TEC WORKSHOP

Link: https://www.tecchannel.de/a/e-mail-sicherheit-fuer-den-posteingang,1779570

Schutz vor Spam, Mailware und Datenverlust
E-Mail-Sicherheit für den Posteingang

Datum: 07.01.2009
Autor(en): Johann Baumeister

Der E-Mail-Eingang stellt den Administrator vor komplexe Aufgaben: Spam und Mailware dringen in das Unternehmen ein und müssen weggefiltert werden. Die verbleibenden E-Mails müssen hingegen sicher vor dem Löschen geschützt und langfristig auffindbar archiviert werden.

35 Milliarden E-Mails sollen nach einer Prognose des Marktforschungsinstituts IDC weltweit im Jahr 2005 täglich versendet worden sein. Für das Jahr 2008 geht HP von 5500 PByte an E-Mail-Datenvolumen allein in Deutschland aus. Davon werden 90 Prozent als Spam betrachtet. Unabhängig davon, wie man diese Werte einstuft, eines ist sicher: Das Wachstum bei verseuchten oder unerwünschten Mails ist ungebrochen.

Trotz ihrer Anzahl müssen alle E-Mails, und somit auch der Spam, bearbeitet werden. Meist trennt man in der ersten Stufe die unerwünschten E-Mails ab und löscht sie zeitnah. Der dann noch verbleibende kleine Rest ist jedoch umso entscheidender für viele Unternehmen. Aufgrund der vermehrten Nutzung von E-Mail als allgemeiner Kommunikationsplattform fließen mehr und mehr Angebote, Verträge oder Bestellungen über die Mail-Systeme. Für den Kontakt mit dem Endverbraucher stellt Mail neben Telefon ohnehin meist die einzige Drehscheibe dar, über die er sich informiert, bestellt oder auch beschwert. In vielen Geschäftszweigen gehört die E-Mail bereits heute zur zentralen Kommunikationsplattform mit dem Kunden. Auch von staatlicher Seite wächst der Druck zur digitalen Kommunikation. Seit einigen Jahren sind Unternehmen in Deutschland etwa verpflichtet, Lohnsteuer-Anmeldungen und Umsatzsteuer-Voranmeldungen elektronisch abzuwickeln.

Zur Untersuchung und Vorselektion der eingehenden E-Mails bietet der Markt ein breites Portfolio an Tools an, darunter Virenscanner, Malware-Scanner und Content-Filter. Deren Trefferrate hängt entscheidend davon ab, wie gut sie mit Attachments umgehen können. **Sendmail**[1] beispielsweise gibt an, neben der Mail und HTML-Texten auch alle gängigen Anhänge mit den Formaten MPG, JPG, Active X, PDF, Word, Excel, Powerpoint, RTF und weitere in den Scanablauf einzubeziehen.

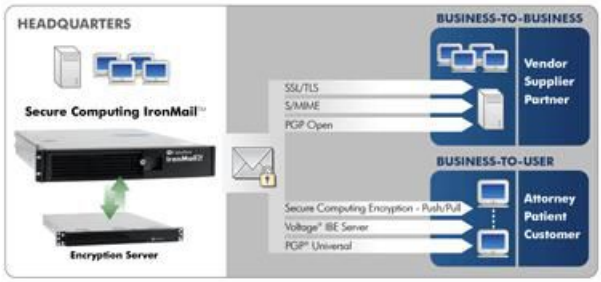
Artikelserie

1. E-Mail-Schutz durch Appliances

Die Untersuchung auf bösartigen Code in E-Mails und das Erkennen von Spam basiert häufig auf ähnlichen Algorithmen. So kann die Prüfung des Absenders oder die Analyse der Anhänge für beide Zwecke genutzt werden. Daher finden sich häufig Überschneidungen oder zumindest enge Kooperationen zwischen beiden Bereichen.

