Sichere E-Mail

Was Sie über SPF wissen sollten

eco Guide zum Sender Policy Framework

SPF – Sender Policy Framework

SPF (Sender Policy Framework)

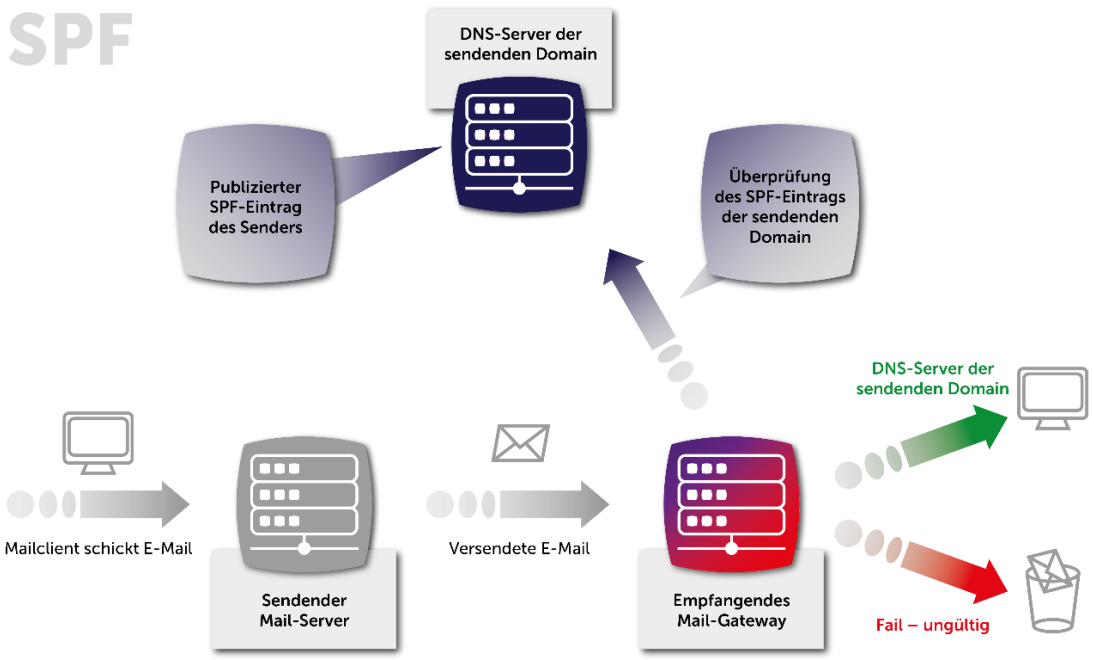
ist ein Sender-Legitimierungsverfahren. Es hilft dabei Mailsysteme zu identifizieren, welche im Namen einer bestimmten Domain E-Mails versenden dürfen und erklärt zusätzlich wie mit jenen Mailsystemen verfahren werden soll, welche nicht zum Senden im Namen der betroffenen Domain legitimiert sind. Empfangende Mailsysteme können so erkennen, welches System im Namen einer Domain senden darf und welches nicht. SPF verhindert auf diese Weise, dass Angreifer, mit Hilfe nicht legitimierter Systeme, in betrügerischer Absicht E-Mails mit gefälschten Absenderadressen (Spoofing) versenden.

Entstehung

Die erste Version von SPF wurde ursprünglich von Meng Weng Wong und Wayne Schlitt entwickelt und im April 2004 als experimentelle RFC 4406 vorgeschlagen. Die offizielle Standardisierung erfolgte durch die RFC 4408 (2006), welche später durch RFC 7208 (2014) aktualisiert wurde.

Wie funktioniert SPF?

Die Besitzer einer für E-Mail genutzten Domain veröffentlichen eine (1) SPF-Richtlinie (SPF-Record) als TXT-Eintrag im DNS. Diese Richtlinie listet von links nach rechts IP-Adressen oder DNS Record Typen (A, MX) auf, welche berechtigt sind, E-Mails im Namen der Domain zu versenden. Die letzte Angabe in dieser Liste gibt vor, wie mit allen



anderen (nicht legitimierten) Systemen verfahren werden soll. Ein empfangende Mailserver überprüft diesen SPF-Record, indem er die IP-Adresse des sendenden Mailservers mit der veröffentlichten Liste abgleicht.

Limitationen von SPF

Abwesenheit einer Policy (Richtlinie)

SPF kann nur Systeme legitimieren. Es verfügt nur über rudimentäre Möglichkeiten (Ja / Nein-Entscheidung), einem empfangenden System mitzuteilen was (policy) mit einer Nachricht geschehen soll, welche von einem nicht-legitimierten System aus gesendet wird. Es wird heute in Kombination mit dem DMARC-Mechanismus eingesetzt, welches differenziertere Policy-Aussagen treffen kann und zudem mit seiner Fähigkeit Berichte anzufordern Rückschluss auf mögliche Missbrauchsversuche zulässt.

