COMPUTERWOCHE
VOICE OF DIGITAL

Link: https://www.computerwoche.de/a/sicherheit-fuer-den-e-mail-eingang,1226698

Sicherheit für den E-Mail-Eingang

Datum: 31.03.2009
Autor(en): Johann Baumeister

Der Posteingang stellt den Administrator vor komplexe Aufgaben: Spam und Malware müssen weggefiltert, die verbleibenden Mails vor dem Löschen geschützt und langfristig auffindbar archiviert werden.

Nach Schätzungen des Marktforschungsinstituts IDC wurden schon im Jahr 2005 weltweit 35 Milliarden E-Mails pro Tag versendet. Für 2008 geht Hewlett-Packard (HP) allein in Deutschland von einem E-Mail-Volumen in Höhe von 5500 PB (1 Petabyte = 1024 Terabyte) aus. Davon gelten 90 Prozent als Spam. Unabhängig davon, wie diese Werte einzustufen sind, ist eines sicher: Das Wachstum unerwünschter oder verseuchter elektronischer Nachrichten ist ungebrochen.

Dennoch müssen alle E-Mails – somit auch Spam – bearbeitet werden. Meist werden die unerwünschten Nachrichten zunächst ausgesondert und gelöscht. Der verbleibende kleine Rest ist jedoch umso entscheidender: Mehr und mehr Angebote, Verträge und Bestellungen laufen über Mail-Systeme – in vielen Geschäftszweigen ist E-Mail bereits die zentrale Plattform für die Kommunikation mit dem Kunden.

Für die Untersuchung und eventuelle Abwehr eingehender E-Mails bietet der Markt ein breites Spektrum an Tools an – darunter Malware-Scanner und Content-Filter. Deren Trefferrate hängt entscheidend davon ab, wie gut sie mit Attachments umgehen können. Sendmail beispielsweise gibt an, neben der Mail und HTML-Texten auch alle Anhänge mit gängigen Formaten wie MPG, JPG, Active X, PDF, Word, Excel, Powerpoint oder RTF in die Überprüfung einzubeziehen.

Schutz durch Appliances

Die Untersuchung auf Schadcode in E-Mails und die Spam-Erkennung basieren häufig auf ähnlichen Algorithmen. So lässt sich die Prüfung des Absenders oder die Analyse der Anhänge für beide Zwecke nutzen. Daher überschneiden sich die Bereiche oft.

Die Module zur Viren- und Spam-Erkennung sind meist auf vorgeschalteten Netzeinheiten, einem Gateway, einem MTA (Message Transfer Agent) oder auf Appliances hinterlegt. Das Durchmustern auf Spam und Viren sollte so früh wie möglich erfolgen. Doch auch eine nachgeschaltete Analyse kann sinnvoll sein, da die Prüfung des Mail-Stroms auf dem vorgeschalteten Gateway keine Analyse der Postfächer ermöglicht – diese befinden sich ja erst auf den Mail-Servern. Auch die Prüfung der E-Mail im Kontext des Clients und entsprechend individuelle Filterregeln sind erst dort möglich.

Für diese unterschiedlichen Einsatzzwecke haben die Hersteller ebenso unterschiedliche Produkte im Programm. Das Angebot in diesem Segment ist allerdings unübersichtlich. Eigene Appliances zur E-Mail-Bearbeitung bieten beispielsweise Websense mit "E-Mail Security", Secure Computing mit "Secure Mail", Cisco mit "IronPort", Mirapoint mit "RazorGate" oder Borderware mit "Steelgate" an. Auch Symantec hat hier mehrere Produkte im Portfolio.

Der Vorteil von Appliances zur Absicherung des E-Mail-Eingangs ist die zentrale Verwaltung. Die Geräte lassen sich auch um ein Regelwerk für den Umgang mit ein- und ausgehenden Nachrichten ergänzen. Die Policies definieren die maximale Mail-Größe, erlauben nur bestimmte Anhänge und ergänzen die Nachrichten um Angaben zur Corporate Identity. Die Appliance kann aber auch besondere Aufgaben wie eine zentrale Signatur oder spezielles Routing managen.

Zu den größten Ärgernissen beim Umgang mit E-Mails zählt Spam, der zwei Schadeffekte hat: zum einen die Verschwendung von Ressourcen durch das Bearbeiten und Aussortieren von E-Müll, zum anderen das direkt von Spam ausgehende Bedrohungspotenzial. Meist sollen Spam-Mails ihre Empfänger ja dazu animieren, zweifelhafte Produkte zu bestellen und Websites zu besuchen, die sie ansonsten nicht aufgerufen hätten.

