



Tutorial: Robuste Mailserver einrichten, Teil 1

Sendeplan

Peer Heinlein

Trotz aller Bedrohungen von außen stellt sich beim Analysieren der E-Mail-Infrastruktur von Unternehmen meist heraus, dass Schwierigkeiten mit Mailservern hausgemacht und unnötig sind. Grund genug für ein dreiteiliges Tutorial, das die Stolperstellen aufdeckt. Erster Teil: das richtige Versenden von E-Mails.

An sich handelt es sich bei E-Mail „nur“ um einen Internetdienst von vielen. Aber jede Fehlkonfiguration oder auch nur Laxheit kann sich wegen des ausufernden Missbrauchs von E-Mail besonders stark auswirken, weil die vorgesehenen Empfänger denjenigen, der ihnen Mails senden möchte, gründlich unter die Lupe nehmen. Zu

den ersten und wichtigsten Kriterien gehört das Domain Name System (DNS), dem ein Mailserver-Admin daher besondere Beachtung schenken sollte.

Der DNS Pointer Record etwa, der sogenannten Reverse Lookups dient (Abfrage eines Namens zu einer IP-Adresse), gilt allgemein als überflüs-

sige Formsache. Bei Webservern bleibt er beispielsweise unbeachtet, schließlich hat sich der Client den Server ja selbst ausgesucht. Anders verhält es sich bei Mailservern, die beim Mailversand auch als Clients auftreten und von der Gegenstelle entsprechend misstrauisch beäugt und überprüft werden.

Name beeinflusst die Reputation

Das hat seinen Grund: Fehlerhafte DNS-Daten und gefälschte HELO-Meldungen gehören zu typischen Kennzeichen von Spam-Bot-Netzen. Umso penibler sollten echte Mailserver konfiguriert sein – andernfalls ist vorhersehbar, dass die versandten E-Mails unnötig oft in Spamfiltern hängenbleiben.

Ein gültiger, korrekter DNS Reverse Lookup ist darum Pflicht. Der für die IP-Adresse des Servers ausgegebene Hostname muss seinerseits wieder zur IP-Adresse führen, sodass Vorwärts- und Rückwärtsauflösung konsistent sind („double lookup“). Wer hier ungenau ist und einen Hostnamen setzt, der zu einer anderen IP-Adresse führt, handelt sich Schwierigkeiten beim Mailversand ein. Folgendes sollte möglichst nicht passieren:

```
# host 91.198.250.11
11.250.198.91.in-addr.arpa domain name pointer
mx1.heinlein-support.de
# host mx1.heinlein-support.de
mx1.heinlein-support.de has address
213.203.238.10
```

Auch gar nicht im DNS vorhandene Hostnamen sind leider häufig zu sehen:

```
# host 91.198.250.10
10.250.198.91.in-addr.arpa domain name pointer
mx1.heinlein-support.local
# host mx1.heinlein-support.local
Host mx1.heinlein-support.local not found: 3 7
(NXDOMAIN)
```

Manch einer nutzt gar den Default-Eintrag des Providers:

```
# host 91.198.250.10
10.250.198.91.in-addr.arpa domain name pointer
10.250.198.91.static.inetbone.net.
```

In diesem Fall setzt man sich sogar bei eigentlich statischen IP-Adressen dem Risiko aus, dass andere sie bei unglücklicher Namensgebung irrtümlich für den Teil eines „dynamischen“ Dialup-Bereichs mit immer wieder neu vergebenen Adressen halten. Und von so einem Mailserver nehmen viele grundsätzlich keine Mails an.

Die Änderungen für den Pointer Record sind nicht in der Domain-Zone, sondern in der Zone der IP-Adresse vorzunehmen. Kleine und mittlere Unternehmen mit gemieteten Standleitungen müssen dafür häufig den jeweiligen Upstream-Provider kontaktieren, von dem sie die IP-Adressen bekommen haben – ein so geringer wie lohnender Aufwand.

