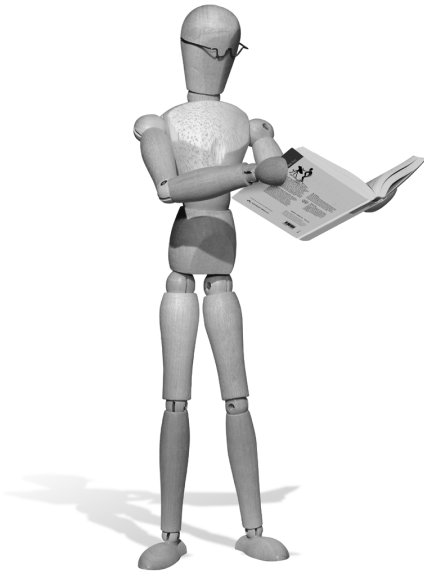


Alistair McDonald

SpamAssassin

Leitfaden zu Konfiguration, Integration
und Einsatz



ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam



3 Offene Relays

Ursprünglich wurde das Internet von einer vertrauensvollen Gemeinschaft genutzt. Sites waren *offen*, die Informationen darin frei verfügbar, Passwörter und Benutzerkonten wurden geteilt und sogar veröffentlicht. E-Mail-Server nahmen E-Mails aus jeglichen Quellen an und sendeten sie an ihr Ziel. Heutzutage hat sich die Natur des Internets gewandelt. Informationen werden nicht mehr so freigebig zur Verfügung gestellt, und Benutzerkonten und Passwörter werden geschützt. Nur noch selten lässt sich ein Server finden, der E-Mails von einem unbekanntem Benutzer annimmt und weiterleitet. Letzteres ist eine unmittelbare Konsequenz aus dem Aufkommen von Spam und den damit verbundenen Kosten und Risiken.

Spam ist zu einem so großen Problem geworden, dass ISPs die Konten von Spammern löschen, die ihnen gemeldet werden. Infolgedessen suchen Spammer nach *offenen Relays*, also nach E-Mail-Servern, über die unbekannte und nicht authentifizierte Benutzer E-Mails senden können. Wenn sie ein solches Relay entdecken, nutzen Spammer es aus, um darüber ihre Spam-E-Mails zu versenden. Dadurch ist es nicht möglich, Spam zu seiner eigentlichen Quelle zurückzuverfolgen.

Ein offenes Relay zu betreiben, zieht für einen Systemadministrator ernste Konsequenzen nach sich. Der Server kann in einer der Open Relay Blacklists (ORBLs) aufgeführt werden. Sobald dies geschehen ist, besteht die Möglichkeit, dass E-Mails von diesem Server von anderen Systemen als Spam zurückgewiesen werden. Außerdem kann die Internetverbindung vom Anbieter zeitweilig oder vollständig abgeschaltet werden, falls das offene Relay nicht so schnell wie möglich nach einer Benachrichtigung geschlossen wird.

Glücklicherweise können alle weit verbreiteten MTAs (Mail Transfer Agents) auf einfache Weise so konfiguriert werden, dass sie sich nicht als offenes Relay benutzen lassen. Für die in diesem Buch besprochenen MTAs – *Sendmail*, *Postfix*, *Exim* und *qmail* – ist dies das Standardverhalten nach der Installation. Bei einer älteren Version dieser MTAs ist die Standardkonfiguration unter Umständen nicht sicher. Falls die Konfiguration eines MTAs geändert wurde, kann dadurch unbeabsichtigt ein offenes Relay geschaffen worden sein.

3.1 E-Mail-Zustellung

Im vorkommerziellen Internet gab es keine direkten Verbindungen zwischen den Systemen. E-Mails für System D wurden von System A an System B und dann an System C gesendet, bevor sie dem System D zugestellt wurden. Der Vorgang, E-Mails für ein anderes System anzunehmen, wird *Relaying* (Weiterleitung) genannt, die betreffenden Computer *Relays*. Administratoren haben ihre Rechner als Relays konfiguriert, um anderen zu helfen. Durch die Teilnahme an diesem Relay-Mechanismus wurde die Last auf die ganze Gemeinschaft aufgeteilt.

Die Ausnutzung von Relays durch Spammer hat die Administratoren dazu gebracht, die Sicherheitsmaßnahmen zu verstärken und E-Mails aus unbekanntem Quellen abzulehnen, sofern sie nicht für einen lokalen Benutzer bestimmt sind. Die Computer müssen also nach wie vor E-Mails für lokale Benutzer akzeptieren, die von anderen Domains kommen oder an diese adressiert sind.