Auftragsverarbeitung, E-Mail-Weiterleitung und Mailinglisten

Das Hauptproblem von SPF liegt in der Annahme (Theorie) die Liste der legitimierten Systeme sei statisch, d. h. es wären immer nur dieselben, wenigen Systeme, welche E-Mail im Namen einer bestimmten Senderdomain in Umlauf brächten. Im Alltag (Praxis) zeigt sich, es existieren viele Situationen in denen durch SPF nicht legitimiere Systeme durchaus berechtigt wären im Namen einer Domain zu senden, aber sie befinden sich nicht auf der Liste legitimierter Systeme. Die Konsequenz ist, Nachrichten von diesen Systemen werden abgewiesen oder so schlecht gestellt, dass diese z. B. automatisch vorsortiert im Spam-Ordner landen und so übersehen werden. Typische Beispiele dafür sind die Behandlung von E-Mail-Weiterleitung, das Versenden von Nachrichten durch Dienstleister (Buchhaltung, Rechnungswesen, E-Mail-Marketing) und Mailinglisten.

Best Practices

DNS-Lookup-Limit beachten

Das DNS-System gestattet nur eine eingeschränkte Anzahl an Zeichen (255 Zeichen) in einer DNS-Antwort. Domains, welche viele Systeme legitimieren müssen, gelangen beim Erstellen der Liste zu legitimierender Syteme schnell an die durch das DNS gesetzten Zeichengrenzen. SPF bietet zur Lösung dieses Problems, mit Hilfe der sogenannten include-Anweisung in einem SPF-Record, die Möglichkeit weitere DNS-Einträge in die Antwort an das nachfragende System einzubinden.

Es ist aber nicht möglich eine beliebige Anzahl an includes vorzunehmen, denn jedes include beding einen weitere DNS-Anfrage (DNS-Lookup) und die SPF-Spezifikation beschränkt die die Anzahl weiterer, durch include-Anweisungen hervorgerufenen DNS-Lookups, auf maximal 10. Diese Einschränkung dient dem Schutz der DNS-Server vor Überlastung (Denial-of-Service-Angriff) und sie soll eine hoheVerarbeitungsgeschwindigkeit während der SPF-Validierung gewährleisten.

Wird das DNS-Lookup-Limit überschritten so soll der SPF-Eintrag, laut Spezifikation, vollständig ignoriert werden. Ein Scheitern des Lookups kann zur Ablehnung der E-Mails führen und deshalb ergibt es Sinn, den SPF-Eintrag von Anfang an konsequent auf die Einhaltung des Lookup-Limits zu prüfen und diesen ggf. zu optimieren:

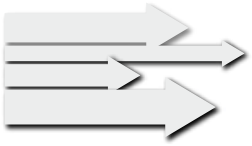
- Vermeiden sie wenn möglich Record-Typen (A, AAAA, MX) anzugeben, weil diese zusätzliche Lookups hervorrufen. Geben sie stattdessen gleich die mit dem Record verbundenen IP-Adresse an.
- Nutzen sie include-Anweisungen nur dann, wenn sie diese nutzen müssen
- Fassen sie einzelne IP-Adressen zu IP-Bereichen (IP-Subnetzen) zusammen, wenn das sinnvoll möglich ist
- Setzen sie parallel auch immer DKIM als Legitimierungsverfahren mit ein, damit ihre sendenden Systeme weiterhin legitimiert sind falls SPF-Lookups scheitern.

Aufbau eines SPF Eintrages

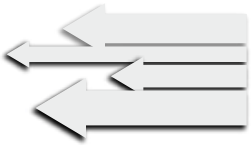
Ein SPF-Eintrag ist ein **TXT-Record**, welcher im APEX, dem kürzesten Teil des Domainnamens, der DNS-Zone einer Senderdomain veröffentlicht wird. Der TXT-Eintrag muss als Erstes immer nennen, um welche Art Eintrag (hier: SPF) es sich handelt und ggf. welche Version der Spezifikation verwendet wird. Im Fall von SPF muss der TXT-Record mit dem Eintrag v=spf1 beginnen. Hier sind die wichtigsten Tags und Modifikatoren, welche in einem SPF-Eintrag verwendet werden:

Tags:

- **ip4** und **ip6**: Gibt spezifische IPv4- oder IPv6-Adressen oder -Adressbereiche an, die senden dürfen.
  Beispiel: ip4:192.168.0.1 oder ip4:192.168.0.0/24
- **a**: Erlaubt alle IP-Adressen, die im A-Record (oder AAAA-Record für IPv6) der Domain stehen.
  Beispiel: a oder a:mail.example.com
- **mx**: Erlaubt alle IP-Adressen der Mailserver, die im MX-Record der Domain angegeben sind.
  Beispiel: mx oder mx:example.com
- **include**: Bindet SPF-Einträge anderer Domains ein (z. B. wenn ein externer Anbieter für das E-Mail-Versenden genutzt wird).
  Beispiel: include:_spf.google.com
- **all**: Dieser Mechanismus muss am Ende eines SPF-Eintrags stehen. Er legt mit Hilfe von Quantifiern fest, was mit nicht berechtigten Servern passieren soll.