Auch der vom Mailserver benutzte Hostname, mit dem er sich bei anderen Mailservern für den Versand von E-Mails im Rahmen des SMTP-HELO-Kommandos meldet, muss im DNS auflösbar sein. Häufig sind nicht existente Hostnamen mit Fantasie-Domains im Einsatz – gerade Exchange-Server melden sich aufgrund der Default-Einstellung „firma.local“ des Active Directory häufig mit einem im weltweiten DNS nicht existierenden HELO-Namen wie „mail.firma.local“.

Saubere Hostnamen sind Pflicht

Technisch gesehen hat der HELO-Hostname keine große Bedeutung, da er sich beliebig „fälschen“ lässt. In der Praxis gleicht er jedoch einer Visitenkarte und dient als wichtiges Unterscheidungsmerkmal zwischen „richtigen“ Mailservern und den simpel gestrickten SMTP-Engines großer Bot-Netze. Wenn diese auf einem infizierten Windows-PC hinter einem DSL-Router mit NAT arbeiten, sind sie häufig nicht in der Lage, einen für sie korrekten Hostnamen mitzusenden. Aus diesem Grund muss der HELO-Hostname eines echten Mailservers exakt zu dessen Reverse-Lookup passen. Selbst wer lediglich einen ähnlichen Hostnamen mit abweichender Schreibweise wie „mail5.example.com“ benutzt, obwohl die IP-Adresse laut DNS zu „mail.example.com“ gehört, holt sich unnötigen Ärger ins Haus.

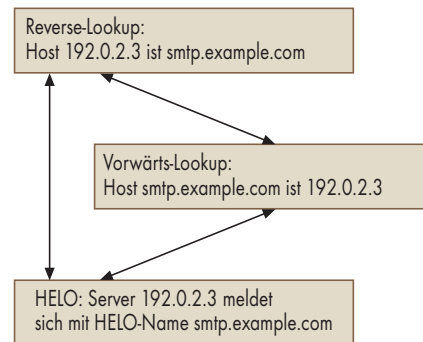
Spamfilter lehnen Mails in solchen Fällen häufig mit der Begründung „helo/hostname mismatch“ ab – zu Recht.

Die DNS-Daten eines Servers müssen stets in jeder Blickrichtung konsistent sein: Die IP-Adresse des Servers ergibt einen Namen, der via DNS wiederum auf die IP-Adresse zeigt. Und am Ende nutzt der Server genau diesen Namen als HELO-Hostnamen während der SMTP-Sessions.

Privatnutzung fast immer erlaubt

Wenige Unternehmen regeln die private Nutzung von E-Mail oder anderen Internetdiensten. Dabei drohen gerade in diesem Bereich erhebliche rechtliche und geschäftliche Risiken, derer sich IT-Administratoren, vor allem aber auch die Unternehmensleitung, bewusst sein sollten. In aller Regel berufen sich die Beteiligten auf ein zu Urzeiten ausgesprochenes oder schriftlich fixiertes Verbot privater Nutzung – müssen jedoch gleichzeitig eingestehen, dass sie de facto auf allen Hierarchieebenen verbreitet ist.

Das deutsche Recht verlangt in diesem Bereich keine bestimmte Form. Mündliche wie konkludente Einigungen (schlüssiges Handeln) sind der schriftlichen Regelung gleichgestellt. Entscheidend ist nur die Frage, worauf sich Unternehmen und Mitarbeiter geeinigt haben. Schriftlich fixierte Verbote sind obsolet, wenn das Unternehmen die allgemeine private Nutzung im Unternehmen tatsächlich kennt und toleriert oder gar explizit (mündlich) erlaubt. Juristen sprechen von der „betrieblich ausgeübten Praxis“ und kommen zu dem Schluss, dass die private Nutzung im Unternehmen in aller Regel doch zumindest wissentlich geduldet und damit erlaubt ist – veraltete schriftliche Vereinbarungen hin oder her.



Hostname, Reverse-Lookup und HELO-Hostname müssen exakt übereinstimmen, sollen E-Mails nicht in Spamverdacht geraten (Abb. 1).