Ein Server sollte alle E-Mails akzeptieren, die von seinen lokalen Benutzern stammen. Darüber hinaus sollte er nur E-Mails für Benutzer und Domains annehmen, an die er tatsächlich ausliefern kann. Wenn ein Server E-Mails für andere Domains akzeptiert, wird er dadurch zu einem offenen Relay.

Ein MTA sollte wie folgt konfiguriert werden:

- Er soll E-Mails für die Domains annehmen, die er bedient, und E-Mails für andere Domains ablehnen.
- Lokale Benutzer sollen E-Mails an andere Domains senden dürfen.
- Eingehende E-Mail soll überprüft und in dem Fall abgelehnt werden, dass sie an ungültige Empfänger gerichtet ist.

Die Liste der Domains, an die der MTA E-Mails weiterleitet, befindet sich in der Konfigurationsdatei und kann vom Systemadministrator geändert werden. Lokale Benutzer können von der Netzwerkschnittstelle authentifiziert werden, um sicherzustellen, dass ihre Anforderungen über die IP-Adresse ihres Computers eingeht. Auch die Validierungsinformationen für diese Benutzer werden in einer Konfigurationsdatei gespeichert. MTAs setzen eine Vielzahl von Methoden ein, um E-Mail-Empfänger zu authentifizieren, darunter LDAP (*Lightweight Directory Access Protocol*) und PAM (*Pluggable Authentication Modules*).

3.2 Testverfahren für offene Relays

Es gibt eine Reihe von automatisierten Testverfahren für offene Relays. Alternativ können Sie diesen Test auch manuell durchführen.

3.2.1 Automatisierte Tests

Es stehen verschiedene automatisierte Testverfahren für offene Relays zur Verfügung. Um auf diese Dienste zurückgreifen zu können, ist eine Telnet-Sitzung erforderlich. Der bekannteste Relay-Tester ist `relay-test.mail-abuse.org`.

Um diesen Dienst zu nutzen, geben Sie das folgende Kommando am Befehlsprompt des zu testenden Mailservers ein:

```
telnet relay-test.mail-abuse.org
```

Im Folgenden sehen Sie eine Beispielsitzung:

```
$ telnet relay-test.mail-abuse.org
Trying 168.61.4.13...
Connected to cygnus.mail-abuse.org.
Escape character is '^]'.
Connecting to 999.888.777.666 ...
<<< 220 domain.com ESMTP My_MTA
>>> HELO cygnus.mail-abuse.org
<<< 250 domain.com
:Relay test: #Quote test
>>> mail from: <spamtest@mta.domain.com>
<<< 250 Ok
>>> rcpt to: <"nobody@mail-abuse.org">
<<< 554 <nobody@mail-abuse.org>: Relay access denied
>>> rset
<<< 250 Ok
:Relay test: #Test 1
>>> mail from: <nobody@mail-abuse.org>
<<< 250 Ok
>>> rcpt to: <nobody@mail-abuse.org>
<<< 554 <nobody@mail-abuse.org>: Relay access denied
>>> rset
<<< 250 Ok
...
>>> QUIT
<<< 221 Bye
Tested host banner: 220 domain.com ESMTP My_MTA
System appeared to reject relay attempts
Connection closed by foreign host.
```

Der Test dauert eine gewisse Zeit, dabei wird versucht, häufige Konfigurationsfehler und bekannte Sicherheitsprobleme von MTAs auszunutzen. Nach dem Abschluss der Überprüfung wird eine Zusammenfassung ausgegeben. In diesem Beispiel handelte es sich bei dem Server nicht um ein offenes Relay.

Es gibt weitere Dienste zur Überprüfung auf offene Relays. Eine Internetsuche nach den Begriffen »telnet open relay« wird einige davon finden.

3.2.2 Manuelle Tests

Diese Tests müssen auf einem Computer ausgeführt werden, der nicht mit dem Netzwerk verbunden ist, in dem sich der E-Mail-Server befindet, da der MTA die Verbindung ansonsten so betrachtet, als komme sie von einem vertrauenswürdigen Rechner. Eine Einwahlverbindung ist für diese Zwecke ideal. Bei diesem Test werden Befehle eingegeben, wie sie ein MTA verwendet, der E-Mail von einem entfernten Host sendet.