Die Module zur Viren- und Spam-Erkennung sind meist auf vorgeschalteten Netzwerkeinheiten, einem Gateway, MTA (Message Transfer Agent) oder eigenen Appliances hinterlegt. Zwar sollte die Untersuchung auf Spam und Viren so früh wie möglich erfolgen. Dennoch kann auch eine nachgeschaltete Analyse sinnvoll sein, denn die Untersuchung des Mail-Stroms auf dem vorgeschalteten Gateway ermöglicht keine Prüfung von Postfächern, da diese ja erst auf den Mail-Servern existieren. Die Prüfung der E-Mail im Kontext des Clients und dementsprechend individuelle Filterregeln sind natürlich auch erst dort möglich.

Für diese unterschiedlichen Einsatzzwecke liefern die Hersteller ebenso unterschiedliche Produkte. Das Angebot in diesem Segment ist unübersichtlich. Eigene Appliances zur E-Mail-Bearbeitung bieten beispielsweise Websense mit E-Mail Security, Secure Computing mit Secure Mail, Ironport, Mirapoint oder Borderware mit Steelgate. Auch Symantec hat hier mehrere Produkte im Angebot.



Verschlüsselung: IronMail von Secure Computing ermöglicht die Mail-Verschlüsselung durch eine zweite separate Appliance.

Der Vorteil von Appliances zur Sicherung des E-Mail-Eingangs liegt in deren zentralen Verwaltung. Die Appliance kann auch gleich um ein Regelwerk für den Umgang mit dem ein- und ausgehenden Mail-Verkehr ergänzt werden. Diese Policies definieren die maximale Mail-Größe, erlauben nur bestimmte Anhänge und ergänzen die E-Mails um Angaben zur Corporate Identity. Die Appliance kann aber auch besondere Aufgaben wie eine zentrale Signatur oder ein spezielles Routing managen.

2. Die dunkle Seite der E-Mail-Nutzung

Zu den größten Ärgernissen beim Umgang mit E-Mails gehört heute Spam. Dieser hat genau genommen zwei schädliche Effekte. Der eine besteht in der Vergeudung von Ressourcen durch das Bearbeiten und Aussortieren von Spam. Der zweite Effekt ist die Gefährdung, die von Spam direkt ausgeht. Meist sollen Spam-Mails den Empfänger ja dazu animieren, zweifelhafte Produkte zu bestellen und Websites zu besuchen, die der Empfänger der Mail ansonsten nicht aufgerufen hätte.

Welche Ausmaße diese Plage mittlerweile erreicht hat, zeigt die jüngste Studie eines Forscherteams der **University of California**[2] in Berkeley und San Diego. Nach deren Untersuchung führt nur eine von 12,5 Millionen versandten Spam-Mails beim Absender zum Erfolg. Daher müssen unzählige Spam-E-Mails verschickt werden, bis sich dieses zweifelhafte Geschäftsmodell rechnet.