Doch die freundliche Großzügigkeit eines Unternehmens kann sich als teurer Bumerang erweisen, denn der Anspruch auf private Mails kann praktisch zum Bestandteil des Arbeitsvertrages werden, den der Arbeitgeber kaum noch einseitig ändern kann.

Erhebliche juristische Risiken

Für Unternehmen tut sich damit ein Abgrund juristischer Komplikationen auf. Personenbezogene private Daten unterliegen dem Bundesdatenschutzgesetz – und dürften genau genommen gar nicht dauerhaft gespeichert werden, beispielsweise im mehrwöchigen oder auf Ewigkeit angelegten Backup oder Mailarchiv des Unternehmens. Mitarbeiter könnten selbst im Krankheits- oder Kündigungsfall ihrem (ehemaligen) Arbeitgeber den Zugriff auf ihr Postfach untersagen, wenn sich darin private E-Mails befinden (können!). Ein Umstand, der ein Unternehmen in den Ruin treiben kann – oder zumindest ein wirkungsvolles Druckmittel gekündigter Arbeitnehmer ist, die ihre Abfindung in die Höhe schrauben wollen.

Kaum ein Unternehmer weiß, welches hohe juristische wie unternehmerische Risiko er eingeht, wenn er aus Gefälligkeit die private Nutzung toleriert. Neben dem (meist unerwünschten) Verbot der privaten Nutzung bleibt allein die Schaffung einer eigenen Mail-Infrastruktur für private Zwecke – mit eigenen Mailadressen, zum Beispiel per Subdomain wie in „user@privat.example.com“. Auch eine vom Mailclient des Desktops klar abgegrenzte Nutzungsmöglichkeit, zum Beispiel durch einen Webmailer, kann zur Trennung hilfreich sein.

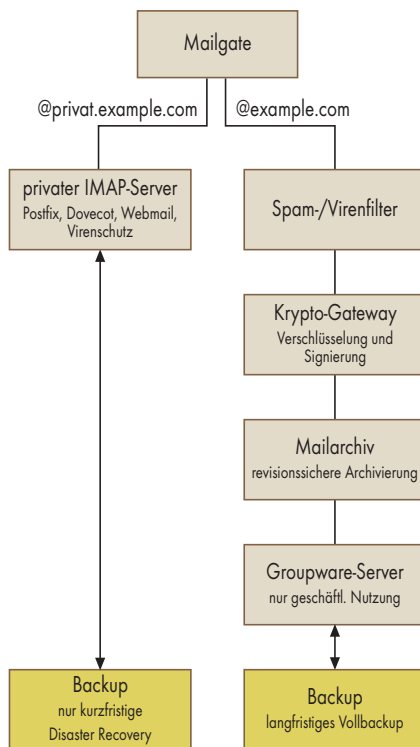


- Die Mailserver-Infrastruktur in Unternehmen sollte insbesondere in Sachen DNS sorgfältig geplant sein.
- Wer nicht nur ein-, sondern auch ausgehende E-Mails auf Spam- und Virenbefall prüft, leistet einen wichtigen Beitrag zur Netzsicherheit.
- Mitarbeitern, die Unternehmens-Mailserver mitnutzen dürfen, sollten dafür dedizierte Systeme und eine eigene Domain bekommen, um rechtliche Komplikationen zu vermeiden.

Seit einigen Jahren befinden sich Mechanismen wie SPF (Sender Policy Framework) oder DKIM (Domain Key Identified Mail) als Spamschutz in der Diskussion – was eigentlich gar nicht korrekt ist. Beide können lediglich dem Fälschen der Absenderadressen von E-Mails entgegenwirken. Damit lässt sich definieren, welche Server für welche Absender-Domains zuständig sind. Das hat immerhin indirekte Auswirkungen auf die Verbreitung von Spam, da es das Versenden von Mails mit beliebig ausgedachten fremden Domains erschweren kann. Leider lassen einige Domain-Registrierungsstellen eine kostenlose Test-Registrierung von Domains zu, die Spammer einige Tage lang unbehelligt nutzen können – inklusive Authentifizierung. Insofern ist der tatsächliche Effekt bislang äußerst gering.

