesen Umfragen zufolge deutlich unter den Kosten pro Benutzer für lokal installierte Lösungen. Unternehmen müssen den pro Person angesetzten Betrag von 63 Dollar (oder höher) für die Verwaltung einer lokal installierten Lösung mit den Kosten pro Benutzer für gehostete Lösungen vergleichen.

Sie sollten sich ferner darüber im Klaren sein, dass sich die Einsparungen nicht nur auf die Infrastrukturkosten beschränken, sondern bei einer gehosteten Lösung auch die Verwaltungskosten zurückgehen. Auch wenn diese Lösung zur Verwaltung der E-Mail Sicherheit nicht ganz ohne Aufwand möglich ist, so können die Kosten hierfür jedoch deutlich verringert werden. In einer anderen Osterman-Studie stellte sich heraus, dass Unternehmen für jede Lösung zur Content-Sicherheit (einschließlich E-Mail-Sicherheit) pro Jahr durchschnittlich 133 Stunden für das Verwalten von Pattern-Dateien, Signaturen und sonstigen kritischen Updates sowie das Upgraden

der Ressourcenkapazität aufbringen, um die Bandbreite und die Speicherkapazität auszuweiten oder neue Server und Appliances hinzuzufügen. Diese Aufgaben sind bei einer gehosteten Lösung für E-Mail-Sicherheit überflüssig. Somit sparen Unternehmen mindestens 6,4 % (133 Stunden ÷ 2080 Stunden eines typischen Arbeitsjahres) an Verwaltungskosten.

Seltener auftretende Systemausfälle, weniger Sicherheitsverletzungen und frei gewordene Arbeitszeit können zusätzliche Einsparungen ergeben, die nun für andere, kritischere Projekte aufgewendet werden können.

- Die Auswirkungen von Systemausfällen sind vielschichtig und reichen von einem kaum spürbaren Abfall der Mitarbeiterproduktivität bis hin zu beträchtlichen Gewinneinbußen auf Grund von Umsatzverlusten oder verärgerten Kunden. Das Fazit der für dieses Whitepaper durchgeführten Untersuchung ergab, dass bei lokal installierten Systemen für Messaging-Sicherheit monatlich mit einem durchschnittlichen Systemausfall von 30 Minuten gerechnet werden muss. Dies bedeutet, dass Benutzer jedes Jahr 6 Stunden lang nicht gegen Spam, Malware oder sonstige Bedrohungen geschützt sind, ganz zu schweigen von dem beträchtlichen Zeitaufwand, den die IT-Abteilung zum Beheben dieser Systemausfälle aufbringen muss.

  Die meisten gehosteten Lösungen für E-Mail-Sicherheit werden durch Service Level Agreements ergänzt, die weniger Systemausfälle garantieren als lokal installierte Lösungen und häufig Geld-zurück-Zusagen enthalten.

- Sicherheitsverletzungen, die aus einer unzureichenden Infrastruktur für Messaging-Sicherheit oder aus Systemausfällen resultieren, können erheblichen Schaden anrichten. Unsere Untersuchungen ergaben, dass 46 % der Befragten in den vergangenen 12 Monaten einer Sicherheitsverletzung zum Opfer gefallen waren und dass die Kosten pro Sicherheitsverletzung fast 63.000 Dollar betrugen. Die Kosten von Sicherheitsverletzungen können diesen Wert allerdings weit übersteigen.

  Gehostete Lösungen für E-Mail-Sicherheit filtern E-Mail-Bedrohungen aus, bevor sie das Netzwerk erreichen und verhindern so, dass Bedrohungen geschäftliche Nachteile mit sich bringen. Bei lokal installierten Lösungen für E-Mail-Sicherheit bestehen Sicherheitslücken leider auch nach der Verfügbarkeit von Signatur-Updates allzu oft mehrere Stunden lang weiter. Umfrageergebnisse lassen darauf schließen, dass durchschnittlich über fünf Stunden vergehen, bevor Signatur-Updates in der Infrastruktur des Unternehmens verteilt werden. Bei gehosteter E-Mail-Sicherheit erhalten Unternehmen sofort den aktuellen, von ihrem Anbieter verfügbaren Schutz. Diese Vorteile können zu einer weiteren Erhöhung des Schutzes und einer Verringerung von Sicherheitsverletzungen führen und so Kosten einsparen.

