Mail-Server: Wie funktioniert SMTP-Auth?

Geschichtliches zu SMTP-Auth

Das SMTP-Protokol (Simple Mail Transfer Protocol) ist eines der ältesten Internet-Protokolle und stammt aus einer Zeit, wo niemand an Missbrauch oder ähnliches gedacht hat. Hingegen wurde damals häufiger mit Ausfällen einzelner Rechner auf dem Weg zum Empfänger gerechnet.
Daher ist es vom Ursprung darauf ausgelegt, ähnlich wie TCP/IP-Pakete, von einem Server zum nächsten weiter gereicht zu werden (relaying).

Erst nach einiger Zeit, als das Internet öffentlicher wurde, kamen die ersten Spammer auf. Damals noch weniger mit Medikamenten als mit Links auf Porno-Seiten.
Großen Provider und (Free-)Mail-Diensten wurden gerne dafür ausgenutzt um diese Spam-Mails auf den Weg zu schicken.
Da damals nur eine Authentifizierung zum Mail-Abholen (POP = Post Office Protocol) gab, hat man diese dafür genutzt und eine Pseudo-Authentifizierung gebastelt: SMTP-after-POP.
Hierbei mußte der User sich per POP (also Mail abholen) authentifizieren und konnte dann innerhalb eines bestimmten Zeitrahmens (z.B. 5 Minuten) seine Mails verschicken. Diese Methode war zwar relativ aufwendig, brauchte aber keine Änderungen in den bestehenden Protokollen.

Diese Funktion ist heute noch in vielen Mail-Clients zu finden wenn auch inzwischen etwas versteckt: Der Button "Abholen & Versenden" tut dies genau in dieser Reihenfolge.

Nach einiger Zeit konnten sich die Entscheider (in erster Linie die Internet Society bzw. deren RFC-Gruppe) auf ein neues Protokoll einigen.
Damit es mit dem alten Protokoll keinen Konflikt gibt, hat man sich entschieden eine andere Begrüßungsformel zu benutzten: Statt dem bisherigen freundlichen `HELO` wird dabei die verdrehte Version `EHLO` gesendet. Damit weiß der Mailserver direkt ob es sich um das SMTP- oder das ESMTP-Protokoll handelt.

In der Praxis:

Inzwischen ist jeder Email-Server darauf ausgelegt, keine ihm fremden Emails zu verschicken (non-relay).
Sollte dies bei dem einen oder anderen doch mal sein, ist dies i.d.R. eine Fehlkonfiguration.

Leider war die RFC nicht konsequent genug und hat leider nciht die Authentifizierungsmöglichkeiten festgelegt.
So kam es, daß die beiden großen Email-Clients (damals Outlook von Microsoft und die Netscape-Suite) verschiedene Methoden implementiert haben: Netscape trieb `PLAIN` voran und Microsoft das `LOGIN`-Verfahren.

Beide Methoden waren unsicher, da das Passwort letztendlich unverschlüsselt über die Leitung geschickt wird.
Später wurde noch die `CRAM-MD5` entwickelt und alle modernen Email-Programme können diese Authentifizierung.

Mail-Server: Wie funktioniert SMTP-Auth?

Dennoch empfiehlt sich immer die Verbindung sowohl beim Mail-Abholen (POP3 oder IMAP) als auch beim Versand eine Verschlüsselte Verbindung zu nutzen. Am einfachsten mit TLS.

Links:

- huschi.net: Eine typische SMTP-Sitzung
- huschi.net: ESMTP-Dialog (SMTP-Auth)
- Wikipedia: SMTP-after-POP
- Wikipedia: SMTP-Auth
- RFC 2554 - SMTP Service Extension for Authentication
- huschi.net: Habe ich ein Open-Relay?
- huschi.net: Über meinen Server werden Spam's verschickt!

Eindeutige ID: #1310
huschi
2008-07-09 10:40