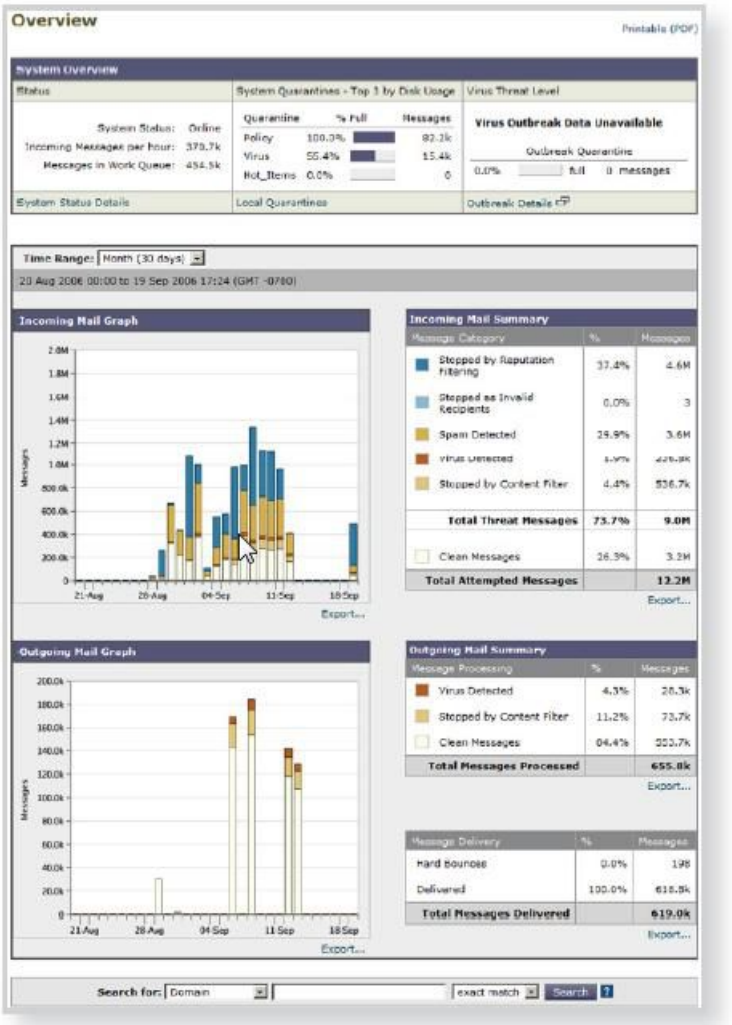
Retarus[3], ein Unternehmen, das E-Mail-Dienste anbietet, stellte im Herbst 2008 „einen Besorgnis erregenden Anstieg der Zahl virenverseuchter E-Mails“ fest. Es soll sich demnach um die Vorhut einer neuen Spam-Welle zu handeln. Nachdem es in den ersten acht Monaten des Jahres 2008 in puncto Versendung von Viren und Malware relativ ruhig war, verzeichnet der E-Mail-Profi nun wieder einen dramatischen Zuwachs an infizierten Nachrichten.

MessageLabs[4], ein Anbieter von E-Mail-Managed-Services, der jüngst von **Symantec**[5] übernommen wurde, ermittelte im November ein Spam-Rate von 70 Prozent. Die Angriffe durch Viren sind nach den MessageLabs-Messungen derzeit rückläufig. Phishing allerdings bleibt auf dem Niveau der zurückliegenden Monate.

3. Effektive Spam-Filterung

Der effizienteste Weg, Spam fernzuhalten, wäre, diese gar nicht erst über die WAN-Strecke zum Empfänger zu transportieren, sondern bereits vorab auszusortieren. Hierzu gibt es diverse Ansätze, wie etwa die Senderkennung, die sich allerdings bis dato nicht durchsetzen konnte. In den allermeisten Fällen bleibt nur der Weg, Spam beim Empfänger auszusortieren. Diverse Spam-Filter versuchen das – mit mehr oder minder gutem Erfolg. Sie beruhen meist auf der Analyse der E-Mail nach Schlüsselworten oder Textformatierungen. Andere Verfahren kombinieren RBL („Real Time Blackhole Lists“) mit diversen Filtern und überprüfen den Absender durch DNS-Lookup. Oftmals werden auch heuristische Methoden zur Spam-Erkennung eingesetzt.

Um eine hohe Trefferrate zu erreichen, kann man all diese Verfahren kombinieren. In der Praxis wird die Analysetiefe durch die zur Verfügung stehenden Rechenkapazität des Spam-Filters begrenzt. Um hier Engpässe zu verhindern, kann man beispielsweise E-Mails mit besonders großen Anhängen zeitversetzt scannen.