- Entscheidungsträger ignorieren außerdem häufig die Opportunitätskosten, die beim Einsatz interner Mitarbeiter zur Verwaltung einer lokal installierten Infrastruktur für Messaging-Sicherheit anfallen. Zwar ist die Messaging-Sicherheit für Unternehmen von extrem hoher Bedeutung, sie können sich hierdurch jedoch nicht von der Konkurrenz abheben. Wenn dagegen mehr IT-Arbeitszeit für Projekte zur Verfügung steht, die beispielsweise die Wartezeiten von Kunden verringern, die technische Unterstützung benötigen oder auf die Beantwortung ihrer Verkaufsanfrage warten, tätigt ein Unternehmen eine Investition, die zu einem Wettbewerbsvorteil und möglicherweise zu einer Wertschöpfung führt, die die für die IT-Mitarbeiter aufgebrachten Kosten weit übersteigt. Fazit: Gehostete Lösungen für E-Mail-Sicherheit führen zu einer spürbaren Entlastung von IT-Mitarbeitern, so dass die Unternehmen diese Mitarbeiter gezielt in Bereichen einsetzen, in denen sie einen Beitrag zum Unternehmenswachstum leisten.

VERGLEICH ZWISCHEN GEHOSTETEN UND LOKAL INSTALLIERTEN LÖSUNGEN FÜR E-MAIL-SICHERHEIT

In diesem Abschnitt werden die Funktionen gegenwärtig erhältlicher gehosteter Lösungen für E-Mail-Sicherheit erörtert. Gehostete Lösungen sind nicht für alle Umgebungen geeignet, und die angebotenen Lösungsoptionen sind von Anbieter zu Anbieter unterschiedlich. Entscheidungsträger, die die richtigen Fragen stellen, können die tatsächlichen Vorteile und Verteilungsoptionen einer gehosteten Lösung für E-Mail-Sicherheit jedoch genau abwägen.

Die meisten Entscheidungsträger wollen in erster Linie wissen, ob eine gehostete Lösung gleichermaßen Kontrolle und Datenschutz bieten kann wie eine lokal installierte Lösung. Gehostete E-Mail-Sicherheit bietet meist genau die Vorteile oder Schutzmaßnahmen, die Unternehmen erwarten. In vielen Fällen werden diese Erwartungen sogar weit übertroffen. Im Folgenden wird die Auffassung eines Teils der Entscheidungsträger zusammengefasst und den Optionen gegenübergestellt, die gehostete Services für E-Mail-Sicherheit tatsächlich bieten.

KONTROLLE

- **Auffassung:** Eines der häufigsten Argumente gegen die Verwendung webbasierter Services ist der von vielen IT-Entscheidungsträgern befürchtete Verlust der Kontrolle, den die Auslagerung der Messaging-Infrastruktur nach sich ziehen könnte. Studien haben gezeigt, dass es hier um zahlreiche Kontrollfaktoren geht, darunter Sicherheit, Nachrichtenverfolgung, Berichterstattung und Richtlinienerstellung.

- **Realität:** Führende Anbieter gehosteter Lösungen bieten zumeist eine starke Kontrolle der Sicherheit, in der Regel durch Funktionen für webbasierte Verwaltung und Bereitstellung. Somit können IT-Mitarbeiter neue Benutzer hinzufügen, neue Services für spezifische Benutzer bereitstellen und im Allgemeinen das gleiche Serviceniveau wie ein lokal installiertes System bieten.

  Einige gehostete Lösungen für E-Mail-Sicherheit bieten außerdem Mail-Nachverfolgung sowie Zugriff auf Protokolle und Berichte und ermöglichen so einen Einblick in das System und die Überwachung bestimmter E-Mails. Somit können Administratoren E-Mail-Probleme beheben, auch wenn es sich um eine gehostete Lösung handelt.

