

Gehostete E-Mail-Services für Unternehmen

# Post it

Bert Ungerer



Erfahrene Postmaster mögen ob des Vergleichs lächeln, aber für andere bedeuten Einrichten und Aufrechterhalten von E-Mail-Services angesichts heutiger Herausforderungen eben doch „Rocket Science“. Das Outsourcing dieses Internet-Dienstes als Alternative zum eigenen Mailserver hat daher Konjunktur – nicht nur wegen der Spam-Massen.

**S**icheres, rechtskonformes Transportieren und Speichern von E-Mails umfasst nicht nur eine ganze Palette von Internet- und LAN-Diensten, sondern erfordert auch eine Menge juristischer Expertise. Der nötige Umfang an Fachwissen fordert selbst einen hauptberuflich tätigen Admin täglich heraus. Nebenbei gilt es laufend eine schier unglaubliche Menge an Spam von den Anwendern fernhalten und andere Angriffe auf die Mail-Systeme abzuwehren. In größeren Unternehmen kann das alles selbst einen gestandenen, hauptberuflichen Administrator viel Arbeitszeit und -kraft kosten. Die stünde bei einer Auslagerung des Mailservers

für sinnvollere Dinge zur Verfügung, etwa zur Unterstützung des Kerngeschäfts. Die zugekaufte Dienstleistung kommt erst recht für kleinere Firmen infrage, die sich womöglich gar keine Planstelle für einen Postmaster leisten können.

Je nachdem, seit wann eine Domain im Allgemeinen oder eine Empfängeradresse im Besonderen existiert, träfen ohne Gegenmaßnahmen heutzutage bei manchem Internet-Anwender zehnen-, zum Teil sogar hundertmal mehr Spam als erwünschte E-Mails ein. Dieses praktische und trotz aller Unzulänglichkeiten immer noch unverzichtbare Medium wäre nicht mehr benutzbar,

gäbe es keine automatisierten Filtersysteme.

Anbieter von Kommunikationsdienstleistungen – dazu gehört eben auch E-Mail – sind geradezu zum Filtern gezwungen. Arbeitgeber und Provider sind verpflichtet, das ordnungsgemäße Funktionieren von E-Mail sicherzustellen. Dazu gehört aber sicher nicht das Zustellen schädlicher Inhalte wie Spam und Viren, sondern deren Abweisung. Wer einen Mail-Service als Dienstleistung in Auftrag gibt, sollte dies ganz oben auf seiner Anforderungsliste stehen haben: Unerwünschtes darf gar nicht erst ins System gelangen.

## Zwang zum Filtern

Markieren und Zustellen wie in der Frühphase der Spam-Filterung sind nicht mehr Stand der Technik und ohnehin völlig unpraktikabel, denn kein Anwender sieht noch Eingangsorter durch, in denen vielleicht eine von Tausenden Mails eventuell doch erwünscht

sein könnte. Zudem besteht beim Zustellen von Spam die Gefahr, dass die Anwender aus Neugierde E-Mails öffnen, die auf verseuchte Webseiten führen („Drive-by Download“) oder solche mit illegalen Inhalten wie Kinderpornografie – denn sogar vor Werbung dafür schrecken Spammer nicht zurück.

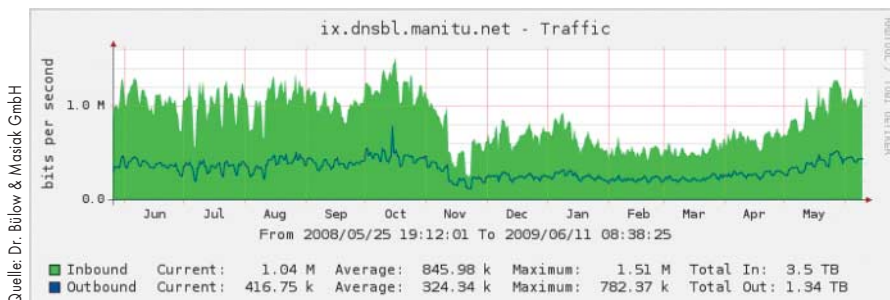
Das Abweisen von Spam hat neben der Rechtssicherheit einen weiteren entscheidenden Vorteil: Alle nachgelagerten Systeme, insbesondere zur Archivierung, belegen entsprechend weniger Netz-, CPU-, Speicher- und nicht zuletzt Administrations-Ressourcen. Und eine Spam-Mail, die gar nicht erst ins Firmennetz gelangt, kann dort keine unerwünschten Nebenwirkungen entfalten. Dazu gehört das Provozieren von „Abwesenheitsnotizen“, die an Unbeteiligte gehen, weil der Spam-Versender deren Mail-Adressen als Absenderadressen missbraucht hat.