SPF – Sender Policy Framework



Quantifier

- **+** (Pass)
  Die E-Mail soll angenommen werden. Diese Angaben ist zulässig, aber sie wird selten explizit angegeben, da sie bereits implizit der Standardwert ist und immer dann Anwendung findet, wenn keiner der nachfolgenden Quantifier angegeben wird.
- **-** (Fail)
  Die E-Mail soll abgelehnt werden, wenn der Absender-Server nicht autorisiert ist.
- **~** (SoftFail)
  Die E-Mail soll akzeptiert, aber als potenziell unsicher markiert werden.
- **?** (Neutral)
  Keine Aussage über die Authentizität der E-Mail.

```
DOMAIN.TLD TXT "v=spf1 ip4=192.0.2.0 ip4=192.1.2.0/24
ip6=fe80::0202:b3ff:fe1e:8329/64 include:sub.example.com -all"
```

Beispiele eines SPF-Eintrags

v=spf1: SPF-Version 1.

ip4:192.168.0.1: Nur der Server mit dieser IP-Adresse darf E-Mails senden.

include:_spf.google.com: Externe Server von Google (z. B. Google Workspace) sind ebenfalls berechtigt. Durch das Einbinden des Google SPF-Eintrags autorisieren Sie effektiv alle Google-Mailserver, E-Mails in Ihrem Namen zu versenden. Wenn Sie nur bestimmte Google-Dienste nutzen, ist dies möglicherweise zu umfassend.

-all: Alle anderen Server sind nicht autorisiert und E-Mails von ihnen sollen abgelehnt werden.

Beispiel für SPF mit verschiedenen Qualifizierern

```
v=spf1 +ip4:192.0.1.5 -ip4:198.51.100.10 ~include:_spf.extern.com ?a -all
```

+ip4:192.0.1.5: Die IP-Adresse 192.0.1.5 ist autorisiert, E-Mails für die Domain zu senden **(Standardqualifizierer + für Pass)**.

-ip4:198.51.100.10: E-Mails von der IP-Adresse 198.51.100.10 sollen abgelehnt werden **(- für Fail).**

~include:_spf.extern.com: E-Mails von Servern, die im SPF-Eintrag **_spf.extern.com** aufgeführt sind, werden akzeptiert, aber als unsicher markiert **(~ für SoftFail).**

?a: Alle IP-Adressen, die als A-Record der Domain hinterlegt sind, werden mit neutraler Bewertung **(? für Neutral)** berücksichtigt.

-all: Alle anderen Server werden abgelehnt, da sie nicht autorisiert sind **(- für Fail)**.

Es gibt auch die Möglichkeit ein Redirect zu machen:

DOMAIN.TLD TXT "v=spf1 redirect:sub.example.com"

Wenn man ein Redirect setzt, sind - abgesehen von "v" - keine weitere Parameter erlaubt. Beispielsweise -all oder ~all sollte in dem Fall auch weggelassen werden! Letzteres ist ein häufig gemachter Fehler.

SPF Version

Für SPF existiert nur eine Version: spf1.
Die Version "spf2.0/*" ist keine SPF Version, sondern SenderID und obsolet. Mehr Information dazu: http://www.open-spf.org/SPF_vs_Sender_ID.

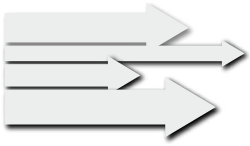
Für weitere Details zur Implementierung verweisen wir auf https://www.rfc-editor.org/rfc/rfc7208.

SPF-Überprüfung beim Empfänger

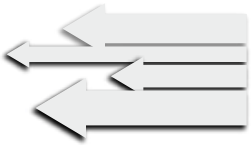
Wenn ein empfangender Mailserver eine E-Mail erhält, überprüft dieser, ob die IP-Adresse des sendenden Mailsystems im SPF-Eintrag der verwendeten Envelope Sender Domain als legitimiertes System gelistet ist. Je nach Ergebnis der Prüfung kann die E-Mail entweder akzeptiert, als verdächtig markiert oder abgelehnt werden und / oder als Kriterium zur Reputationsbemessung hinzugezogen werden.

Leider schlägt SPF in vielen zentralen Anwendungsfällen von E-Mail fehl, beispielsweise bei Weiterleitungen oder der Nutzung von Mailinglisten. Daher wird SPF fast ausschließlich in Kombination mit anderen Authentifizierungsmethoden verwendet.

Weitere Informationen bezüglich des Zusammenspiels von DMARC, DKIM und SPF finden Sie in den Dokumenten der Kompetenzgruppe-E-Mail in unserem Downloadbereich auf https://www.eco.de



SPF – Sender Policy Framework



Kontakt:
Michael Weirich
Projekt Manager IT-Sicherheit
eco – Verband der Internetwirtschaft e. V.

Mobil: +49(0)171 – 554 0303
E-Mail: michael.weirich@eco.de
Web: https://www.eco.de/