Authentifizieren von Absenderadressen

Stattdessen überwiegen die Nebenwirkungen: Viele erwünschte E-Mails gehen wegen unglücklicher SPF-Einstellungen verloren. Neben den in den



Mit einem separaten IMAP-Server parallel zur Unternehmens-Groupware können Arbeitgeber ihren Mitarbeitern auf rechtlich einwandfreie Weise private Maildienste zur Verfügung stellen (Abb. 2).

DNS-Daten einer Domain einzutragen- den SPF-Daten definieren zu viele Admins über das Schlüsselwort *-all*, dass E-Mails aus ihrer Domain von sämtlichen nicht genannten Servern als unerwünscht anzusehen sind.

Das mag auf den ersten Blick richtig sein, birgt jedoch Tücken: Weiterleitungen, Mailinglisten, Forenbeiträge, Link-Empfehlungen, Web-Grußkarten und andere gebräuchliche Kommunikationsformen bringen es mit sich, dass auch andere Server E-Mails mit der eigenen Mailadresse als Absenderangabe versenden. Daher nützt es auch nichts, das Empfangen von E-Mails mit der eigenen Absenderdomain pauschal zu unterbinden.

Selbst große Provider wie GMX definieren in ihren eigenen SPF-Records jedoch ein *-all*, schließen also das Versenden von E-Mails mit GMX-Absendern über andere Server kategorisch aus. Auch eine Art von Kundenbindung:

```
# host -t TXT gmx.de
gmx.de descriptive text "v=spf1
ip4:213.165.64.0/23 ip4:74.208.5.64/26 -all"
```

Empfiehlt ein GMX-Nutzer nun einem anderen GMX-Nutzer einen Artikel auf heise online, sieht GMX die nun vom Heise-Mailserver ausgehende E-Mail der eigenen Kunden höchstwahrscheinlich als Spam an.

SPF und SRS: Mehr Fragen als Antworten

Geht es nach den SPF-Erfindern, soll das „Sender Rewriting Scheme“ (SRS) derlei Ungemach verhindern. SRS wirft jedoch mehr Fragen auf als es Antworten gibt – und kein derzeit bekannter Mailserver unterstützt es. Es empfiehlt sich darum, in SPF-Records stattdessen ein *~all* oder *?all* zu setzen:

```
host -t TXT heinlein-support.de
heinlein-support.de descriptive text "v=spf1
ip4:213.203.238.0/25 ip4:195.10.208.0/24 mx
include:jpberlin.de ?all"
```

DKIM hingegen verhält sich gegenüber Weiterleitungen tolerant, da die kryptografischen Signaturen beim Weiterleiten erhalten bleiben und sich weiterhin überprüfen lässt, ob eine signierte E-Mail tatsächlich von einem Mail-Relay der jeweiligen Domain stammt. Insofern entfallen zahlreiche Designschwächen von SPF. Doch auch hier lauert Gefahr: Die erst jüngst in RFC 5617 gegossenen „Author Domain Sig-

ning Practices“ (ADSP) ermöglichen es Postmastern, vorzugeben, wie andere Systeme mit unsignierten E-Mails ihrer Domain umgehen sollten.

Auch hier besteht die Gefahr, dass Postmaster ihre Systeme so konfigurieren, dass alle Mails ihrer Domain stets signiert sein müssen und andernfalls verworfen werden dürfen. Bei einer rein geschäftlichen oder sicherheitskritischen Nutzung mag das sinnvoll sein – bei normaler privater Nutzung dürften auch hier die naturgemäß unsignierten, aber zulässigen Mails aus verschiedenen Webdiensten verloren gehen.

Business-Signaturen müssen sein

Seit „elektronische“ Handelsbriefe denjenigen auf Papier gleichgestellt sind, müssen Unternehmen E-Mails mit den üblichen handelsrechtlichen Angaben ausstatten – dazu gehören die Handelsregisternummer, der Sitz des Unternehmens oder bei Aktiengesellschaften auch der Name des Vorsitzenden des Aufsichtsrates. Diese Angaben müssen nach einschlägiger Rechtsprechung in der E-Mail selbst enthalten sein, versteckte Angaben im Mail-Header oder ein Link auf ein Web-Impressum genügen nicht.