Geben Sie an einem Befehlsprompt Folgendes ein:

```
telnet mta.mycorp.com 25
```

Dabei ist `mta.mycorp.com` der Hostname des zu testenden MTAs und `25` der SMTP-Port. Achten Sie darauf, dass die E-Mail-Adressen in den Zeilen `MAIL FROM:` und `RCPT TO:` nicht von dem zu testenden MTA bedient werden. Im Folgenden sehen Sie eine Beispielsitzung:

```
$ telnet mta.mycorp.com 25
Trying 42.42.42.42...
Connected to mta.mycorp.com.
Escape character is '^]'.
220 mta.mycorp.com ESMTP some_mta
MAIL FROM:user1@someplace.org
250 Ok
RCPT TO:user2@anotherorg.com
250 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: user1@someplace.org
To: user2@anotherorg.com
Subject: Whatever
This has been relayed through mycorp.com
.
250 Ok: queued as 7A7F18D888
```

Wenn in der Ausgabe hinter dem Eintrag `RCPT TO:` eine Zeile auftaucht, die mit `250 Ok` beginnt, zeigt das an, dass die E-Mail zur Auslieferung angenommen wurde und dass der MTA als offenes Relay konfiguriert ist. Das folgende Beispiel zeigt einen Host, bei dem das Relaying deaktiviert wurde:

```
$ telnet mta.mycorp.com 25
Trying 42.42.42.42...
Connected to mta.mycorp.com.
Escape character is '^]'.
220 mta.mycorp.com ESMTP some_mta
MAIL FROM:user1@someplace.org
250 Ok
```

```
RCPT TO:user2@anotherorg.com
554 <user2@anotherorg.com>: Relay access denied
```

Die Fehlermeldung gibt an, dass der MTA die Weiterleitung der E-Mail aus einer nicht vertrauenswürdigen Quelle abgelehnt hat.

3.3 MTA-Konfiguration

Alle hier beschriebenen MTAs bieten weit gehende Konfigurationsmöglichkeiten. Testen Sie Änderungen nach Möglichkeit zunächst auf einem Testserver und nicht auf einem Produktivsystem, damit Sie die Konfiguration des MTA nicht so abändern, dass er nicht mehr korrekt funktioniert.

3.3.1 Sendmail

Sendmail ist der Urahn aller MTAs. Sein hohes Alter deutet darauf hin, dass er einiges von der Freundlichkeit des vorkommerziellen Internets geerbt hat, weshalb ältere Installationen E-Mails weiterleiten könnten. Wenn Sie eine ältere Installation konfiguriert und dann mit einer neueren aktualisiert haben, können einige der Konfigurationseinstellungen erhalten geblieben sein, die die Weiterleitung von E-Mails erlauben.

Sendmail befindet sich im Paket bei den meisten Linux-Distributionen sowie bei HP/UX, AIX, Solaris und anderen kommerziellen UNIX-Produkten, wobei jeder Hersteller die Konfigurationsdateien in einem anderen Verzeichnis unterbringen kann. In diesem Kapitel werden bei der Besprechung der Konfigurationsdateien die Standard-speicherorte und -dateinamen verwendet.

Sendmail Version 8.9 und höher

Bei Sendmail Version 8.9 und höher führt die Datei `/etc/mail/relay-domains` die Domains auf, für die Sendmail E-Mails akzeptiert. Die Syntax ist eine Liste von Domains oder IP-Adressen, wobei pro Zeile eine Domain aufgeführt wird:

```
mydomain.com
anotherdomain.com
myassociate.com
```

Wenn die Sendmail-Konfiguration geändert wurde, sollte das Programm neu gestartet und der weiter vorn beschriebene Test auf offene Relays durchgeführt werden.

Frühere Sendmail-Versionen

Bei früheren Sendmail-Versionen als 8.9 besteht die ideale Lösung in einer Aktualisierung. Falls dies nicht möglich sein sollte, führen Sie die folgenden Anweisungen aus:

1. Verwenden Sie `grep` mit einem Editor, um zu überprüfen, ob die Zeilen `use_ip` oder `check_rcpt4` in der Hauptkonfigurationsdatei von Sendmail, `sendmail.cf`, stehen:

```
$ cd /etc/mail
$ grep use_ip sendmail.cf
$ grep check_rcpt4 sendmail.cf
```

2. Wenn die Datei `sendmail.cf` die Zeilen `use_ip` oder `check_rcpt4` nicht enthält, sollten Sie sie am Ende der Datei `sendmail.m4` wie folgt hinzufügen:

```
HACK(\`use_ip',\`/etc/mail/LocalIP')dn]
HACK(\`check_rcpt4')dn]
```

3. Erstellen Sie die Datei `sendmail.cf` nach dem Ändern von `sendmail.m4` neu:

```
# m4 < sendmail.mc > sendmail.cf
```

4. Die Datei, in der `use_ip` aufgeführt wird, sollte nur die IP-Adressen enthalten, für die die Weiterleitung von E-Mail zulässig ist. Dabei steht jede IP-Adresse in einer eigenen Zeile. Subnetze lassen sich einfach dadurch angeben, dass Sie die letzte Ziffer in der durch Punkte getrennten Schreibweise weglassen:

```
127.0.0.1
10.100.0
```

Dieses Beispiel weist Sendmail an, eingehende E-Mails nur von `localhost` (127.0.0.1) und von Rechnern im Adressraum 10.100.0/24 anzunehmen.