## Dienstleister bieten Mehrwert

Zum automatisch erzeugten und schwer kontrollierbaren „Backscatter“ (auch „Reverse Spam“ oder „Collateral Spam“ genannt) gehören darüber hinaus Fehlermeldungen (Bounces) etwa wegen überfüllter Anwender-Postfächer. Beliebte sind auch Bounces wegen unbekannter Empfängeradressen, die ein fehlerkonfigurierter Eingangsserver nicht selbst prüfen konnte. Schlimmstenfalls können derlei Störungen zu Blacklist-

Eintragungen führen, die wiederum das Versenden von E-Mail behindern. Einen weiten Bogen muss man aus demselben Grund um „Lösungen“ schlagen, die Spam bewusst mit „Gegensпам“ (Challenge) beantworten, deren Empfänger eine Aufgabe lösen müssen (Response), damit wiederum die ursprüngliche (Spam-)Mail ankommt.

Derlei Tücken sind einem Anbieter gehosteter Mail-Dienste in der Regel bereits bekannt. Er kann seinen Kunden neben der Erfahrung im Bearbeiten großer Mengen an E-Mails die üblichen Vorteile eines Hosters bieten: Etwa ein klimatisiertes Rechenzentrum mit zugangsgeschützten Räumlichkeiten und guter Netzanbindung. Darüber hinaus bieten Mail-Hoster mehr Aus-



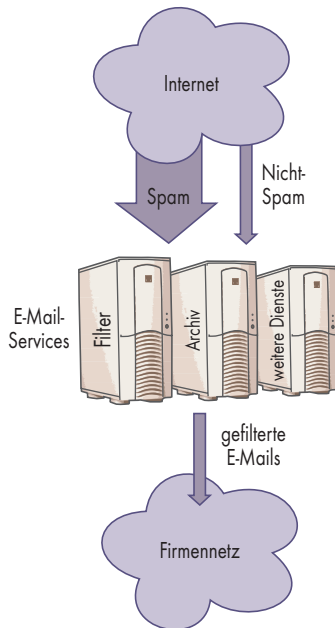
**Das Spam-Aufkommen (hier in Form von Abfragen an die iX-Blacklist) liegt - nach einem Einbruch Ende 2008 - wieder auf dem extrem hohen Niveau von vor einem Jahr und je nach betroffener Domain zum Teil bei weit über 90 % aller Mails. Ein Grund für viele Unternehmen, zumindest den eingehenden E-Mail-Verkehr per Outsourcing abwickeln zu lassen (Abb. 1).**



- Als Mittel zur Befreiung von Spam und zur vorschriftsmäßigen Archivierung der erwünschten E-Mails bietet sich Mailserver-Outsourcing an.
- Neben großen Anbietern wie Microsoft und Google, die sich durch Zukäufe gewappnet haben, gibt es eine Reihe unabhängiger Spezialisten für „Managed Mail Services“.
- Externe E-Mail-Dienste lassen sich oft nicht nur als Mailserver-Ersatz nutzen, sondern bieten unter anderem auch Plattformen für Groupware-Funktionen.

Anzeige

fallsicherheit, als sich eine Firma üblicherweise leistet und als sie für den von sich aus fehlertoleranten Store-



**Je mehr Kunden ein Anbieter von E-Mail-Services hat, desto besser kann er unerwünschte Inhalte von den Empfängern fernhalten. Außer den Standarddiensten Filterung und Archivierung kommen unter anderem Webmailer oder Systeme zur Kundenbindung (CRM) als „Added Values“ in Betracht (Abb. 2).**

and-Forward-Dienst E-Mail eigentlich notwendig ist. Schaden kann sie natürlich nicht, wenn sie aber gegebenenfalls als Extra-Posten auf der Abrechnung auftaucht, ist Redundanz für den Mail-Empfang jedoch verzichtbar. Etwas anders sieht es bei der Archivierung aus, die im Falle von Schlamperei schnell in juristisch unsicheres Fahrwasser führt (siehe auch Kasten „Aufbewahrungspflicht ...“).

