Mail-Server: SPF: Sender Policy Framework

Problem:

Häufig erhält man Bounce-Emails von Mails, die man gar nicht selbst verschickt hat.

Erklärung:

Das SMTP-Protokoll ist leider gar nicht darauf ausgelegt, den Absender zu prüfen.

(Es hat ja schon lange genug gedauert überhaupt den Empfänger zu prüfen und den Versand nur über Authentifizierung zu zu lassen.)

Daher kann man (fast) beliebig Emails mit fremden Absender verschicken. Man braucht lediglich einen SMTP-Server, der diese Emails erstmal an nimmt.
(Z.B. der eigene Server auf dem man sich dank SMTP-Auth anmeldet.)
Und schon sind die Email's mit falschen Absender auf dem Weg.

Lösung:

Neben vielen anderen Lösungen, die darauf basieren, daß jeder Absender erstmal sich irgendwo registrieren muß, gibt es aber auch eine DNS-Basierte Lösung:

Sender Policy Framework (kurz SPF)

Diese Technik wird bereits von AOL, GMX und Yahoo unterstützt und sollte auch weitere Verbreitung finden.

Die Basis ist einfach ein weiterer Eintrag im Nameserver.
Es handelt sich um einen einfachen TXT-Record (TXT=Text), der vom empfangenen SMTP-Server abgerufen wird.
Innerhalb des TXT steht dann der SPF, der aussagt, von welchen Servern die Emails dieser Domain verschickt werden dürfen.
Gehört der einliefernde Server dazu, wird die Email angenommen. Wenn nicht, wird sie abgewiesen. (Vgl. Reverse-DNS)

Hier erstmal: DON'T PANIK!

Domains ohne SPF-Record werden grundsätzlich angenommen!

Wie sieht der SPF-Eintrag aus?

Fangen wir mit einem Beispiel an (gmx.de):

```
v=spf1 ip4:213.165.64.0/23 -all
```

- `v=spf1` SPF-Version
- `ip4:213.165.64.0/23` alle IP's im Bereich 213.165.64.1 bis 213.165.65.254 dürfen Emails mit `@gmx.de` verschicken.
- `-all` für alle anderen IP's gilt dies nicht.

Es gibt noch einige andere Möglichkeiten, wie man die IP's definiert und andere ausschließt. Aber das würde hier zu weit führen.

Wir haben hier ein schönes Beispiel, welches für die meisten bereits genau das darstellt, was gebraucht wird.
Man braucht lediglich einen solchen TXT-Record anlegen (geht leider nicht bei jedem Domain-Provider) und schon sollten Yahoo, AOL und GMX keine gefakten Emails mehr mit Eurem Absender annehmen.

Wie prüfe ich SPF in meinem Mailserver?

Da dies eine Server-Admin-FAQ ist, besteht natürlich auch diese Frage. Leider ist sie zu ausführlich um darauf zu antworten. Daher überlasse ich anderen das Wort:

OpenSPF: Impelemtations (engl.)

Weitere Info's:

- OpenSPF & SPF Protocol Specification
- Bei Wikipedia.de.
- GMX: Informationen für Administratoren anderer Mailserver
- AOL: SPF Information
- Kritisch: Mailabsenderverifikation bringt nichts

Eindeutige ID: #1160
huschi
2011-09-18 21:16