3.3.2 Postfix

Postfix ist ein vergleichsweise moderner MTA, der von Anfang an auf Sicherheit ausgelegt wurde. Er ist modular aufgebaut, wobei jede Komponente gewöhnlich nur eine Aufgabe durchführt – was die Sicherheit sehr stark erhöht. Trotz seiner sehr verschiedenen internen Struktur ähnelt Postfix äußerlich Sendmail sehr, weshalb ältere Systeme, auf denen Sendmail verwendet wird, ohne große Schwierigkeiten auf Postfix umgestellt werden können.

Der Standardspeicherort für die Hauptkonfigurationsdateien von Postfix ist `/etc/postfix/main.cf`, aber dies gilt nicht für alle Distributionen. Standardmäßig leitet Postfix keine E-Mails weiter. Die Weiterleitung wird an zwei Stellen der Konfigurationsdateien festgelegt: der Konfigurationsdirektive `mynetworks` und dem Konfigurationsparameter `relay_domains`.

Die Konfigurationsdirektive `mynetworks`

Die Zeile `mynetworks` sollte nur die Rechner auflisten, für die Postfix E-Mail weiterleiten darf. Wenn sie nicht spezifiziert wird, schließt ihr Standardwert alle Rechner mit ähnlichen IP-Adressen ein. Dies ist jedoch für Produktivserver manchmal zu weit

gefasst. Es lohnt sich, dies auf eine strengere Bedingung abzuändern, da ansonsten ein teilweise offenes Relay entsteht, das E-Mails von Hosts im selben Subnetz weiterleitet.

Eine typische `mynetworks`-Direktive sieht etwa wie folgt aus:

```
mynetworks = 10.0.100.0, 127.0.0.1, 10.0.100.102
```

Diese Direktive erlaubt den Zugriff vom Server selbst über die Loopback-Schnittstelle zu `localhost` und von zwei anderen IP-Adressen. Eine oder beide davon können zum Hostsystem oder zu anderen Systemen innerhalb des Firmennetzwerks gehören. Dies ist ein Beispiel für eine strenge Einstellung.

Der Konfigurationsparameter `relay_domains`

Die andere wichtige Konfigurationseinstellung von Postfix in der Datei `main.cf` ist `relay_domains`. Sie führt die Domains auf, für die der Rechner E-Mails annimmt, selbst wenn der Sender nicht in der Liste `mynetworks` auftaucht. Ein Beispiel dafür sehen Sie im Folgenden:

```
relay_domains = mycorp.com, mail.mycorp.com, mysiblingcorp.com
```

Der Standardwert für `relay_domains` ist von einem anderen Konfigurationsparameter abgeleitet, `mydestination`, dessen Standardwert wiederum gewöhnlich der Hostname ist. Dies stellt eine sichere Standardeinstellung dar.

Nach einer Änderung der Postfix-Konfiguration sollten die Postfix-Daemons mit dem Parameter `reload` des Kommandos `postfix` angewiesen werden, ihre Konfiguration neu zu laden:

```
# postfix reload
```

Sie sollten jedes Mal, wenn die Postfix-Konfiguration geändert und neu geladen wird, eine Überprüfung auf offene Relays vornehmen.

3.3.3 Exim

Exim ist ein schlanker und moderner MTA, der auf SMail basiert. In seiner Betriebsweise unterscheidet er sich von dem modularen Ansatz von Postfix oder `qmail`.

Standardmäßig führt Exim keine Weiterleitung durch, wobei es jedoch in der Konfigurationsdatei einige Einstellungen gibt, die zur unbeabsichtigten Schaffung eines offenen Relays führen können. Diese Einstellungen finden sich in der Hauptkonfigurationsdatei von Exim, `/etc/exim/exim.conf`.

Exim-Konfigurationsparameter

In der Datei `exim.conf` listet der Konfigurationsparameter `local_domains` die Domains auf, die von der lokalen Instanz von Exim bedient werden. Dabei sollte es sich um eine Liste gültiger und vertrauenswürdiger Domains handeln:

```
domainlist local_domains = mycorp.com : myothercorp.com : *.virtualcorp.com
```

In diesem Beispiel sind zwei Domains aufgeführt und ein Jokerzeichen für eine dritte Domain enthalten. Jede E-Mail für einen Benutzer mit einer E-Mail-Adresse, die `*.virtualcorp.com` entspricht, wird akzeptiert. Jokerzeichen sollten mit Vorsicht eingesetzt werden, da sie zu einer umfangreicheren Domainliste führen können, als beabsichtigt war.