Effektive Spam-Filterung

Der effizienteste Weg, Spam abzuwehren ist, ihn gar nicht erst über die WAN-Strecke zum Empfänger zu transportieren, sondern bereits im Vorfeld auszusortieren. Dafür gibt es verschiedene Ansätze – unter anderem die Senderkennung, die sich bis dato allerdings nicht durchgesetzt hat. Meist bleibt nur, den E-Müll beim Empfänger herauszufiltern. Spam-Filter tun dies – mit mehr oder minder großem Erfolg. Sie beruhen meist auf der Analyse der E-Mail nach Schlüsselwörtern oder Textformatierungen. Andere Verfahren kombinieren RBL ("Real Time Blackhole Lists") mit diversen Filtern und überprüfen den Absender durch DNS-Lookup. Häufig werden auch heuristische Methoden zur Spam-Erkennung eingesetzt.

Um eine hohe Trefferquote zu erzielen, lassen sich diese Verfahren kombinieren. In der Praxis wird die Analysetiefe allerdings durch die zur Verfügung stehende Rechenkapazität des Spam-Filters begrenzt. Diesbezügliche Engpässe lassen sich verhindern, indem beispielsweise E-Mails mit besonders großen Anhängen zeitversetzt gescannt werden.

Manche Hersteller setzen auf eigene Reputationstechniken. Cisco (IronPort) beispielsweise stellt im Internet ServerSysteme bereit, die Absender klassifizieren. Aus der Historie des E-Mail-Verkehrs von oder zu einem Absender werden dann Werte ermittelt, die Auskunft da-rüber geben, ob es sich bei seinen Aussendungen um Spam oder um Malware handelt.

Microsoft-Forefront

Microsoft bietet für seinen Mail-Server Exchange ein eigenes Sicherheitswerkzeug aus der Forefront-Familie. Bei "Forefront für Exchange" handelt es sich im Prinzip um ein Framework, in das die Sicherheitsprodukte von Drittanbietern eingeklinkt werden. Es fungiert als Verwaltungs- und Kommunikationsplattform für den Exchange Server, während die eigentlichen Security-Systeme von Partnern stammen - derzeit die Firmen AhnLab, Authentium, CA, Norman, Kaspersky, Sophos und Virus Buster sowie Microsofts eigene Anti-Virus Engine, die auf der Technik von Gecad basiert.

Seit der Version 2007 ist Exchange in Rollen unterteilt, die für die zum Betrieb des Mail-Servers benötigten Funktionen stehen. Forefront lässt sich auf die Exchange-Rollen "Mailbox", "Hub Transport" und "Edge Transport" anwenden. Hinter der Rolle Mailbox liegen die Postfächer der Benutzer und ihre Verwaltung, während Hub Transport den Austausch der Mails übernimmt und für die interne wie die externe Kommunikation über das Internet benötigt wird. Edge Transport wiederum ist nur für die Kommunikation mit dem Internet erforderlich.

Archivieren und wiederfinden

Prinzipiell lassen sich bei der Mail-Nutzung drei Phasen unterscheiden. In der relativ kurzen aktiven Phase wird die E-Mail empfangen, bearbeitet oder beantwortet. In der folgenden Referenzphase liegt die Nachricht ungenutzt vor. Mitunter sucht der Benutzer sie wieder hervor, um ihre Inhalte erneut aufzugreifen, eine Reklamation zu bearbeiten oder schlicht einen Kontakt ausfindig zu machen. Die dritte und längste Phase ist die Beweisphase. In dieser Zeit sind die Mails aufgrund gesetzlicher Bestimmungen aufzubewahren und für einen Zugriff durch die Behörden bereitzuhalten. Hierbei dient die E-Mail als Nachweis für einen Geschäftsvorfall. Die Verpflichtung, elektronische Nachrichten als Geschäftspost aufzubewahren, ist durch diverse gesetzliche Vorgaben geregelt.

Die Archivierung kann im einfachsten Fall durch Backups der Mail-Postfächer erfolgen, was jedoch nur in unkomplizierten Szenarien ratsam ist. Die Werkzeuge dafür sind dateibasiert und damit unabhängig vom Mail-System. Die Wiederherstellung einzelner Nachrichten ist indes meist nicht möglich.