Der Funktionsumfang variiert je nach Hersteller. Einige bieten auch Content-Überwachung, wie z. B. flexible Richtlinienerstellung und Content-Filter, und somit zusätzlich zum Ausfiltern von Bedrohungen wie Spam und Malware in E-Mails auch Unterstützung bei der Einhaltung von Richtlinien und der Vermeidung von Datenlecks. Es empfiehlt sich möglicherweise, dass Entscheidungsträger Hersteller konsultieren, die sowohl lokal installierte als auch gehostete Lösungen anbieten. Diese Hersteller bieten in ihrer gehosteten Lösung unter Umständen die gleichen speziell abgestimmten Funktionen wie bei ihren lokal installierten Produkten. Außerdem besteht die Möglichkeit, gehostete und lokal installierte Lösungen zu einer Hybridlösung zu kombinieren, so dass einige dieser Funktionen webbasiert und andere lokal installiert sind. Das ermöglicht Unternehmen zusätzliche Flexibilität, die lokal installierten Content-Überwachungsfunktionen den Vorzug geben, das Netzwerk jedoch durch eine gehostete Lösung vor Bedrohungen schützen möchten.

SICHERHEIT UND DATENSCHUTZ

- **Auffassung:** Messaging-Systeme speichern einen Großteil der kritischen Daten, die Unternehmen für Ihre Geschäftstätigkeit benötigen, und viele Unternehmen unterliegen Datenschutzbestimmungen, wonach die meisten dieser Daten vertraulich behandelt werden müssen. Viele Entscheidungsträger befürchten, dass beim Einsatz gehosteter Services vertrauliche Daten von skrupellosen Mitarbeitern des Service-Anbieters eingesehen oder entwendet werden könnten. Außerdem sorgen sie sich, dass der Datenschutz auf irgendeine Art und Weise gefährdet werden könnte.

- **Realität:** Gehostete Lösungen für E-Mail-Sicherheit nutzen automatische Prozesse zum Durchsuchen von E-Mails ohne jeglichen menschlichen Eingriff. Darüber hinaus bieten Hersteller ein Service Level Agreement, das den Datenschutz garantiert. Somit werden auch Datenschutzbestimmungen abgedeckt, nach denen das Unternehmen nachweisen muss, dass es für einen angemessenen Schutz von E-Mail-Inhalten sorgt.

  Außerdem bieten führende Hersteller gehosteter Lösungen einen sehr hohen physischen Schutz der Datenzentren durch Zwei-Faktor-Authentifizierung bei vielen Eingängen, Videoüberwachung, Mitarbeiterpräsenz rund um die Uhr usw. Auch wurden viele Datenzentren durch externe Zertifizierungsstellen geprüft, die diese Sicherheitsmaßnahmen validieren. Viele intern verwaltete Systeme verfügen nicht über ein vergleichbares Maß an Sicherheit.

ARBEITSPLATZSICHERHEIT

- **Auffassung:** Einige Entscheidungsträger befürchten, dass die Hersteller gehosteter Lösungen die Arbeitsplatzsicherheit der IT-Mitarbeiter gefährden, die die lokal installierte Infrastruktur verwalten.

- **Realität:** Es ist aus diversen Gründen unwahrscheinlich, dass ein Unternehmen nach dem Umstieg auf einen Anbieter gehosteter Lösungen IT-Mitarbeiter entlässt. Eine IT-Abteilung muss immer vielfältigere und komplexere Systeme verteilen und verwalten. Die Auslagerung der Sicherheit an einen Anbieter, der sich auf diesen Bereich spezialisiert hat, ermöglicht es Unternehmen, ihre IT-Mitarbeiter für Aufgaben einzusetzen, bei denen ihre Fähigkeiten besser genutzt werden können. Dadurch leisten sie direkt einen Beitrag zu den Umsatzzielen des Unternehmens.

FINANZIELLE SICHERHEIT VON ANBIETERN GEHOSTETER LÖSUNGEN

- **Auffassung:** Einige Entscheidungsträger machen sich Gedanken darüber, ob bestimmte Anbieter gehosteter Lösungen finanziell auf sicherem Boden stehen oder ob sie irgendwann ihren Betrieb einstellen.

- **Realität:** Einige Hersteller gehosteter Lösungen haben eine bessere Finanzgrundlage als andere. Diesen Aspekt können Unternehmen jedoch problemlos in der Prüfungsphase der Anbieterauswahl klären. Außerdem können Anbieter lokal installierter Systeme auch den Betrieb einstellen, so dass Kunden keine Upgrade-Möglichkeiten haben und somit genau so anfällig sind.