Ein E-Mail-Dienstleister konzentriert den E-Mail-Verkehr an viele Kunden-Domains zunächst auf sich, bevor er ihn „gereinigt“ an Mailserver der jeweiligen Kunden weiterleitet oder ihn – je nach Vertragsgestaltung und gebotener Infrastruktur – direkt in Postfächer im eigenen Haus einsortiert. Die Domain-Besitzer geben im DNS-Eintrag für den zuständigen Eingangs-Server (MX Record) einfach einen oder mehrere Server des Service-Anbieters an. Je mehr Kunden zusammenkommen, desto besser funktioniert das Prinzip. Neu beginnende Spam-Angriffe lassen sich umso schneller erkennen und abwehren, je mehr Domains und damit auch Spam der Anbieter auf sich versammeln kann.

Tatsächlich gibt es bereits einige sehr große Mail-Dienstleister, die dieses Prinzip bestens für sich und ihre Kunden nutzen können. Der rasch wachsende Markt für ausgelagerte E-Mail-Services

war in den letzten Jahren von spektakulären Übernahmen gekennzeichnet. Microsoft, Google, Cisco und Symantec haben sich mit Frontbridge, Postini, IronPort und MessageLabs in Position gebracht. Daneben bieten zahlreiche eigenständige Anbieter aus verschiedenen Bereichen ihre Dienste an, etwa Spezialisten für Spam-Filterung wie die Berliner eleven GmbH oder antispameurope aus Hannover und viele weitere (siehe Tabelle und iX-Links).

## Angebote für den Großbedarf

Vor der Entscheidung für einen Dienstleister stehen einige prinzipielle Überlegungen. Sollen der oder die Mailserver im eigenen Hause stehen oder im Rechenzentrum des Service-Anbieters? Hier drohen gelegentlich Missverständnisse: Manch ein Anbieter versteht unter „Managed Service“ ein System (häufig in Form einer Appliance), das beim Kunden steht. Die Kundenfirma hat aber selbst nichts mit der Systemadministration zu tun, sondern lässt sie von außen stattfinden. Weitere prinzipielle Fragen betreffen den bereits erwähnten Standort der Postfach-Server oder ob sich der Service auch auf ausgehende E-Mails erstrecken soll. Sämtliche Details sind in der Regel individuell zu