Weiter als das singuläre Backup der Mail-Speicher geht die sachbezogene Speicherung der Mail samt zugehörigem Vorgang, Produkt oder Geschäftsvorfall. Durch Journalfunktionen, Erstellung von Metadaten und Volltextsuche erfolgt dann ein verknüpfter Zugriff auf die jeweilige "Sache" oder den Vorgang. Dieser ist jedoch kaum durch die Mail allein beschrieben: Ein Angebot besteht typischerweise aus einer Mail und einer PDF-Datei, die das Produkt spezifiziert. Die Bestellung mag als Kunden-E-Mail, die Rechung wiederum als Ausdruck vorliegen. Um eine vorfallsbezogene Ablage der Daten zu ermöglichen, müssen die Mail-Systeme mit allen an dem Vorgang beteiligten Systemen verknüpft werden. Das erfordert Werkzeuge, die mit dem Dokumenten- und Content-Management, dem Archiv- und dem ERP-System kooperieren.

ILM und hierarchische Speicher

Die Tools zur Archivierung von Geschäftsvorfällen unterscheiden sich grundlegend von denen, die schlicht Kopien von Dateien auf Tapes oder Disks ablegen. Sie laufen unter den Produktkategorien HSM (hierarchisches Speicher-Management) beziehungsweise ILM (Information-Lifecycle-Management) und sind eng mit den Systemen integriert, für die sie ihre Dienste anbieten. Tools dieser Art interagieren meist direkt mit dem E-Mail-System, dem Dateisystem und mitunter auch Content-Management-Systemen (CMS) wie dem Sharepoint Portal Server. Durch zentrale oder benutzerdefinierte Regeln erfolgt die Verknüpfung der E-Mails mit den Anhängen, den Dateien im Dateisystem und den Inhalten im CMS. Die Verknüpfung der einzelnen Informationsschnipsel bildet den Geschäftsvorgang ab, der als Einheit (Vorgang) auf den Archivmedien hinterlegt wird.

In den Quellsystemen (etwa Mail-System, Dateisystem) sind bei der vorgangsbezogenen Archivierung nur noch Verknüpfungen zum Archivspeicher vorhanden. Ferner erfolgen die Trennung des Mail-Headers vom eigentlichen Mail-Inhalt und von den Anhängen sowie die singuläre Speicherung (Single-Instance-Speicherung) bei identischen Anhängen in mehreren Mails. Die Verlagerung der Informationen vom Primärsystem ins Archivsystem lässt sich sowohl manuell als auch automatisiert durch vielfältige Kriterien parametrisieren. Dazu gehören das Alter der Informationen, ihre Größe und die Häufigkeit der Zugriffe, aber auch Angaben zur Dauer der Aufbewahrung (Retention Period) – mit automatischer Löschung, sobald diese abgelaufen ist. Um die gesetzeskonforme Speicherung aller vorgangsbezogenen Informationen zu gewährleisten, müssen Archivierungsregeln, -abläufe und -medien entsprechend festgelegt werden.

Mimosa beispielsweise liefert mit Nearpoint eine Archivierungslösung für E-Mail-Bestände und wirbt mit einem schnellen Restore im Fehlerfall. Mimosa und Netapp haben im November 2008 eine Kooperation angekündigt. NetApp kooperiert in Sachen Archivierungslösungen aber auch mit Commvault und Quest. Die Archivierungsanwendungen sind für mehrere Informationssysteme ausgelegt, darunter auch Microsoft Exchange, Microsoft Office SharePoint, Dateidienste und Lotus Notes. Die Anwender erhalten dabei Zugriff auf mehrere Speicherklassen und Protokolle. Enthalten sind ferner Funktionen wie Deduplizierung, kaskadierende Snapshots und Thin Provisioning. Netapps SnapLock versiegelt zudem die Daten gegen Löschung und Änderungen, so dass die gespeicherten Inhalte auch revisionssicher sind.

Alternativer Archivierungsansatz

Während das Gros der Archivierungslösungen erst nach dem Spam-Filter aktiv wird, zeichnet Hewlett-Packards (HPs) Mail-Recorder "Streamwriter" den gesamten SMTP-Datenstrom direkt bei der Ankunft auf.

Eine nachgeschaltete Archivierung birgt aus HP-Sicht das Risiko, dass geschäftskritische E-Mails durch den Spam-Filter aussortiert und somit nicht archiviert werden. Prinzipiell ist das Argument nicht von der Hand zu weisen – geht man allerdings davon aus, dass etwa 90 Prozent der Nachrichten Spam sind, bedeutet dies, dass auch 90 Prozent E-Müll aufgezeichnet werden. Rechtlich unklar ist in diesem Kontext auch die Behandlung privater Mails.

Fazit

Sichere E-Mail-Kommunikation zu gewährleisten ist ein komplexes Unterfangen: Die Vielfalt der übermittelten Informationen und ihre Anhänge öffnen viele Angriffswege. Um Sicherheitslücken, die mit der Kommunikation via E-Mail einhergehen, zu vermeiden, wird daher künftig eine Armada unterschiedlicher Tools nötig sein. (kf)