EINSATZ ERSTKLASSIGER LÖSUNGEN

- **Auffassung:** Einige Entscheidungsträger befürchten, dass die Anbieter gehosteter Lösungen nicht gerade erstklassige Anbieter auswählen.

- **Realität:** Eine lokal installierte Infrastruktur ist flexibler, da Unternehmen unter einer Vielzahl von Anbietern auswählen können. Allerdings bieten immer mehr führende Hersteller von Sicherheitslösungen auch eine gehostete Lösung für E-Mail-Sicherheit an. Die Hauptüberlegung bei Messaging-Sicherheit ist außerdem das Aufhalten von Malware und Spam. Am wichtigsten ist es daher, eine Lösung zu wählen, die den jeweiligen Ansprüchen am besten gerecht wird, und nicht der Wunsch, aus dem größtmöglichen Angebot wählen zu können.

Vorteile des Modells für gehostete Lösungen

Auch wenn gehostete Lösungen für E-Mail-Sicherheit einen ähnlichen Funktionsumfang und vergleichbare Vorteile wie eine lokal installierte Lösung aufweisen, bieten sie außerdem eine beträchtliche Anzahl von Vorteilen, die nur von webbasierten Sicherheitsservices geboten werden und die Entscheidungsträger prüfen und abwägen sollten:

- **Extrem niedrige Vorabinvestition**
  Im Gegensatz zu einer lokal installierten Infrastruktur erfordern gehostete Sicherheitsservices, wenn überhaupt, nur eine geringe Vorabinvestition. Einige Anbieter verlangen Einrichtungsgebühren, doch meist sind diese wesentlich niedriger als bei lokal installierter Hardware und die Kosten der für die Verteilung und Konfiguration dieser Systeme erforderlichen IT-Mitarbeiter.

- **Keine Wartung von Hardware oder Software erforderlich**
  Gehostete E-Mail-Sicherheit verwendet laut Definition keine lokal installierte Infrastruktur. Daher müssen die IT-Mitarbeiter auch keine Hardware oder Software warten. Upgrades werden vom Anbieter vorgenommen, denn dieser hat das nötige Fachwissen im Bereich Sicherheit und für die betroffene Lösung.

- **Einfache und schnelle Verteilung**
  Unternehmen müssen zum Verteilen einer gehosteten Lösung für E-Mail-Sicherheit normalerweise nur ihren MX-Eintrag so umleiten, dass er über den Service geleitet wird. Damit ist die Implementierung auch in verteilten Umgebungen ganz einfach, und die Installation der Lösung erfolgt ohne Beeinträchtigung anderer vorhandener Infrastrukturen.

- **Niedrigere Kosten für IT-Mitarbeiter**
  Wegen der geringen Verteilungskosten von webbasierten Services und des Wegfalls der normalerweise für lokal installierte Software anfallenden Wartungsaufgaben sind die IT-Kosten wesentlich niedriger. Wie bereits erwähnt, können IT-Mitarbeiter nun für Aufgaben eingesetzt werden, die dem Unternehmen eine größere Wertschöpfung einbringen als das Installieren von Software-Patches und Verwalten von Spam-Filtern.

- **Besser vorhersagbare Kosten**
  Die Kosten einer lokal installierten Infrastruktur können oft nicht genau abgeschätzt werden. Bei einer starken Zunahme von Spam müssen Unternehmen zum Beispiel häufig neue Hardware, Software oder Appliances anschaffen und verteilen, um sich gegen diese neue Bedrohung zu wappnen. Dieser Fall tritt bei gehosteten Services praktisch nie ein, da Anbieter webbasierter Lösungen das zusätzliche Malware- und Spam-Aufkommen fast ausnahmslos absorbieren, ohne die Kosten für Speicher und Bandbreite an ihre Kunden weiterzugeben. Unternehmen zahlen in der Regel eine benutzerbasierte monatliche oder jährliche Abonnementgebühr und wissen somit genau, was an Kosten auf sie zukommt.