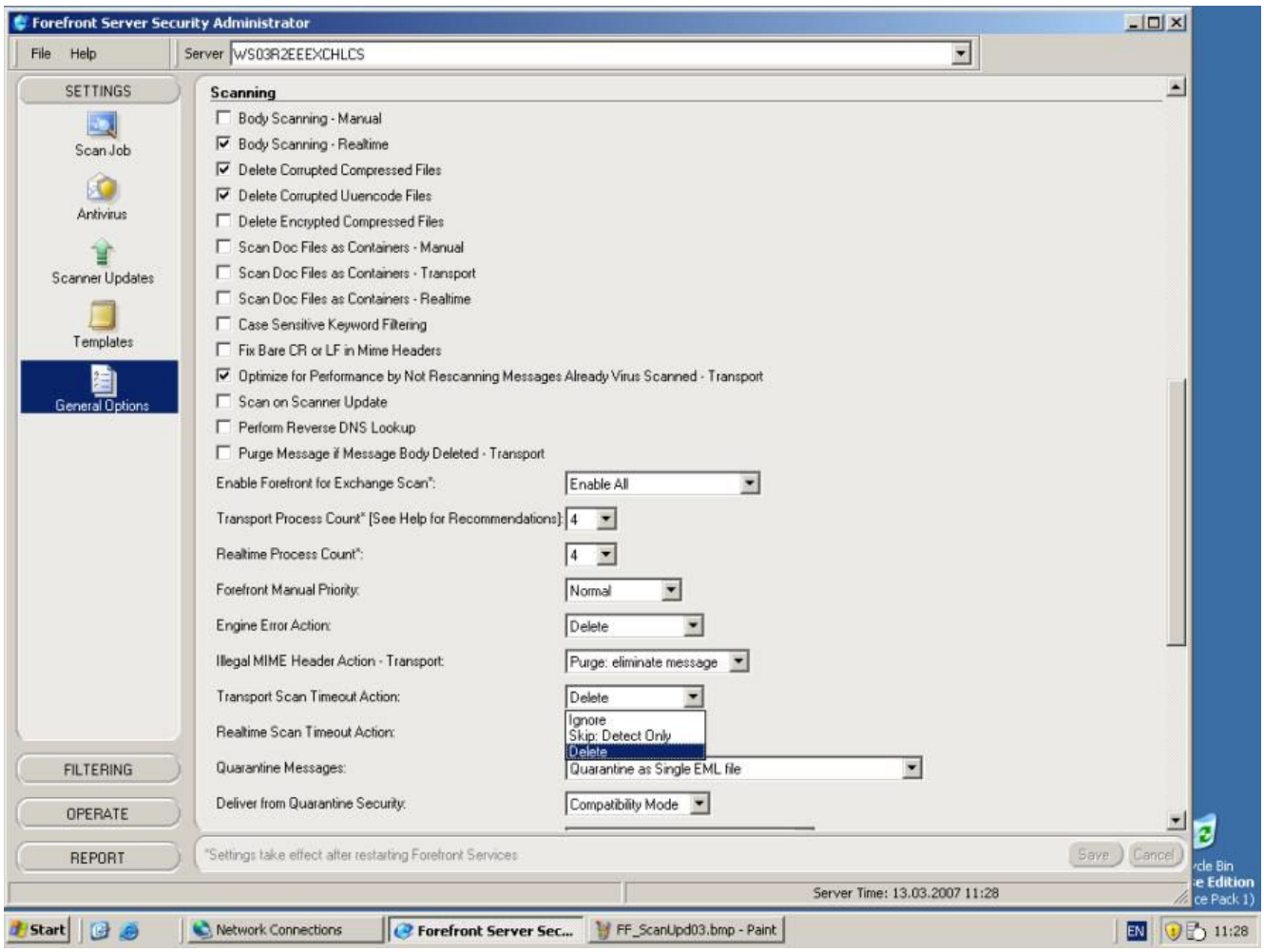


Dashboard: Umfangreiche Auswertungen zur Bedrohungslage präsentiert IronPort mit seiner Appliance.

Manche Hersteller, wie etwa **IronPort**[6], setzen auf eigene Reputationstechniken. IronPort stellt im Web Server-Systeme bereit, die eine Klassifizierung der Absender vornehmen. Aus der Historie des E-Mails-Verkehrs von oder zu diesem Absender werden dann Werte ermittelt, die Auskunft darüber geben, ob es sich bei E-Mails von diesem Absender um Spam oder sonstige Malware handelt.