Der Parameter `relay_to_domains` führt alle Domains auf, für die eine Weiterleitung durchgeführt wird, obwohl sie nicht lokal bedient werden. Das folgende Beispiel enthält eine einzelne Domain (`mysiblingcorp.com`), für die E-Mails angenommen und weitergeleitet werden:

```
domainlist relay_to_domains = mysiblingcorp.com
```

Wenn E-Mails für andere Domains nicht angenommen werden sollen, verwenden Sie eine leere Liste, z.B. wie folgt:

```
domainlist relay_to_domains =
```

Die Direktive `relay_from_hosts` führt die IP-Adressen auf, die eine Verbindung zu dieser Instanz von Exim aufnehmen und ihre E-Mails an andere Domains weiterleiten lassen können. Dabei sollte es sich nur um Rechner handeln, die auch E-Mails vom betreffenden Computer senden dürfen:

```
hostlist relay_from_hosts = 127.0.0.1 10.0.100.0/24
```

Dieses Beispiel umfasst die Loopback-Schnittstelle (`localhost`) und ein Subnetz, das Verbindung mit dieser Instanz von Exim aufnehmen und seine E-Mails an andere Domains weiterleiten lassen kann.



Achtung

Die Einstellung `0.0.0.0/0` würde allen Rechnern erlauben, Verbindung aufzunehmen und E-Mails weiterzuleiten. Dies ist wahrscheinlich die gefährlichste Einstellung, was offene Relays betrifft.

Bei einer Änderung der Exim-Konfiguration sollte ein HUP-Signal an Exim gesandt werden, um das Einlesen der neuen Einstellungen zu erzwingen:

```
# exiwhat
9999 daemon: -qlh, listening for SMTP
# kill -HUP 9999
```

Beim Kommando `kill` müssen Sie `9999` durch den Wert ersetzen, der von `exiwhat` zurückgegeben wird.

Selbstverständlich sollte bei einer Änderung der Konfiguration eine Überprüfung auf offene Relays durchgeführt werden, nachdem Exim die neuen Einstellungen gelesen hat.

3.3.4 qmail

qmail ist ein moderner SMTP-Server, bei dessen Entwicklung Sicherheit ein wichtiges Ziel war. Er nutzt den modularen Ansatz von Postfix und führt standardmäßig keine Weiterleitung durch. Einige Distributionen können dieses Verhalten aber ändern, so dass es am besten ist, die korrekte Konfiguration einer Installation zu bestätigen.

qmail akzeptiert nur Mail für Domains, die in der Datei `rcpthosts` aufgeführt sind. Die Konfigurationsdateien befinden sich gewöhnlich in `/var/qmail/`, wobei der vollständige Pfad zur Datei `rcpthosts` `/var/qmail/control/rcpthosts` lautet.

Im Folgenden sehen Sie ein Beispiel für eine `rcpthosts`-Datei:

```
mydomain.com
mysiblingcorp.com
```

Nach einer Änderung der Datei `rcpthosts` ist es nicht notwendig, qmail neu zu starten. Die Prozesse werden nur bei einer eingehenden Verbindung ausgeführt, so dass stets die jüngste Version der Konfigurationsdatei gelesen wird. Auch nach einer Änderung der Konfiguration von qmail sollte ein Test auf offene Relays durchgeführt werden.

3.4 Zusammenfassung

E-Mails wurden in einer freien und offenen Umgebung entwickelt, doch Spam hat diese Umgebung dazu gezwungen, weniger Vertrauen und Offenheit zu zeigen. Der Betrieb eines offenen Relays kann dazu führen, dass der betreffende E-Mail-Server auf einer Blacklist erscheint, wodurch gültige E-Mails, die von diesem Server ausgehen, vom Empfänger nicht angenommen werden. Als weitere Folge kann es zu einer Beendigung der Internetdienste durch den ISP kommen.

Eine Überprüfung auf offene Relays ist einfach, wobei es kostenlose Dienste im Internet gibt, die diese Aufgabe durchführen. Alle MTAs lassen sich mit einigen wenigen, einfachen Konfigurationsschritten so einrichten, dass eine offene Weiterleitung unterbunden wird. In diesem Kapitel wurde erklärt, wie Sendmail, Postfix, Exim und qmail konfiguriert werden, damit sie nicht als offene Relays fungieren.