

SPF - Stopp dem Absenderspoofing?

Beigesteuert von Sven Michels

SPF - eine Einfuehrung in Kuerze

SPF - Stopp dem Absenderspoofing? E-Mail ist ein Thema voller Spam. Darum gibt es mittlerweile viele Mittel Spam zu bekämpfen. Zu den verbreitetsten Mitteln gegen Absenderspoofing zählt neben Microsofts Sender-ID[2] und Yahoos Domain-Keys[3] wohl SPF[1]. SPF steht für Sender Policy Framework (früher bekannt als Sender Permitted From) und soll, wie die anderen Techniken, sog. Spoofing von Absenderadressen verhindern.

- Wie funktioniert SPF?

SPF ermöglicht jedem Domainbesitzer das Festlegen von Mailservern die für seine Domain zuständig sind. Aehnlich wie beim MX-Record werden alle Server angegeben, die für das versenden von Mails für diese Domain zuständig sind (hier besteht der Unterschied zum MX-Record, dieser gibt an welche Server für den Empfang von Mails dieser Domain zuständig sind). SPF Einträge werden momentan durch TXT-Records realisiert. Ein SPF-Record sieht z.B.

folgendermassen aus:

Beispiel gmx.de: "v=spf1 ip4:213.165.64.0/23 -all"

Dieser Record sagt in dem Fall aus, das Mails von gmx.de ausschliesslich über Mailserver innerhalb des IP-Bereich 213.165.64.0/23 verschickt werden dürfen. Der "-all" Switch am Ende ist hierbei das "ausschliesslich". Alternativ kann auch "~all" gesetzt werden, wenn man zwar alle Absenderserver eingetragen hat, aber nicht möchte, das Mails aufgrund von SPF von anderen Abgelehnt werden. Setzt man den "?all"-Switch, ist SPF neutral zu behandeln.

- Wie kann ich SPF-Records verwenden?

Zunächst gibt es 2 Möglichkeiten wie man SPF Nutzen kann:

Als Mailserver Administrator können Sie SPF-Checks verwenden um Mails offensichtlich gefälschten Absendern zu filtern. Hierbei sind Sie jedoch darauf angewiesen, das die Absenderdomains SPF-Records enthält. Für die gängigsten MTAs gibt es Patches oder Plugins die SPF-Checks ermöglichen.

Als Domainbesitzer müssen Sie lediglich einen TXT-Record in Ihrem DNS-Server hinterlegen. Was genau der SPF-Record enthalten muss, kann der SPF-Record Generator auf OpenSPF einem sagen. Dort muss man lediglich ein paar einfache Fragen beantworten und am Ende enthält man den entsprechenden SPF-Record sowie eine entsprechende Anleitung für den jeweiligen DNS Server.

- Was bringt mir SPF?

SPF bringt noch nicht viel. Die Verbreitung von SPF ist viel zu gering um wirklich wirkungsvoll zu sein. Das Publizieren von SPF-Records bringt wenig wenn der Server auf dem eine Mail eingeliefert wird nicht auch entsprechend auf SPF-Records prüft. Im Umkehrschluss bringt es wenig SPF am Mailserver zu prüfen wenn nicht jeder auch SPF-Records publiziert. Einige grosse E-Mail Provider wie z.B. GMX haben SPF bereits implementiert. Auch AOL publiziert SPF-Records und checkt solche auf den eingehenden Mailservern.

- Ist SPF sicher?

Auch hier gilt wie immer "nichts ist wirklich sicher". Vorallem muss bei SPF beachtet werden, das z.B. das einfache E-Mail-Weiterleiten (oder sog. "Bouncen") nicht mehr möglich ist. E-Mail Weiterleitungen wie sie jeder Mailserver, z.B. in Form von Aliasen, anbietet, leiten eine Mail unverändert weiter. Hat der Absender jetzt SPF-Records und der "echte" Empfänger auf seinem Mailserver SPF Checks aktiviert, würde die Mail abgelehnt werden, da die Mail des Absenders nicht mehr über seinen Server beim Empfänger eingeliefert wird, sondern über den der die Weiterleitung vornimmt. Um das Weiterleitungs-Problem zu umgehen, hat man einfach einen weiteren "Flicken" erfunden: SRS. Hierbei soll der weiterleitende Mailserver dann entsprechend den Absender umschreiben. Ausserdem sind mittlerweile auch Spammer schon dahinter gekommen das SPF-Records durchaus "positiv" bewertet werden.

- Fazit

Als Fazit kann man sagen, das SPF ein netter Versuch gegen Absenderspoofing ist. Leider ist aber auch SPF nur eine Art Flicker auf dem eigentlichen Problem: SMTP. Das SMTP Protokoll selbst bietet keinerlei echte Verifizierung und solche Aufbauten wie SPF versuchen diese nun Nachträglich zu fixen. Dabei kann jedoch nicht auf alles Rücksicht genommen werden, wie z.B. Weiterleitungen. Durchaus verwendbar ist SPF zum Scoren von Mails. Eine Mail die SPF "verifiziert" ist, ist durchaus etwas vertrauenswürdiger als z.B. eine Mail die trotz SPF-Record über einen anderen Server eingeliefert wurden (aber auch hier gilt: achtung bei Weiterleitungen!).

Links zum Artikel:

- SPF Webseite
- Microsoft Sender-ID
- Yahoo DomainKeys
- Angepasste Version des SPF Policyd zum Taggen von Mails

© Sven ‚Darkman' Michels, sectoor GmbH 2006