Die meisten Unternehmen haben diese Anforderungen umgesetzt. Einige schießen aber über das Ziel hinaus. Wer sämtliche E-Mails zwangsweise mit der Geschäftssignatur versieht, lässt auch private E-Mails der Mitarbeiter plötzlich quasi auf „Firmen-Mail-Briefpapier“ versenden, was interessante juristische Fragen rund um Anscheins- und Duldungsvollmachten aufwirft. So kann etwa der Eindruck entstehen, die private Versteigerung auf eBay erfolge in Wirklichkeit im Namen des Unternehmens.

In der Offline-Welt dürfte die Nutzung des Unternehmens-Briefpapiers zu privaten Zwecken in aller Regel mindestens zu einer arbeitsrechtlichen Abmahnung, wenn nicht sogar zur Kündigung führen. Im Internet hingegen herrscht hier oft allgemeine Sorg- und Gedankenlosigkeit bei allen Beteiligten.

Disclaimer: Juristisch wirkungslose Prosa

Viele Unternehmen erweitern die Pflichtangaben in Mailsignaturen um eine längere Signatur, die den Empfänger

über dessen angebliche Pflichten aufklärt – zum Beispiel: Die Mail sei ausschließlich für ihn bestimmt und nicht weiterzugeben. Sollte das doch nicht der Fall sein, sei die E-Mail zu löschen und der Absender über dessen Irrtum zu informieren. Und für das Weiterleiten „unberechtigt“ empfangener E-Mails stehen teils empfindliche Strafandrohungen im Raum.

Derartige „Disclaimer“ sind ebenso weit verbreitet wie juristisch wirkungslos. Eine rechtliche Wirksamkeit könnten sie als privatrechtliche Verträge zwischen Absendern und Empfängern nur dann entfalten, wenn beide Parteien zustimmen. Ein Absender kann Empfängern derlei jedoch nicht einseitig aufzwingen. In das bloße Empfangen und Lesen einer E-Mail kann niemand hineinkonstruieren, der Empfänger würde sich den in der E-Mail-Signatur enthaltenen Vorschriften unterwerfen wollen. Für eine juristische Wirksamkeit der E-Mail-Disclaimer fehlt in aller Regel ein entsprechender beiderseitiger Vertrag.

Disclaimer lassen sich also allenfalls als (ganz unjuristische) Bitte an den Empfänger verstehen – nicht mehr, nicht weniger. Ob dieser der Bitte jedoch folgen möchte, ist alleine seine Entscheidung. Da Disclaimer oft sowie so nur allgemeine Selbstverständlichkeiten beschreiben, dürften sie vorrangig als überflüssiger Datenschnitt anzusehen sein.

Allenfalls wenn zwei Vertragsparteien bereits einen wirksamen Geheimhaltungsvertrag geschlossen haben (Non-Disclosure Agreement, NDA), könnte eine entsprechende Mailsignatur sicherstellen, dass besagte E-Mail zweifelsfrei darunterfallen soll. Üblicherweise sind NDAs jedoch so weitreichend formuliert, dass auch dafür keine Notwendigkeit besteht. Und sollte eine E-Mail versehentlich an einen unbeteiligten Dritten gehen, so wäre auch der kein Vertragspartner des NDA und damit auch nicht an etwaige Vorgaben der Signatur gebunden.

Versuch und Irrtum

Als es vor vielen Jahren im Internet noch recht gemächlich zugeht, galt es als sinnvoll, E-Mails bis zu fünf Tage lang zu speichern, sollte ein Zielsystem vorübergehend nicht erreichbar sein. In dieser Zeit versucht der Client weitere Zustellungen – und erst nach Ablauf der Frist erhält der Absender eine Be-

nachrichtigung über den missglückten Versand.

