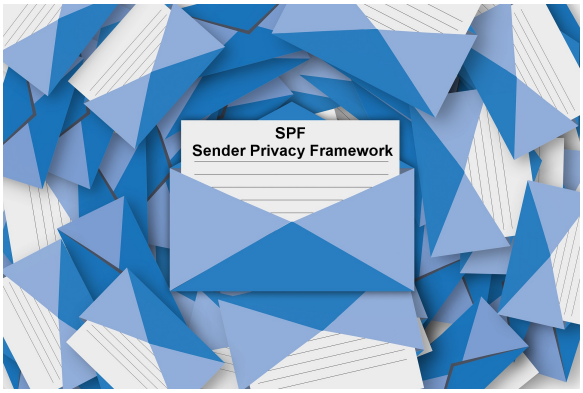
SPF



SPF ("Sender Policy Framework")

soll verhindern, dass ein Versender (z.B. ein Spammer) unberechtigt E-Mails im Namen eines seriösen Unternehmens verschickt (sog. "Phishing-Mails").

Das Prinzip ist simpel: Bei der Versand-Domain des Absenders werden alle Mail-Server eingetragen, die in dessen Namen Mails verschicken dürfen; beim Eintreffen eines Mails wird dann vom empfangenden Mail-Server überprüft, ob der versendende Server überhaupt berechtigt war, das Mail zu verschicken.

Der empfangende Mailserver hat über den SPF-Record der Domain die Möglichkeit zu prüfen, ob die erhaltene E-Mail von einem authorisierten Mailserver stammt, oder von einem nicht authorisierten Server. Im letzten Fall kann die Email über den SPF Spamschutz identifiziert und als SPAM deklariert werden.

SPF erstellen und prüfen

Um einen SPF Eintrag zu erstellen, können Sie als Beispiel einen der vielen Generatoren verwenden, die Online zur Verfügung stehen. Zum Überprüfen kann man auch auf diverse Web-Tools zurückgreifen, wie beispielsweise: MX Toolbox

Info

Der SPF Record lässt sich auch auf der Kommandozeile mit dem Befehl `host` oder `dig` abfragen. Beispiel:

```
$ host -t TXT domain.at
domain.at descriptive text "v=spf1 a mx ip4:xxx.xxx.xxx.xxx/xx ip4:
xxx.xxx.xxx.xxx/xx [...] -all"
```

Der Aufbau eines SPF-Records:

Jeder SPF Record startet mit der Versionsnummer, aktuell also "**v=spf1**". Folgend können beliebig viele Ausdrücke angegeben werden, die von vorne nach hinten bearbeitet werden. Viele dieser Ausdrücke sind Direktiven, die für die Autorisierung des Versendens zuständig sind. Diese bestehen aus einem Qualifikator und einem Mechanismus, der auswertet, ob es für eine IP Adresse einen Treffer oder keinen gibt. Der erste Mechanismus, der einen Treffer liefert, ist für das Ergebnis der gesamten Auswertung des SPF-Records bestimmend.

Diese Tabelle zeigt Qualifikatoren:

Q.	Ergebnis-Code	Beschreibung
+	Pass	die Direktive definiert autorisierte Sender; dies ist der Standard, d. h. ist kein Qualifikator angegeben, so wird + angenommen
-	Fail	die Direktive definiert nicht autorisierte Sender
~	SoftFail	die Direktive definiert nicht autorisierte Sender, der Empfänger soll diesen Fehlschlag aber großzügig behandeln.
?	Neutral	die Direktive definiert Sender, über deren Legitimität nichts ausgesagt werden soll; Der Sender muss akzeptiert werden.

Einige Mechanismen:

Mechanismus	Direktive trifft zu, wenn...
all	immer
a	… ein A-(oder AAAA-)Record der befragten (oder explizit angegebenen) Domäne die IP-Adresse des Senders enthält
mx	… ein MX-Record der befragten (oder explizit angegebenen) Domäne die IP-Adresse des Senders enthält
ip4	… die angegebene IPv4-Adresse die IP-Adresse des Senders ist bzw. das angegebene IPv4-Subnetz diese enthält
ip6	… die angegebene IPv6-Adresse die IP-Adresse des Senders ist bzw. das angegebene IPv6-Subnetz diese enthält
include	… eine zusätzliche SPF-Anfrage zur im Include-Statement angegebenen Domain die IP-Adresse des Senders enthält

Viele weitere Informationen findet man auf der offiziellen Webseite des SPF-Projektes: http://www.openspf.org/Project_Overview