4. Microsoft Forefront

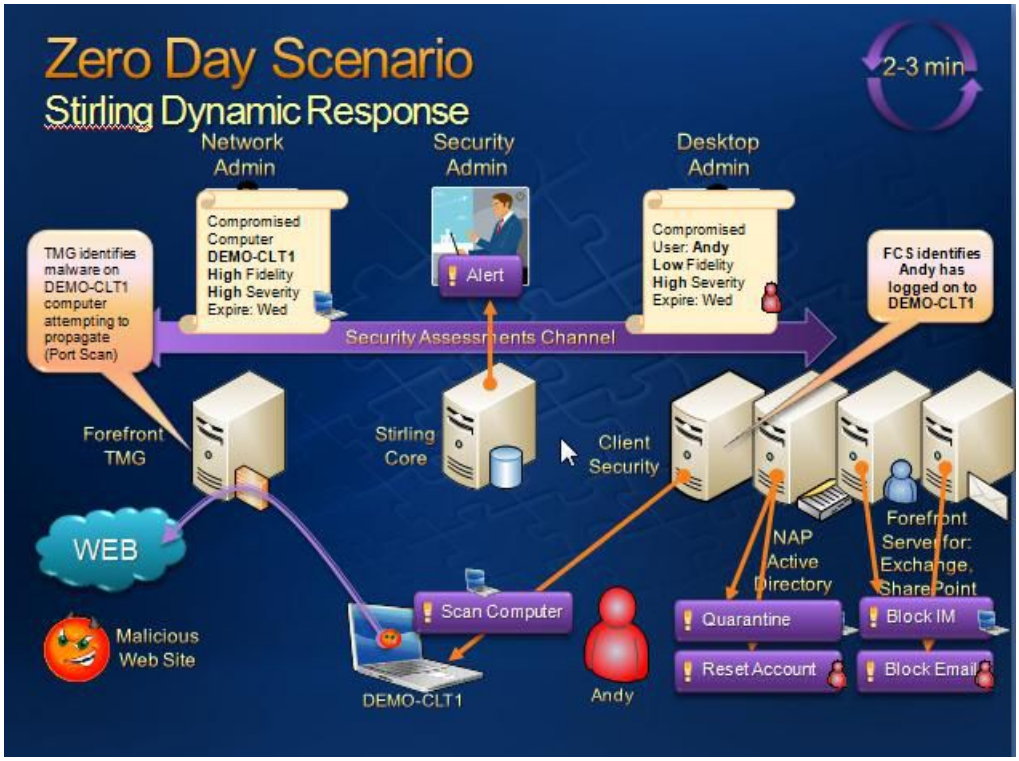
Seit einiger Zeit besitzt Microsoft für seinen Mail-Server Exchange auch ein eigenes Sicherheitswerkzeug aus der **Forefront-Familie**[7]. Zu dieser Familie gehören eine Firewall, ein Access-Gateway, Schutzsoftware für Windows-Clients sowie Tools für verschiedene Microsoft-Server, darunter auch Exchange. In Prinzip handelt es sich bei Forefront für Exchange um ein Framework, in das die Sicherheitsprodukte von Drittanbieter eingeklinkt werden. Forefront fungiert dabei gewissermaßen als Verwaltungs- und Kommunikationsplattform für den Exchange Server. Die eigentlichen Sicherheitssysteme kommen von den Partnern. Diese sind derzeit die Firmen AhnLab, Authentium, CA, Norman, Kaspersky, Sophos und Virus Buster sowie Microsofts eigene Anti-Virus Engine, die auf der Technologie von Gecad basiert.



Exchange-Sicherheit: Microsoft liefert mit Forefront for Exchange ein eigenes Tool-Set zur Überwachung des E-Mail-Verkehrs.