Aus heutiger Sicht dürften fünf Tage zu lang sein. In der Zeit, in der eine E-Mail beispielsweise aufgrund eines Tippfehlers im Domainnamen auf den Servern dahinsiecht, kann im Privat- wie auch im Geschäftsleben schon viel passiert sein.

Heute gilt darum eine Zeit von drei, eventuell sogar nur zwei Tagen als sinnvoll. Die Anwender können davon ausgehen, dass relevante Mailserver heute kaum einmal so lange ausfallen. Gleichzeitig sollte die Frist nicht allzu kurz sein, damit beispielsweise regulär geplante Wochenend-Wartungsarbeiten nicht gleich in Mail-Rückläufern (Bounces) enden.

In der Mailserver-Software (Mail Transfer Agent, MTA) Postfix kann man die Zeit bis zum Bounce leicht auf drei Tage senken:

```
postconf -e "maximal_queue_lifetime=3d"
```

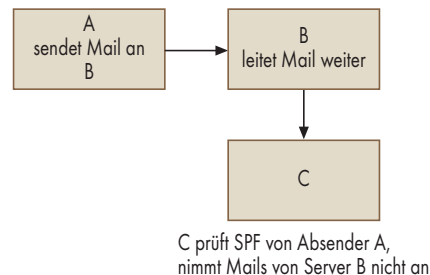
Zu unterscheiden sind an dieser Stelle „echte“ E-Mails und Bounces. Ist selbst die Bounce-Nachricht nicht mehr zustellbar, liegt häufig wirklich etwas im Argen. In aller Regel handelt es sich dann kaum mehr um echte E-Mails, sondern um Spamrückläufer oder andere verquere E-Mails. Auf stark belasteten Servern kann es darum hilfreich sein, speziell deren Lebensdauer auf einen Tag zu senken:

```
postconf -e "bounce_queue_lifetime=1d"
```

Ausgehende Spamfilterung

Ein Inhaltsfilter für eingehende E-Mails ist in nahezu jedem Netz selbstverständlich. Anders lässt sich die Spam- und Virenflut kaum in den Griff bekommen. Umso erstaunlicher, dass den ausgehenden Mailverkehr selten ein Filtersystem kontrolliert. Sind Administratoren gegenüber der technischen Kompetenz ihrer Nutzer sonst oftmals skeptisch eingestellt, herrscht in Sachen Mailversand ungetrübt Vertrauen.

Zu Unrecht: Neben vorsätzlich agierenden schwarzen Schafen in der Anwenderschaft sind gehackte Webformulare oder virenfizierte Windows-PCs im eigenen Netz Anlass genug für das Filtern ausgehender E-Mails. Anderenfalls ist es nur eine Frage der Zeit, dass vom eigenen Netz Spam ausgeht. Die IP-Adresse des Mailservers kann in solchen Fällen schnell auf einer der



Mit Verfahren wie SPF können Weiterleitungen ins Stocken geraten oder auf Servern Dritter generierte E-Mails unter Spamverdacht geraten (Abb. 3).

zahlreichen Blacklists (DNSBLs) landen. Er kann dann für eine gewisse Zeit praktisch keine E-Mail mehr versenden. Ein Administrator sollte schon aus reinem Selbstschutz dem ausgehenden E-Mail-Verkehr mit mindestens ebenso viel Misstrauen begegnen wie dem eingehenden. Ein Filter kann die Aufmerksamkeit frühzeitig auf einen etwaigen Virenbefall im eigenen Netz lenken.

Unter Postmastern umstritten ist die Idee, den ausgehenden Port 25 für einen direkten SMTP-Versand durch die Clients zu sperren. Bot-Netze lassen sich auf diese Weise daran hindern, Spam direkt von den betroffenen „Zombie“-PCs aus über eigene SMTP-Engines zu versenden. Das hindert jedoch jeden Anwender daran, Port 25 zu nutzen – beispielsweise zum Abliefern eigener E-Mails bei einem externen Provider. Theoretisch ließe sich ein Firmen-Mailserver dafür nutzen, Mails mit privaten Domains in den Absenderadressen zu versenden. In der Praxis machen jedoch Systeme wie SPF dem Ganzen einen Strich durch die Rechnung.

