von Bruno Sousa
<bruno/at/linuxfocus.org>

Über den Autor:

Bruno studiert in Portugal. Seine Freizeit widmet er Linux und der Photographie.

Eine Einführung in SPF

Zusammenfassung:

SPF steht für *Sender Policy Framework* [Rahmenwerk für Absender−Richtlinien], und es soll ein Standard gegen die Fälschung von e−mail−Absenderadressen sein. Dieser Artikel bietet eine kurze Einführung in SPF und seine Vor− und Nachteile.

Übersetzt ins Deutsche von:
Viktor Horvath
<ViktorHorvath(at)gmx.net>

SPF entstand im Jahre 2003; sein Erfinder Meng Weng Wong griff die besten Features von Reverse MX und DMP *(Designated Mailer Protocol)* auf.

SPF benutzt das Feld Return−Path (oder MAIL FROM) aus dem e−mail−Kopf, denn alle MTAs [*Mail Transfer Agents*, also Mailserver wie z.B. *sendmail*, A.d.Ü.] arbeiten damit. Es gibt auch eine neue Idee von Microsoft, *Purported Responsible Address* (PRA) [zu deutsch etwa: vorgegebene verantwortliche Adresse]. PRA bezieht sich auf die Adresse des Nutzers, die ein MUA [*Mail User Agent*, also ein e−mail−Programm, A.d.Ü.] wie Thunderbird benutzt.

Wenn wir nun SPF und PRA kombinieren, können wir eine Sender−ID erhalten, die dem Empfänger die Prüfung des MAIL FROM−Felds (SPF−Check) und der PRA ermöglicht. Wahrscheinlich werden die MTAs das MAIL FROM−Feld prüfen und die MUAs die PRA.

SPF braucht zur korrekten Arbeit DNS. Das bedeutet, daß die „reverse MX“−Daten veröffentlicht werden müssen, die angeben, welche Rechner e−mails der Domäne *versenden*. Das ist etwas anderes als die heute benutzten MX−Daten, die angeben, welche Rechner e−mails der Domäne *empfangen*.

Was benötigt SPF?

Um dein System mit SPF zu schützen, mußt du:

1. deinem DNS−Eintrag den TXT−Record hinzufügen; dort befindet sich die Information, die SPF abfragt.

2. dein e−mail−System (qmail, sendmail) für SPF konfigurieren, d.h. so, daß es für jede auf deinem Server eingehende Nachricht die Prüfung durchführt.

Der erste Schritt wird auf dem DNS−Server der jeweiligen Domäne durchgeführt. Im nächsten Abschnitt besprechen wir die Details eines solchen Records. Du mußt die Syntax kennen, die dein DNS−Server benutzt (bind oder djbdns). Aber keine Sorge, auf der offizielle SPF−Webseite gibt es einen exzellenten Wizard, der dir helfen wird.

Der TXT−Record von SPF

Die SPF−Daten sind in einem TXT−Record enthalten, und zwar in folgendem Format:

```
v=spf1 [[pre] type [ext] ] ... [mod]
```

Die Bedeutung jedes Parameters ist wie folgt:

<table>
<tr><th>Parameter</th><th>BeschreibungDescription</th></tr>
<tr><td>v=spf1</td><td>Version von SPF. Beim Sender−ID−Verfahren könntest du auf „v=spf2“ stoßen.</td></tr>
<tr><td>pre</td><td>Definiert einen Rückgabewert, wenn eine Übereinstimmung gefunden wird.

Die möglichen Werte sind:
Wert — Beschreibung
+ — Standard: Erfolg, wenn ein Test beweiskräftig ist.
− — Test fehlgeschlagen. Dieser Wert wird normalerweise für „−all“ benutzt, um zu sagen, daß es keine früheren Treffer gibt.
~ — „Sanfter“ Fehlschlag. Dieser Wert wird normalerweise benutzt, wenn ein Test nicht beweiskräftig ist.
? — Neutral. Dieser Wert wird normalerweise benutzt, wenn ein Test nicht beweiskräftig ist.</td></tr>
<tr><td>type</td><td>Bestimmt den Typ, der für die Verifikation benutzt werden soll.

Die möglichen Werte sind:
Wert — Beschreibung
include — um die Tests einer angegebenen Domäne miteinzubeziehen. Schreibweise: „include:domain“
all — um die Testsequenz zu beenden. Bei „−all“ wird erfolglos abgebrochen, wenn nicht alle Tests bis hierhin erfüllt sind. Wenn man sich nicht sicher ist, kann man die Form „?all“ benutzen, was bedeutet, daß der Test mit Erfolg beendet wird.
ip4 — Benutze IPv4 zur Verifikation. Das kann in den Formen „ip4:ipv4“ oder „ip4:ipv4/cidr“ geschrieben werden, um einen Bereich anzugeben. Dieser Typ wird sehr</td></tr>
</table>