- **Schnellere Reaktion auf neue Bedrohungen**
  Bei gehosteten Lösungen für E-Mail-Sicherheit kann der Anbieter die Lösung direkt mit den neuesten Schutzkomponenten aktualisieren. Er kann allgemeine Lösungsupdates anwenden, ohne diese Updates als „neue“ Produktversion aufzulegen. Unternehmen mit einer lokal installierten Lösung lassen sich mit der Verteilung neuer Versionen oft relativ viel Zeit – insbesondere Großunternehmen, die mehrere Server aktualisieren müssen. Die Verwendung älterer Produktversionen kann sich jedoch nachteilig auf die Wirksamkeit der Lösung auswirken. Bei gehosteter E-Mail-Sicherheit erhalten Kunden den aktuellen, von ihrem Anbieter verfügbaren Schutz.

- **Andere Vorteile**
  Gehostete Lösungen für E-Mail-Sicherheit bieten flexible Verteilungsoptionen. Sie können als eigenständige Lösung oder in Kombination mit einem lokal installierten System bereitgestellt werden und sozusagen als Vorfilter des lokal installierten System dienen.

Was sollten Sie tun?

Entscheidungsträger müssen die Gesamtbetriebskosten für alle Aspekte ihrer Messaging-Infrastruktur kennen, um fundierte Entscheidungen zu treffen. Außerdem müssen sie den Funktionsumfang führender gehosteter Sicherheitslösungen im Vergleich zu lokal installierten Lösungen bewerten. In den meisten Fällen werden sie feststellen, dass gehostete Sicherheit ihre Anforderungen an Sicherheit, Datenschutz und Kontrolle genau trifft oder diese sogar übersteigt mit den einmaligen Vorteilen: höherer Schutz und niedrigere Kosten. Hier nun einige der Fragen, die Entscheidungsträger den Anbietern gehosteter Lösungen für E-Mail-Sicherheit in der Bewertungsphase möglicherweise stellen:

- Wie hoch sind die benutzerbasierten Kosten Ihres Service für unsere Anzahl von Benutzern? Ist die Implementierung des Service mit sonstigen Kosten verbunden?

- Bieten Sie im Rahmen Ihres Serviceangebots ein Service Level Agreement (SLA)? Ist im SLA eine hohe Verfügbarkeit (d. h. geringe Ausfallzeiten) garantiert? Ist eine Geld-zurück-Garantie enthalten? Beinhaltet das SLA sonstige Services?

- Welche Funktionen für Richtlinienverwaltung und Content-Filter sind im Serviceumfang enthalten? Sind Mail-Nachverfolgung und Berichte enthalten? Wie kann ich als Kunde Administrationsaufgaben überwachen?

- Gehört eine Datenschutzgarantie zum Leistungsumfang Ihres Service? Ist beim Suchvorgang ein Benutzereingriff erforderlich? Wurde die Sicherheit Ihrer Datenzentren durch externe Zertifizierungsstellen bestätigt?

- Wie lange sind Sie schon in der Branche für Sicherheitsservices tätig? Wird der gehostete Service durch interne, direkt von Ihnen unterstützte Technologien ergänzt? Gibt es Vergleichstests, die die Wirksamkeit der Lösung nachweisen?

- Bieten Sie auch lokal installierte Lösungen? Falls ja, welche Verteilungsoptionen sind verfügbar? Gehostet? Gateway? Mail-Server? Andere Optionen?

Anhand der Antworten auf diese Fragen kann ein Unternehmen die Eignung einer gehosteten Sicherheitslösung für die Unternehmensumgebung bewerten. Unternehmen sollten gehostete Lösungen als Alternative oder Ergänzung zu einer lokal installierten Infrastruktur ins Auge fassen. Andernfalls könnten die Auswahlmöglichkeiten beschränkt sein und höhere Betriebskosten anfallen.

Trend Micro InterScan™ Messaging Hosted Security

In den letzten 20 Jahren hat sich Trend Micro ausschließlich auf den Bereich Content Security konzentriert und ein umfassendes Fachwissen zum Thema Unternehmenssicherung gesammelt. Im Bereich gehostete E-Mail-Sicherheit bietet Trend Micro InterScan™ Messaging Hosted Security, eine Lösung, die Unternehmen vor Spam, Viren, Spyware, Phishing und anderen E-Mail-Bedrohungen schützt. Die Ergebnisse dieser Studie zeigen, dass Unternehmen mit der gehosteten Lösung für E-Mail-Sicherheit von Trend Micro mindestens 75 % an Infrastruktur- und Verwaltungskosten einsparen können. Größere Unternehmen können von noch höheren Einsparungen profitieren.