Neben Port 25 bieten darum viele Provider den Port 587 (Submission) zum Einliefern von Mails an, bei dem es sich in Wirklichkeit um nichts anderes als einen SMTP-Port mit zwangsweise vorgeschriebener Authentifizierung über SMTP-AUTH handelt. Die Absender könnten also bei einer Sperre von Port 25 in der Firewall ihres Arbeitgebers oder Providers einfach auf Port 587 ausweichen. Leider bieten viele Provider ihren Kunden keine Mail-Einlieferung über den Submission-Port an – aus Unwissenheit. Einen technischen Grund dafür gibt es nicht.

In Postfix ist Port 587 in der *master.cf* schnell aktiviert – und wie die *smtpd_client_restrictions* des *smtpd*-

Moduls zeigen, handelt es sich um nichts weiter als eine normale SMTP-AUTH-Verbindung:

```
submission inet n - n - - smtpd
-o smtpd_etrn_restrictions=reject
-o smtpd_client_restrictions=permit_sasl_7
authenticated,reject
```

SMTP-Verbindungen von Anwendern mit Desktop-Mailclients genießen hohe Priorität – schließlich führt selbst ein temporärer Übertragungsengpass sofort zu einer Warnmeldung auf dem Desktop des Anwenders, dessen Mails nun in der Outbox liegen bleiben und der womöglich ein Ticket beim Helpdesk aufmacht. Mit Mails von anderen Relays hingegen kann man deutlich rabiater umgehen: Hier führt ein temporärer Fehler in der Mail-Übertragung ja lediglich zu einer Speicherung in der Queue des einliefernden Mailsystems und zu einem erneuten Zustellversuch nach wenigen Minuten, sodass temporäre Übertragungsfehler kaum auffallen.

SMTP ist nicht gleich SMTP

Verbindungen von Desktop-Clients, also in der Regel ausgehende Mails, sollten daher vom eingehenden Mailverkehr anderer Mailserver getrennt sein. Da in beiden Fällen Port 25 zum Einsatz kommt, bietet sich einfach eine zweite IP-Adresse an. Gerade Rootserver können davon profitieren: Die MX-Records der Domain annoncieren für den Mailempfang einen Hostnamen wie mx01.example.com, der auf die erste IP-Adresse des Systems zeigt. Hinter dem von den Mailclients genutzten Hostnamen (mail.example.com) hingegen verbirgt sich die zweite IP-Adresse des Systems.

Auf diese Weise können Postmaster über ein getrenntes Rate Limiting sicherstellen, dass den Desktop-Clients sogar während einer Flut eingehender Spam- oder Bounce-Mails („Backscatter“) stets eine ausreichende Zahl an SMTP-Verbindungen zur Verfügung steht. Zudem lässt sich der Server für

Desktop-Nutzer auf einfache Weise etwas anders konfigurieren – beispielsweise was Spamschutz angeht, automatisches Anhängen von E-Mail-Signaturen mit Geschäftsdaten, automatisches Verschlüsseln oder Signieren mittels S/MIME oder GPG oder eine Authentifizierung der Adressen ausgehender E-Mails mittels DKIM. Wer beispielsweise beim eingehenden Mailverkehr eine Spam- und Virenfilterung in Echtzeit anstrebt (Pre-Queue-Filter, mehr dazu im nächsten Teil dieses Tutorials), sollte E-Mails authentifizierter Nutzer lieber weiterhin im Post-Queue-Modus filtern, da keine Backscatter-Mails nach außen gelangen können.