<table>
<tr><td></td><td><table>
<tr><td></td><td>empfohlen, denn er verursacht die geringste Last auf den DNS−Servern.</td></tr>
<tr><td>ip6</td><td>Benutze IPv6 zur Verifikation.</td></tr>
<tr><td>a</td><td>Benutze einen Domänennamen zur Verifikation.
Ein DNS−Lookup wird für ein „A RR“ durchgeführt.
Er kann „a:domain“, „a:domain/cidr“ oder „a/cidr“ geschrieben werden.</td></tr>
<tr><td>mx</td><td>Benutze den DNS MX RR−Eintrag zur Verifikation.
Der MX RR−Eintrag legt den empfangenden MTA fest; ist er z.B. nicht derselbe wie der sendende MTA, werden die auf MX basierenden Tests fehlschlagen.
Er kann „mx:domain“, „mx:domain/cidr“ oder „mx/cidr“ geschrieben werden.</td></tr>
<tr><td>ptr</td><td>Benutze den DNS PTR RR−Eintrag zur Verifikation.
In diesem Fall wird ein PTR RR−Eintrag und eine Reverse−Map−Anfrage benutzt. Wenn der erfragte Hostname in derselben Domäne liegt, ist die Kommunikation verifiziert.
Er wird „ptr:domain“ geschrieben.</td></tr>
<tr><td>exist</td><td>Test für die Existenz einer Domäne.
Er wird „exist:domain“ geschrieben.</td></tr>
</table></td></tr>
<tr><td>ext</td><td>Bestimmt eine optionale Erweiterung des Typs. Wird es weggelassen, wird nur ein einzelner Record−Typ für die Abfrage benutzt.</td></tr>
<tr><td>mod</td><td>Die letzte Typ−Direktive; dient als Record−Modifier.

<table>
<tr><td>Modifier</td><td>Beschreibung</td></tr>
<tr><td>redirect</td><td>Leitet die Verifikation weiter, so daß die SPF−Einträge der angegebenen Domäne benutzt werden.
Schreibweise: „redirect=domain“.</td></tr>
<tr><td>exp</td><td>Dieser Eintrag muß der letzte sein; er ermöglicht eine individuelle Fehlermeldung.

<pre>IN TXT "v=spf1 mx -all exp=getlost.example.com"

getlost IN TXT "Sie sind nicht autorisiert, e-mail für diese Domäne zu versende
+++n."</pre></td></tr>
</table></td></tr>
</table>

Hey, ich bin ein ISP

ISPs werden etwas „Ärger“ mit ihren wechselnden Nutzern haben, wenn sie Mechanismen wie SMTP−nach−POP statt SASL SMTP benutzen.

Nun ja, wenn du ein ISP bist und dich um Spam und Adreßfälschungen sorgst, mußt du deine e−mail−Politik

überdenken und mit SPF anfangen.

Hier sind einige Punkte, denen du folgen könntest.

1. Zuerst konfiguriere deinen MTA für die Benutzung von SASL, z.B. kannst du ihn auf die Ports 25 und 587 legen.
2. Warne deine Nutzer über die Politik, die du gerade verfolgst (spf.pobox.com zeigt ein Beispiel, siehe Verweise).
3. Gib deinen Nutzern eine Toleranzfrist, d.h. du veröffentlichst zwar deine SPF−Daten im DNS, aber mit sanft fehlschlagenden Tests (~all) statt gewöhnlichen (−all).

Damit schützt du deine Server, deine Kunden und die restliche Welt vor Spam...

Es gibt viele Informationen für dich auf der offiziellen SPF−Webseite, worauf wartest du?

Worauf muß man aufpassen?

SPF ist eine perfekte Lösung, sich gegen Adreßbetrug zu schützen. Es hat jedoch eine Beschränkung: Herkömmliche e−mail−Weiterleitung funktioniert nicht länger. Dein MTA kann nicht einfach e−mails empfangen und weitersenden. Du mußt die Sender−Adresse neu schreiben. Patches für die geläufigen MTAs werden auf der SPF−Seite bereitgestellt. In anderen Worten, wenn du SPF−DNS−Einträge veröffentlichst, solltest du auch deinen MTA für das Neuschreiben der Sender−Adressen aktualisieren, sogar wenn du noch keine SPF−Einträge überprüfst.

Schlußfolgerungen

Du glaubst vielleicht, daß die Implementation von SPF etwas verwirrend ist. Tatsächlich ist es nicht kompliziert, und im übrigen hast du einen großartigen Wizard, der dir bei der Bewältigung deiner Mission hilft (siehe Verweise).

Wenn du dir Sorgen über Spam machst, hilft dir SPF, indem es deine Domäne vor Fälschungen schützt, und alles, was du dazu tun mußt, ist, eine Textzeile auf deinem DNS−Server zu ändern und deinen Mailserver zu konfigurieren.

Die Vorteile von SPF sind groß. Jedoch, wie ich einmal jemandem gesagt habe, ist es kein Unterschied wie Tag und Nacht. Der Nutzen von SPF kommt mit der Zeit, wenn es andere auch einsetzen.

Ich habe die Sender−ID und ihren Bezug zu SPF erwähnt, aber keine näheren Erklärungen gegeben. Wahrscheinlich kennst du bereits den Grund dafür; die Politik von Microsoft ist immer dieselbe: Softwarepatente. Bei den Verweisen kannst du die Position von openspf.org zur Sender−ID lesen.

In einem folgenden Artikel werden wir über die Konfiguration des MTA sprechen, bis dann!

Ich wollte dir eine kurze Einführung zu SPF bieten. Wenn du mehr darüber erfahren willst, folge einfach den Referenzen, mit deren Hilfe dieser Artikel geschrieben wurde.

Referenzen [engl.]

Die offizielle SPF−Webseite
Die offizielle FAQ von SPF
Der offizielle SPF−Wizard
Die Position von openspf.org bezüglich der Sender−ID
Ein exzellenter Artikel über Sender−ID und SPF
Warne deine Nutzer über die SASL−Umstellung
HOWTO − Wie man einen SPF−Record schreibt

2005−01−12, generated by lfparser_pdf version 2.51