tronet Servicecenter

Hornetsecurity Sender Policy Framework (SPF)-Filter

Maik Oblong - 2017-09-12 - Kommentare (0) - Spam- und Virenfilter

Das *Sender Policy Framework* (SPF) ist ein Verfahren, das das Fälschen der Absenderadresse einer E-Mail verhindern soll. Der Administrator einer Domain hinterlegt in der DNS-Zone einen *Resource Record* vom Typ TXT. In diesen *Resource Records* sind die IP-Adressen oder der Hostname der Server hinterlegt, die E-Mails versenden dürfen. Der Empfänger der E-Mail prüft dann den *Resource Record* gegen die Informationen, die im E-Mail Header vorhanden sind und lehnt die E-Mail ab, sollten die Informationen nicht übereinstimmen.

Wir empfehlen grundsätzlich die Verwendung eines SPF-Filters. Sollten Sie den SPF-Filter für Ihre Domain aktivieren wollen, setzen Sie sich bitte mit unserem Kundensupport in Verbindung. Bevor Sie den Kundensupport kontaktieren, müssen Sie die folgenden Entscheidungen treffen:

1. Variante

Der SPF-Filter kann in zwei verschiedenen Varianten verwendet werden:

- *Variante 1*: Hier wird die Prüfung nur verwendet, wenn eine E-Mail von einer internen Domain empfangen wird. Hier wird dann der TXT-Record der eigenen Domain geprüft.
- *Variante 2*: Hier wird die Prüfung bei allen eingehenden E-Mails angewandt. Hier wird der TXT-Record der sendenden Domain abgerufen und die Informationen im Header gegengeprüft.

Welche Variante Sie einsetzen, ist Ihnen überlassen. Bei der *Variante 2* kann es ggf. zu *erhöhten False Positives* (korrekte E-Mails werden ungerechtfertigterweise aussortiert)

kommen, falls der TXT-Record Fehler aufweist (z.B. eine IP-Adresse inkorrekt ist oder fehlt). Wir empfehlen, mit *Variante 1* zu starten und bei Bedarf auf *Variante 2* zu wechseln.

2. Hard- oder Softfail

Der TXT-Record wird unterscheiden müssen zwischen einem Hard- oder Softfail bei der Prüfung des TXT-Records. Diese Prüfung greift, sollte der TXT-Record nicht mit den Header-Informationen übereinstimmen. Dieser wird gekennzeichnet durch:

- Hardfail = *-all*: E-Mails werden bei Nichtübereinstimmung direkt abgewiesen.
- Softfail = *~all*: E-Mails laufen bei Nichtübereinstimmung in die Quarantäne.

Wir empfehlen einen Softfail, um bei False Positives entsprechend reagieren zu können.