### E-Mail-Dienstleister für Unternehmen

Anbieter	Produkt	URL
antispameurope GmbH	Managed Services	<a href="http://www.antispameurope.de/index.php?option=com_content&amp;task=view&amp;id=63&amp;Itemid=63">www.antispameurope.de/index.php?option=com_content&amp;task=view&amp;id=63&amp;Itemid=63</a>
arvato systems GmbH	Hosted Exchange	<a href="http://www.arvato-systems.de/">www.arvato-systems.de/</a>
CEMA AG	Hosted Exchange	<a href="http://www.mycema.de/default.aspx">www.mycema.de/default.aspx</a>
Cisco Systems, Inc.	IronPort Hosted Email Security	<a href="http://www.ironport.com/de/products/hosted_email_security.html">www.ironport.com/de/products/hosted_email_security.html</a>
Claranet GmbH	SpamVir Protect	<a href="http://www.claranet.de/netzwerke/sicherheit/spam-protection">www.claranet.de/netzwerke/sicherheit/spam-protection</a>
Cortado (ThinPrint AG)	Hosted Exchange	<a href="http://www.cortado.de/">www.cortado.de/</a>
Elabs AG	Hosted Exchange	<a href="http://www.elabs.de/">www.elabs.de/</a>
eleven GmbH	eleven Managed Services	<a href="http://www.eleven.de/index.php?option=content&amp;task=view&amp;id=152&amp;Itemid=377">www.eleven.de/index.php?option=content&amp;task=view&amp;id=152&amp;Itemid=377</a>
Fastnet SA	MailCleaner Hosted Services	<a href="http://www.mailcleaner.net/antispam/onlineversion.html">www.mailcleaner.net/antispam/onlineversion.html</a>
FeltenFinkbeiner GmbH	Hosted Exchange	<a href="http://www.feltenfinkbeiner.de/">www.feltenfinkbeiner.de/</a>
Future-X Software GmbH	Hosted Exchange	<a href="http://www.host-dich.de/">www.host-dich.de/</a>
Google Inc.	Google Apps Standard/Professional	<a href="http://www.google.com/a/help/intl/de/admins/editions.html">www.google.com/a/help/intl/de/admins/editions.html</a>
Heinlein Professional Linux Support GmbH	diverse Mail-Hosting-Services	<a href="http://www.heinlein-support.de/">www.heinlein-support.de/</a>
idosec AG	idoSPAM (extern)	<a href="http://www.idosec.com/">www.idosec.com/</a>
IKARUS Security Software GmbH	myMailWall Managed Security Services	<a href="http://www.mymailwall.at/">www.mymailwall.at/</a>
ittelliance GmbH	Hosted Exchange	<a href="http://www.ittelliance.de/">www.ittelliance.de/</a>
Lufthansa Systems AG	Hosted Exchange	<a href="http://www.lhsystems.com/">www.lhsystems.com/</a>
Microsoft Corporation	Hosted Exchange	<a href="http://www.microsoft.com/germany/exchange/2007/services/ueberblick.mspx">www.microsoft.com/germany/exchange/2007/services/ueberblick.mspx</a>
Netintelligence Ltd	Mail Filter & Anti Spam	<a href="http://www.netintelligence.com/de/mailfilter.htm">www.netintelligence.com/de/mailfilter.htm</a>
Norman Data Defense Systems GmbH	Norman Online Protection	<a href="http://www.norman.com/smb/all_products/email/norman_online_protection/de">www.norman.com/smb/all_products/email/norman_online_protection/de</a>
pdv-systeme Sachsen GmbH	SpamTitan	<a href="http://www.pdv-sachsen.net/index.php/anwendungen/viren-und-spamschutz/299-schutz-fuer-ihre-e-mails-spamtiton">www.pdv-sachsen.net/index.php/anwendungen/viren-und-spamschutz/299-schutz-fuer-ihre-e-mails-spamtiton</a>
PIRONET NDH AG	Hosted Exchange	<a href="http://www.pironet-ndh.com/">www.pironet-ndh.com/</a>
PROFI Engineering Systems AG	PROFI AntiSpam	<a href="http://www.profi-ag.de/">www.profi-ag.de/</a>
QualityHosting AG	Hosted Exchange	<a href="http://www.qualityhosting.de/">www.qualityhosting.de/</a>
retarus GmbH	Managed E-Mail Services	<a href="http://www.retarus.com/de/products/enterprise_messaging_solutions/retarus_managed_email_services.php">www.retarus.com/de/products/enterprise_messaging_solutions/retarus_managed_email_services.php</a>
Skyfillers GmbH	Hosted Exchange	<a href="http://www.skyfillers.com/">www.skyfillers.com/</a>
SoftScan GmbH	E-Mail Security Service	<a href="http://www.softscan.de/content/de/produkte/e-mail_security">www.softscan.de/content/de/produkte/e-mail_security</a>
Symantec Corporation	MessageLabs	<a href="http://www.messagelabs.de/contact">www.messagelabs.de/contact</a>
WEBMAXX GmbH	Hosted Exchange	<a href="http://www.webmaxx.de/">www.webmaxx.de/</a>

klären, denn bei ausgelagerten Mail-Services handelt es sich bis auf Ausnahmen wie Google Mail um ein Projektgeschäft, das die Kunden so flexibel gehandhabt wissen möchten, wie das Medium E-Mail es eben erlaubt.

Einige Anbieter ermöglichen einen kostenlosen Testbetrieb, meist für einen Monat. Auf diese Weise können die potenziellen Kunden verschiedene Anbieter miteinander vergleichen, ohne gleich mehrere Accounts erwerben zu müssen.

