POP3 ÜBER SSL (UNTER REDHAT 7)

Versionen:

Autor: Thomas King (king@t-king.de)
V1.0BETA (13.01.2001)

Copyright:

Danksagung:

- Alexandra Kopf
- Alle die mich mit Informationen versorgt haben

Aktuelle Version:

Die aktuellste Version dieses Dokuments bekommt man unter: http://www.t-king.de/linux/pop3s.html.

Vorab:

Dies ist ein kleine Anleitung die die Konfiguration von POP3 über SSL (unter Redhat 7) beschreibt. Die Linux-Distribution von RedHat ist unter http://www.redhat.com/ erhältlich. Natürlich läßt sich diese Anleitung auch für andere Distributionen anwenden.
Das „normale“ POP3-Protokol ist nicht verschlüsselt und wird somit im Klartext über das Netzwerk verschickt. Durch „mitsniffen“ ist es möglich die kompletten Nachrichten sowie das Loginpasswort abzuhören. Damit dieses Sicherheitsloch geschlossen werden kann, wurde POP3 über SSL entwickelt.
Ich möchte in dieser Anleitung nicht auf die genaue Funktionsweise von SSL, POP3 oder stunnel eingehen. Diese Anleitung soll die Konfiguration erklären und als Gedankenanstoß und Einstieg dienen.
Die meisten Informationen zu dieser Anleitung habe ich von verschiedenen man-pages. Leider konnte ich keine deutsche oder englische Anleitung zu POP3 über SSL oder ähnliches, deshalb habe ich auch diese Anleitung verfasst. Meine Vorgehensweise für die Konfiguration wurde sehr vom „try and error“-Prinzip geprägt. Ich möchte an dieser Stelle auch sehr deutlich darauf hinweisen, das meine Vorgehensweise sicher nicht das Optimum darstellt und das man noch einiges daran verbessern kann. Ich bitte um Verbesserungsvorschläge!
Leider können die meisten aktuellen Mailclients noch nicht mit POP3 über SSL umgehen (Ausnahmen: pine (mit SSL Addon), Kmail, Fetchmail, MS Outlook Express, ...).
Die Konfiguration wird hier anhand von den Programmen xinetd, qpopper, stunnel erklärt. Es ist sicher möglich diese Anleitung auch auf andere Programme (inetd, andere POP3-Server, ...) anzuwenden.

Installation:

Zuerst muss man die einzelnen Programme installieren:

- xinetd ist der standardmäßige Superdaemon von RedHat 7 und sollte bei der Installation von (RedHat-)Linux mitinstalliert worden sein
- stunnel ist ein SSL-Wrapper und ist auf den RedHat 7 CD's enthalten
- qpopper ist ein POP3-Server von Qualcomm (eigene freie Qualcomm-Lizenz) und unter ftp://ftp.qualcomm.com/eudora/servers/unix/popper/ als Quellcode oder auf dem contrib.redhat.com Server als RPM erhältlich.

Auf die direkte Installation der RPM- bzw. der Quellcode-Pakete möchte ich an dieser Stelle nicht eingehen, da dies an anderer Stelle schon oft erklärt wurde.

Konfiguration:

Damit man auf POP3 über SSL zugreifen kann, muss man dem Superdaemon xinetd mitteilen, das er auf Port 995 (standardmäßiger Port für pop3s [=POP3 über SSL]) lauschen soll und bei Anfragen die Programme stunnel und popper starten soll. Dies geschieht indem man eine Datei pop3s im Verzeichnis /etc/xinetd.d/ erstellt. Die Datei muss diesen Inhalt haben:

```
service pop3s
{
        socket_type             = stream
        wait                    = no
        user                    = root
        server                  = /usr/sbin/stunnel
        server_args             = pop3s -l /usr/sbin/popper -- -R -s -t /var/log/pop3s
        log_on_success          += USERID
        log_on_failure          += USERID
        nice                    = 10
}
```

Ich möchte an dieser Stelle nicht den grundlegenden Aufbau von xinetd Konfigurationsdateien erklären, hierfür sei auf die man-page von xinetd.conf und die Homepage www.xinetd.org mit der sehr guten FAQ verwiesen. Deshalb werde ich nur die Einträge server und server_args erklären.
Der Parameter Server beschreibt den Serverprogramm das bei einer Anfrage auf den Port 995 (=pop3s) aufgerufen werden soll. Server_args beschreibt die Argumente, die an das Serverprogramm beim starten übergeben werden. Das Argument pop3s legt den Service Name fest. Mit -l übergibt man das Programm das von stunnel gestartet werden soll. Die doppelten Bindestriche (--) beenden die eigentlichen Stunnel-Parameter und zeigen an, das die folgenden Parameter für das zu startende Programm (hier popper) bestimmt sind. Die Parameter -R -s -t /var/log/pop3s sind qpopper Parameter und sollen hier nicht weiter erläutert werden (auch hier sei auf die man-page von qpopper verwiesen).

Damit man mit SSL verschlüsseln kann benötigt man ein SSL-Certifikat. Dieses kann man mit stunnel und dem Befehl *make stunnel.pem* im Verzeichnis /usr/share/ssl/cert erzeugen. Die genaue Funktionsweise von SSL soll hier auch nicht erklärt werden, statt dessen soll auf entsprechende Internetseiten verwiesen werden (Links hierzu findet man bspw. auf der Homepage von stunnel).

Nachtrag:

Diese Anleitung ist wesentlich durch meine eigenen Erfahrungen und durch mein begrenztes Wissen geprägt. Ich bitte deshalb ausdrücklich um Feedback, Verbesserungsvorschläge, Erweiterungswünsche und was einem sonst so einfällt.
Alle die wesentlich zur Weiterentwicklung dieser Anleitung beitragen werden natürlich namentlich im Abschnitt Danksagung erwähnt.