Als gehostete Lösung hat InterScan Messaging Hosted Security sofortigen Zugriff auf Sicherheitsupdates und die aktuellen, von Trend Micro angebotenen Schutzmaßnahmen. Dieser Service nutzt alle internen Technologien, und Support wird direkt von Trend Micro bereitgestellt. Alle Bedrohungen werden vom Netzwerk ferngehalten, so dass Unternehmen IT-Mitarbeiterzeit sparen und die Produktivität von Endbenutzern steigt. Zusätzlich kümmert sich das weltweite Experten-Team von Trend Micro um alle Hotfixes, Patches, Updates und das Anwendungstuning, um Sicherheit und Leistung der Lösung kontinuierlich zu optimieren.

Mit InterScan Messaging Hosted Security profitieren Kunden von der Wirksamkeit einer branchenführenden Lösung. In einem kürzlich von West Coast Labs durchgeführten unabhängigen Anti-Spam-Vergleichstest erzielte InterScan Messaging Hosted Security die höchste Spam-Trefferquote und überzeugte als beste Lösung unter neun bekannten, lokal installierten Lösungen. InterScan Messaging Hosted Security wird vom Trend Micro Smart Protection Network unterstützt, das Bedrohungsinformationen mit Hilfe von E-Mail-, Web- und File-Reputation-Datenbanken miteinander in Beziehung setzt, damit an allen Angriffspunkten ein sofortiger Schutz geboten werden kann. Dieser Schutz wird durch eines der offensivsten Service Level Agreements (SLA) der Branche ergänzt.

- 100 % Verfügbarkeit
- Spam-Schutz in mindestens 95 % der Fälle
- Fehlalarmrate von weniger als 0,0004 %
- Weniger als zwei Minuten Latenz bei der E-Mail-Zustellung
- Keine E-Mail-basierte Vireninfektion
- Sicherstellung des E-Mail-Datenschutzes durch Zertifizierung der Datenzentren

Im Fall einer Nichteinhaltung der im SLA festgelegten Verpflichtungen stehen Kunden erhebliche Wiedergutmachungsmaßnahmen zur Verfügung.

Neben dem Schutz vor Bedrohungen bietet InterScan Messaging Hosted Security ferner flexible Richtlinienoptionen zum Anpassen von Sicherheits- und Content-Filtern, damit die Einhaltung von Richtlinien durchgesetzt und Datenlecks verhindert werden können. Als zusätzlichen Service bietet Trend Micro Unternehmen außerdem eine Funktion zur Verschlüsselung von E-Mails. Dieser Service ist nahtlos in die Content-Filterfunktionen integriert, so dass sie die Verschlüsselung als Aktion für eine Regel festlegen können. Darüber hinaus können Administratoren durch Mail-Nachverfolgung über den Service weitergeleitete E-Mails ganz einfach finden.

Berichte bieten außerdem einen Einblick in das System und machen den Wert des Service innerhalb kürzester Zeit deutlich. Alle diese Funktionen stehen über eine intuitive webbasierte Konsole bereit, die Administratoren die Verwaltung der E-Mail-Sicherheit auch in großen verteilten Umgebungen erleichtert.

Zusammenfassung

Gehostete Messaging-Sicherheit bietet im Vergleich zu lokal installierten Systemen eine Reihe von Vorteilen und kann eine lokal installierte Sicherheitsinfrastruktur ersetzen oder ergänzen. Gehostete Serviceangebote können deutlich kostengünstiger sein als eine lokal installierte Infrastruktur und bieten darüber hinaus einen höheren Schutz bei gleich bleibender Flexibilität und Kontrolle. Sie sorgen außerdem dafür, dass sich interne IT-Mitarbeiter auf Projekte konzentrieren können, die in einem Wettbewerbsvorteil resultieren.

Entscheidungsträger in Unternehmen, die Kosten einsparen und die Sicherheit optimieren möchten, sollten zum Erfüllen einer oder aller ihrer Sicherheits-anforderungen eine gehostete Lösung für Messaging-Sicherheit in Betracht ziehen. Darüber hinaus sollten sie bei einer Kaufentscheidung alle Aspekte der Verwaltung eines lokal installierten und eines gehosteten Systems bewerten.