Seit der Version 2007 ist Exchange in mehrere Rollen aufgeteilt. Diese nennen sich Hub Transport, Edge Transport, Unified Communication, Mailbox und Client Access. Die Rollen stehen für die verschiedenen Funktionen, die für den jeweiligen Betrieb von Exchange benötigt werden. Hinter der Rolle Mailbox liegen die Postfächer der Benutzer und ihre Verwaltung, der Hub Transport übernimmt den Austausch der Mails und wird sowohl für die interne als auch für die externe Kommunikation über das Internet benötigt. Der Edge Transport ist nur bei der Kommunikation mit dem Internet notwendig. Der Rolle Unified Communication wiederum ist gänzlich neu und bildet Funktionen wie die Sprachein- und -ausgabe ab, während die Rolle Client Access die Schnittstelle für spezielle Client-Zugänge wie etwa Outlook Web Access implementiert.

Die Rollen können auf unterschiedlichen Servern installiert werden. Über diesen Weg wird die weitgehend wahlfreie Skalierbarkeit des Mail-Systems erzielt. In kleineren Unternehmen mit einer überschaubaren Anzahl an Mail-Boxen können alle Rollen einem physischen Server zugewiesen werden.



Dynamische Sicherheitsregeln: In der kommenden Version von Forefront verknüpft Microsoft die unterschiedlichen Systeme zu einem Dynamic Response System.

Forefront lässt sich dabei auf die drei Rollen Edge, Hub und Mailbox anwenden. In der kommenden Version von Forefront sollen die bis dato separat agierenden Sicherheitsmodule integriert werden. Microsoft will Forefront so zu einem Dynamic Response System ausbauen, also einem Sicherheitssystem, das dynamisch auf die Bedrohungen reagiert oder auch präventiv agiert. Wird beispielsweise festgestellt, dass ein Benutzer ein übermäßig großes E-Mail-Aufkommen hat, so stehen er und seine Aktionen für einen bestimmten Zeitraum unter verstärkter Überwachung. Diese bezieht auch seine sonstige Interaktionen mit anderen Benutzern, wie etwa über Instant Messaging, ein.

5. Archivieren und wiederfinden

Prinzipiell lassen sich bei der Mail-Nutzung drei Phasen unterscheiden. In der aktiven Phase, die relativ kurz ist, wird die E-Mail empfangen, bearbeitet oder beantwortet. In der nachfolgenden Referenzphase liegt diese E-Mail ungenutzt vor. Mitunter erinnert sich der Benutzer an sie und sucht sie wieder hervor, um den Inhalt der Mail wieder aufzugreifen, eine Reklamation zu bearbeiten oder einfach einen Kontakt ausfindig zu machen. Die dritte und längste Phase ist die Beweisphase. In dieser Zeit sind die Mails wegen gesetzlicher Bestimmungen aufzubewahren und für einen Zugriff durch die Behörden bereitzuhalten. Hierbei dient die E-Mail als Nachweis für einen Geschäftsvorfall. Die Verpflichtung, E-Mails als Geschäftspost aufzubewahren, wird durch mehrere gesetzliche Vorgaben geregelt. Dieser Aspekt der Archivierung und Aufbewahrung gewinnt in letzter Zeit zunehmend an Brisanz.

Die Verpflichtung zur E-Mail-Speicherung stellen gewaltige Anforderungen an die Speichersysteme. Um sich hiervon ein Bild zu machen, kann auf eine Untersuchung der Enterprise Strategy Group zurückgegriffen werden. Zwar bezieht sich diese nicht nur auf E-Mails, aber E-Mails haben einen gewaltigen Anteil daran: Nach Meinung der Analysten wächst das Volumen für die Datenarchivierung der Unternehmen in den nächsten drei Jahren auf über 100.000 PByte. Wenn man dabei den Anteil Deutschlands auf fünf Prozent taxiert, wären bei reinem Disk-Backup hierzulande fünf Millionen Festplatten mit je einem TByte nötig.

Die Archivierung kann im einfachsten Fall durch Backups der Mail-Postfächer erfolgen. Dies ist jedoch nur in einfachen Szenarien angeraten. Die Werkzeuge dafür sind dateibasiert und damit zwar unabhängig von den Mail-Systemen. Eine Wiederherstellung einzelner E-Mails ist aber meist nicht möglich.

