# SPF (Sender Policy Framework) – Schutz vor gefälschten E-Mails

## Inhaltsverzeichnis



SPF (Sender Policy Framework) ist ein Sicherheitsmechanismus, der verhindert, dass E-Mails mit gefälschten Absenderadressen versendet werden. Durch einen SPF-Eintrag in den DNS-Records einer Domain können Mailserver überprüfen, ob eine E-Mail von einem autorisierten Server stammt. Dies schützt vor E-Mail-Spoofing und reduziert das Risiko von Phishing-Angriffen. In Kombination mit DKIM und DMARC bildet SPF eine zentrale Sicherheitsmaßnahme zur Authentifizierung von E-Mails.

SPF (Sender Policy Framework) ist ein Sicherheitsmechanismus, der dazu dient, die Authentizität von E-Mails zu überprüfen und E-Mail-Spoofing zu verhindern. Mithilfe von SPF kann ein Domain-Inhaber festlegen, welche Server berechtigt sind, E-Mails im Namen der eigenen Domain zu versenden.

## 1 Funktionsweise von SPF

SPF basiert auf DNS-Einträgen und hilft Mailservern dabei, eingehende E-Mails auf ihre Echtheit zu überprüfen. Die wichtigsten Schritte sind:

1. **SPF-Eintrag in der DNS-Zone hinterlegen**: Der Domain-Inhaber definiert eine SPF-Richtlinie als TXT-Eintrag in den DNS-Einstellungen der Domain.
2. **Mailserver prüft SPF-Informationen**: Beim Empfang einer E-Mail gleicht der empfangende Mailserver die IP-Adresse des sendenden Servers mit den im SPF-Record hinterlegten Informationen ab.
3. **Entscheidung über die Zustellung**: Je nach SPF-Regelung kann die E-Mail zugestellt, markiert oder abgelehnt werden.

## 2 SPF-Eintrag – Aufbau und Beispiel

Ein SPF-Eintrag ist ein DNS-TXT-Record und enthält die IP-Adressen oder Server, die berechtigt sind, E-Mails für eine Domain zu versenden. Beispiel:

Code

```
v=spf1 ip4:192.0.2.1 include:_spf.mailserver.com -all
```

- `v=spf1` ? Gibt an, dass es sich um einen SPF-Eintrag handelt.
- `ip4:192.0.2.1` ? Diese IP-Adresse darf E-Mails für die Domain versenden.
- `include:_spf.mailserver.com` ? Erlaubt die Nutzung eines externen Mailservers.
- `-all` ? Alle anderen Server sind nicht autorisiert (E-Mails werden abgelehnt).

## 3 SPF-Mechanismen

SPF nutzt verschiedene Mechanismen zur Validierung:

- `+all` ? Erlaubt alle Server (nicht empfohlen).
- `-all` ? Blockiert alle nicht explizit aufgeführten Server (empfohlen).
- `~all` ? Weiche Richtlinie, E-Mails werden nicht abgelehnt, sondern markiert.
- `?all` ? Keine eindeutige Aussage über die Erlaubnis oder Ablehnung.

## 4 Grenzen von SPF

Obwohl SPF eine wichtige Schutzmaßnahme ist, hat es auch Einschränkungen:

- **Kein Schutz vor gefälschten Absendernamen im „From“-Feld** (SPF prüft nur den Mail-Envelope-Absender).
- **Weiterleitungen können SPF brechen**, da die ursprüngliche Absender-IP nicht mehr mit der Domain übereinstimmt.
- **Nicht ausreichend als alleinige Sicherheitsmaßnahme** – sollte mit **DKIM** (DomainKeys Identified Mail) und **DMARC** (Domain-based Message Authentication, Reporting & Conformance) kombiniert werden.

## 5 Fazit

SPF ist ein essenzieller Bestandteil der E-Mail-Sicherheit und hilft, Spoofing zu verhindern. Es sollte in jeder Domain mit aktivem E-Mail-Verkehr korrekt konfiguriert werden, um unerlaubte Absender zu blockieren. Zusammen mit DKIM und DMARC bietet SPF eine wirksame Schutzstrategie gegen E-Mail-Betrug und Phishing-Angriffe.

---