Apropos Kosten: In der Regel ist pro Anwender respektive Postfach etwa ein niedriger einstelliger Euro-Betrag monatlich zu veranschlagen. Am unteren Ende der Preisspanne rangieren die kostenlosen Google-Apps-Accounts, und das mit ansehnlichen Eckdaten: Bis zu 50 Anwender erhalten je 7 GByte Speicherplatz und einige Online-Office- sowie Groupware-Funktionen. Wer keine Vorurteile gegen ausländische Anbieter hegt, die festen Vorgaben und die (auf relativ dezente Weise, siehe Abbildung 3) eingeblendete Werbung hinzunehmen bereit ist, kann bei Google durchaus eine kleine Firma kostenlos mit professionellen Mail-Funktionen und einen wirksamen Spam-Filter ausstaffieren. Das ist allemal besser, als sich einen eigenen, halbherzig zusammengestrickten, selten gewarteten und entsprechend unzuverlässigen Mailserver hinzustellen.

In der Regel sind es genau solche Systeme, die eines Tages Malware und unerwünschte Mitbenutzer anziehen. Schlimmstenfalls haftet in solchen Fällen der Betreiber und muss Schadenersatz leisten, wenn der Server zur Spam- und Virenquelle wird.

## „False Positives“ sind vor allem menschlich

Als scheinbar überzeugendes Argument für die eigene Dienstleistung oder eben gegen die der Konkurrenz ziehen viele Anbieter die gefürchteten „False Positives“ heran – fälschlicherweise als Spam oder Malware einsortierte oder gar gelöschte E-Mails also, die den Empfänger eigentlich unbedingt hätten erreichen müssen. Die Werbeaussagen erwecken gelegentlich den Eindruck, ein erheblicher Teil aller erwünschten Mails sei geradezu geschäftskritisch und keine einzige davon dürfe jemals ungelesen bleiben.

Deutlich entspannter sehen das anscheinend die Mail-Anwender selbst.

Anzeige



**Eigene Domain genügt: Die werbefinanzierte Version von Google Mail ist für bis zu 50 Anwender kostenlos und bietet einen guten Spam-Filter sowie diverse Groupware-Funktionen. Der Postini-Filter lässt sich – kostenpflichtig – auch unabhängig von Google Mail buchen (Abb. 3).**

## Aufbewahrungspflicht auch bei Insolvenz

Sechs oder gar zehn Jahre sind alles andere als überschaubar. Viele Firmen existieren bei Weitem nicht so lange, wie der Gesetzgeber ihnen das Aufbewahren von Geschäftskorrespondenz vorschreibt. Da stellt sich die Frage, was mit den Aufbewahrungspflichten in der Insolvenz und beim Unternehmensverkauf passiert.

Wenn eine Firma nicht mehr existiert (also aus dem Handelsregister gelöscht wurde), bestehen auch keine Archivierungspflichten mehr. Die richten sich an das Unternehmen respektive dessen Organe, also juristische Personen, die dann nicht mehr vorhanden sind. Etwas anderes gilt, wenn es sich um einen Einzelkaufmann oder eine zur Aufbewahrung persönlich verpflichtete Person handelt, beispielsweise einen Arzt oder einen Rechtsanwalt. Der muss trotz „Aufgabe des Geschäftsbetriebs“ und etwaiger Löschung die Akten weiterhin aufbewahren, auch wenn die Gemeinschaftspraxis-GmbH oder die Anwalts-gesellschaft selbst nicht mehr existieren sollte.

### E-Mails und Firma gelöscht

Auch eine insolvente Firma besteht zunächst weiter, bis zur etwaigen Löschung im Handelsregister, wenn Rettungsversuche im Rahmen des Insolvenzverfahrens scheitern. Das gilt auch für die Aufbewahrungsfristen. Allerdings ist dann je nach seiner Stellung der Insolvenzverwalter und nicht mehr der bisherige Geschäftsführer oder Vorstand für die Einhaltung der entsprechenden Pflichten verantwortlich. Das Vernichten von Unterlagen vor oder während einer Insolvenz ist sogar eine schwere Straftat.