6. Information Lifecycle Management und hierarchische Speicher

Weiter als das singuläre Backup der Mail-Speicher geht die sachbezogene Speicherung der Mail mit dem zugehörigen Vorgang, Produkt oder Geschäftvorfall. Durch Journalfunktionen, Erstellung von Metadaten und Volltextsuche erfolgt dann ein verknüpfter Zugriff auf die jeweilige "Sache" oder den Vorgang. Dieser wird jedoch kaum durch die Mail alleine beschrieben sein. Ein Angebot kann typischerweise aus einer Mail und einer PDF-Datei, die das Produkt spezifiziert, bestehen. Die Bestellung mag als Kunden-E-Mail, die Rechung wiederum als Ausdruck vorliegen. Um nun aber eine vorfallsbezogene Ablage der Daten zu ermöglichen, müssen die Mail-Systeme mit allen an dem Vorgang beteiligten Systemen verknüpft werden. Hierfür sind Werkzeuge nötig, die mit dem Dokumentenmanagement, dem Content-Management, dem Archivsystem und dem ERP-System kooperieren.

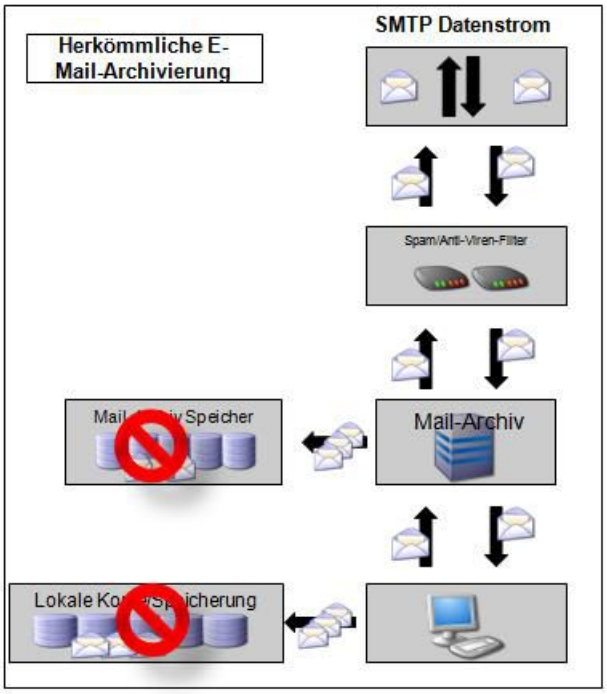
Die Werkzeuge zur Archivierung von Geschäftsvorfällen unterscheiden sich grundlegend von denen, die stupide Kopien von Dateien auf Tapes oder Disks ablegen. Sie segeln unter der Flagge namens HSM (hierarchisches Speicher Management) oder ILM (Information Lifecycle Management) und weisen eine enge Integration mit jenen Systemen auf, 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 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 Sharepoint Server. Diese Verknüpfung der einzelne Informationsschnipsel bildet den Geschäftsvorgang ab, der dann als eine Einheit (der Vorgang) auf den Archivmedien hinterlegt wird.

In den Quellsystemen (Mail-System, Dateisystem etc) sind bei der vorgangsbezogenen Archivierung nur noch Verknüpfungen zum Archivspeicher vorhanden. Ferner erfolgen eine 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 kann sowohl manuell durch den Benutzer als auch automatisiert durch vielfältigste Kriterien parametrisiert werden. Darunter fallen beispielsweise das Alter der Informationen, ihre Größe und die Zugriffshäufigkeit. Dazu gehören auch Angaben zur Aufbewahrungsdauer (Retention Period) mit einer automatischen Löschung beim Ablauf der Aufbewahrungsdauer. Zur Gewährleistung der angemessenen oder gesetzeskonformen Speicherung aller vorgangsbezogenen Informationen sind die Archivierungsregeln, -abläufe und -medien entsprechend festzulegen.