Wenn das System zwei IP-Adressen aufweist, lassen sich außerdem über die *master.cf* von Postfix auf einfache Weise *smtpd*-Prozesse mit unterschiedlichen Optionen an diese IP-Adressen binden – inklusive Submission-Port:

```
# Mails anderer Mailserver
mx.example.com:smtp inet n - n - - smtpd
-o smtpd_proxy_filter=127.0.0.1:10024

# Mails authentifizierter Nutzer
mail.example.com:smtp inet n - n - - smtpd
-o content_filter=smtp:[127.0.0.1]:10024

mail.example.com:submission inet n - n - - smtpd
-o smtpd_etrn_restrictions=reject
-o smtpd_client_restrictions=permit_sasl_7
authenticated,reject
-o content_filter=smtp:[127.0.0.1]:10024
```

Das SSL-Zertifikat des Servers sollte auf den von den Clients genutzten Hostnamen ausgestellt sein – in diesem Beispiel mail.example.com. Es kann jedoch trotzdem pauschal für den gesamten Server gelten, da einliefernde Mailserver – anders als die Mailprogramme der Nutzer – nicht auf den richtigen Hostnamen im Zertifikat achten müssen.

Durchdachte Hostnamen sind hilfreich

Fehler, die einem Administrator unterlaufen, kommen manchmal erst nach Jahren zum Vorschein. Wildwuchs in den Hostnamen oder IP-Adressen der Clients gehört zu den oft begangenen „Jugendsünden“, die sich rächen, sobald Änderungen am Netz anstehen.

Obwohl fast jeder öffentliche Server und Desktop-PC über eine funktionierende DNS-Auflösung verfügt – schließlich wollen die Anwender ja „ins Internet“ – finden sich nicht sel-


ten fest konfigurierte IP-Adressen in den Einstellungen der Anwender. Eine Änderung der Server-IP-Adresse kann damit schnell einen unüberschaubaren Aufwand nach sich ziehen. Wer stattdessen konsequent Hostnamen verwendet, kann mit kleinen Änderungen im DNS-Zonefile der Domain Mailserver in andere Adressbereiche verfrachten, ohne dass es die Anwender bemerken.

Darüber hinaus empfiehlt es sich, Hostnamen zu verwenden, die der Funktionsbeschreibung dienen: Ein Mailserver namens „smtp.example.com“ dient dem Mailversand und (poplimapmail).example.com dem Mailempfang über POP3 oder IMAP. Selbst wenn derzeit dieselbe Maschine SMTP und POP3/IMAP erledigt, kann es nur zu bald notwendig sein, die Dienste aus Lastgründen auf zwei separate Maschinen zu verteilen.

Wohl dem, der für alle Dienste jeweils passende Hostnamen an seine Anwender herausgegeben hat. Gerade kleine Provider in der Wachstumsphase bekommen gelegentlich zu spät die eigenen Fehler der Anfangsphase zu spüren. Wer an IP-Adressen nicht sparen muss, sollte dabei nicht nur verschiedene Namen anlegen, sondern auch von vornherein für SMTP und POP3/IMAP jeweils eigene IP-Adressen nutzen, selbst wenn sie zunächst auf ein und demselben Server zusammenlaufen. Nur wenn Port 25 lediglich auf der IP-Adresse von smtp.example.com erreichbar und die Ports 110 und 143 lediglich auf der IP von mail.example.com verfügbar sind, ist sichergestellt, dass die Anwender stets gezwungenermaßen die richtigen Hostnamen in ihren Mailclients konfigurieren.

Eine spätere Auftrennung der Dienste wird dann zum Kinderspiel: Das Einrichten eines weiteren Servers und eine kleine Änderung im DNS genügt. Bei korrekter Planung bemerkt kein Anwender die Änderung. Ist hingegen jeder Dienst über jede IP-Adresse erreichbar, werden sich im Laufe der Zeit so viele „falsch“ konfigurierte Mailclients einschleichen, dass eine scheinbar harmlose Umstellung im Chaos mit hohem Support-Aufwand enden wird. (un)

PEER HEINLEIN

ist seit 1992 auf E-Mail spezialisiert, Autor des „Postfix-Buchs“ und für die Mailserver, Spam- und Virenabwehr diverser ISPs, Rechenzentren und Unternehmen verantwortlich. 

Tutorialinhalt

Teil I: E-Mails sicher versenden

Teil II: Alle E-Mails außer Spam empfangen

Teil III: E-Mails korrekt erzeugen