Beim Verkauf einer Firma entscheidet die Art und Weise der Übertragung. Werden nur „Assets“, also Vermögen und nicht die Firma an sich verkauft, verbleiben die Aufbewahrungspflichten bei der verkauften Firma, denn die existiert ja bis zur etwaigen Löschung weiter. Wer eine komplette Firma übernimmt, erwirbt mit ihr natürlich alle Rechte und Pflichten – und damit auch die Aufbewahrungspflichten. Dass Geschäftsanteile den Besitzer wechseln, bedeutet nicht zwangsläufig, dass etwa auch der Geschäftsführer ausgetauscht wird. Der ist bis zu seiner Abberufung zum Aufbewahren verpflichtet, gleichgültig, wem die Firma gehört.

Ob pleite oder nicht: Geschäftsführer oder Vorstände müssen sicherstellen, dass die Archivierung geschäftsrelevanter Unterlagen auf professionelle und sichere Weise erfolgt, damit die Firma jederzeit darauf zugreifen kann und um den gesetzlichen Aufbewahrungspflichten zu genügen. Die Archivierung bei externen Dienstleistern unterliegt strengen gesetzlichen Vorgaben, die vertraglich festzuhalten sind. Beispielsweise gelten die „Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme“, kurz GoBS, und in vielen Branchen Sonderregelungen, beispielsweise nach dem Kreditwesengesetz für Banken und Finanzinstitute. Eine gute Vertragsgestaltung ist sehr wichtig. Schlampt der Verantwortliche, kann er persönlich in die Haftung genommen und zum Schadensersatz verurteilt werden. Zudem kann er sich bei nicht ordnungsgemäßer Beachtung der Archivierungsaufgaben ein Bußgeld einfangen.

Tobias Haar

Regelmäßig zeigen Studien, dass ein hoher zweistelliger Prozentsatz aller erwünschten E-Mails unbeantwortet bleibt. Angesichts dessen scheint es egal zu sein, ob die False-Positive-Quote, die eine Filtersoftware dem hinzufügt, bei einem Millionstel oder sogar noch darunter liegt. Wenn unerwünschte E-Mails auf korrekte Weise abgewiesen werden, gibt es ohnehin keine „False Positives“ in dem Sinne, dass eine E-Mail unbemerkt im Nirvana verschwindet, denn dann erfährt der Absender umgehend von seinem eigenen Mailserver, dass die Zustellung nicht geklappt hat.

Wichtiger als die ohnehin kaum überprüfbare False-Positive-Kennzahl ist die Erkennungsrate. Ein Spam-Filter sollte angesichts der derzeitigen Spam-Quote von weit über 90 Prozent schon etwa 99 Prozent des Mülls erkennen, damit Anwender mit durchschnittlich „verbrannten“ Mail-Adressen deutlich mehr Erwünschtes im Posteingang vorfinden als durchgegrutschten Spam.

## Fazit

Die Entscheidung, externen Dienstleistern Verantwortung für die eigenen E-Mails zu übertragen, fällt manchem im Zeitalter der Datenschutzskandale nicht leicht. Viele treffen sie eher notgedrungen als aus Begeisterung für einen innovativen Service. Oftmals gibt die Herausforderung den Ausschlag, mit den täglichen und in letzter Zeit wieder stark wachsenden Spam-Massen zurechtzukommen zu müssen.

Wer Misstrauen beim Auslagern von Internet-Dienstleistungen hegt und deswegen zögert, eigene E-Mails von Dritten verarbeiten zu lassen, sollte sich darüber im Klaren sein, dass theoretisch ohnehin jeder der am Datentransport Beteiligten alles mitlesen kann. Eine Ende-zu-Ende-Verschlüsselung sollte daher ohnehin selbstverständlich sein – nicht nur bei geschäftskritischen Mails. (un)

## Literatur

- [1] Jo Bager, Joerg Heidrich; Gut abgelegt; E-Mails rechtssicher archivieren; c't 13/2009, S. 144
- [2] Bert Ungerer; Sendungsbewusst; E-Mail-Marketing: Fehler beim Newsletterversand und deren Vermeidung; iX 8/2006, S. 92