7. Archivierungslösungen und MailRecorder für den SMTP-Datenstrom

Mimosa beispielsweise liefert mit **Nearpoint**[8] eine Archivierungslösung für E-Mail-Bestände und wirbt mit einem schnellen Restore im Fehlerfall. Mimosa und **NetApp**[9] haben im November 2008 eine Kooperation angekündigt. NetApp kooperiert daneben aber auch noch mit den Archivierungslösungen von **CommVault**[10] und **Quest**[11]. 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. Eingeschlossen sind ferner Funktionen wie Deduplizierung, kaskadierende Snapshots und Thin Provisioning. NetApps SnapLock versiegelt außerdem die Daten gegen Löschen und Änderungen, sodass die gespeicherten Inhalte auch revisionssicher sind.

Einen ganz anderen Ansatz der Archivierung empfiehlt HP. Deren MailRecorder wird von HP als Flugschreiber für E-Mails bezeichnet. Er zeichnet den gesamten SMTP-Datenstrom direkt bei der Ankunft auf. Im Gegensatz dazu operieren die meisten Archivlösungen nach dem Spam-Filter.



Streamwriter: HP platziert seinen MailRecorder vor die Spam-Filter und stellt damit sicher, dass alle Mails aufbewahrt werden.

Nach Meinung von HP birgt die nachgeschaltete Archivierung das Risiko, dass geschäftskritische E-Mails vorher durch den Spam-Filter aussortiert werden und somit nicht archiviert sind. Das Argument ist prinzipiell nicht von der Hand zu weisen. Wenn man allerdings ins Kalkül zieht, dass circa 90 Prozent der E-Mail ohnehin Spam sind, heißt das, dass 90 Prozent Müll aufgezeichnet werden. Unklar dabei ist auch die rechtliche Behandlung von privaten E-Mails.

8. Fazit

Die Gewährleistung der Sicherheit der E-Mail-Kommunikation ist ein komplexes Unterfangen. Die Vielfalt der übermittelten Informationen und ihre Anhänge ziehen mannigfache Angriffswege nach sich.

Zur Vermeidung von Sicherheitslücken, die mit der E-Mail-Kommunikation einhergehen, wird künftig eine Armada an unterschiedlichen Tools nötig sein. Im Netzwerk platzierte Appliances, host-basierter Schutz, UTM, IDS, IPS, Netzwerktrennung durch Firewalls – all das sind Möglichkeiten der technischen Umsetzung.

Im dritten Teil dieser Reihe geht es um die Absicherung des E-Mail-Systems gegen Ausfälle. Dabei stehen Konzepte wie Clustering, Backup und Restore, benutzerdefinierte Wiederherstellung von Mail-Inhalten und Datenrettung im Mittelpunkt. (ala)

Artikelserie

Teil 1: **Regeln für das sichere Erstellen von E-Mails**[15]
Teil 2: **Regeln und technische Schutzmaßnahmen beim E-Mail-Empfang**[16]
Teil 3: **Sichere Infrastruktur für E-Mail-Systeme**[17]

Links im Artikel:

[1] **http://sendmail.com/sm/solutions/inbound/**
[2] **http://berkeley.edu/**
[3] **http://www.retarus.de/**
[4] **http://www.messagelabs.com/**
[5] **http://www.symantec.com/de/de/index.jsp**

[6] **http://www.ironport.com/de/**
[7] **http://www.microsoft.com/germany/forefront/default.mspx**
[8] **http://www.mimosasystems.com/**
[9] **http://www.netapp.com/de/**
[10] **http://www.commvault.de/**
[11] **http://www.quest.com/**
[12] **https://www.tecchannel.de/kommunikation/e-mail/1778559/sicherer_postausgang/**
[13] **https://www.tecchannel.de/kommunikation/e-mail/1779570/e_mail_sicherheit_spam_filter_mailbox_backup/index.html**
[14] **https://www.tecchannel.de/link.cfm?pk=1779571**
[15] **https://www.tecchannel.de/kommunikation/e-mail/1778559/sicherer_postausgang/**
[16] **https://www.tecchannel.de/kommunikation/e-mail/1779570/e_mail_sicherheit_spam_filter_mailbox_backup/index.html**
[17] **https://www.tecchannel.de/link.cfm?pk=1779571**
