Mail: SPF – Sender Policy Framework

Co to jest SPF?

SPF (Sender Policy Framework) to mechanizm uwierzytelniania poczty e-mail, który pomaga chronić domenę przed:

- **spoofingiem** (podszywaniem się pod adresy e-mail),
- **phishingiem**,
- nadużyciem serwerów do wysyłki nieautoryzowanych wiadomości.

SPF pozwala właścicielowi domeny określić, które serwery **mają prawo wysyłać e-maile** w jej imieniu.

Jak działa SPF?

1. Właściciel domeny dodaje specjalny rekord **TXT** do DNS swojej domeny. 2. Gdy serwer odbiorcy (np. Gmail) otrzymuje e-mail:

- sprawdza, z jakiego **adresu IP** wiadomość została wysłana,
- porównuje ten adres z listą serwerów zdefiniowaną w rekordzie SPF domeny nadawcy.

3. Na tej podstawie wiadomość:

- przechodzi test SPF (**pass**),
- lub go nie przechodzi (**fail**, **softfail**, **neutral**, itp.).

Rekord SPF – Gdzie i jak go dodać

Rekord SPF dodaje się jako rekord **TXT** do DNS domeny.

Typ	Nazwa	Wartość (przykład)
TXT	ostrowski.net.pl	`v=spf1 include:mx.ovh.com -all`

* `Nazwa`: to główna domena (bez prefiksu, np. nie `_spf`). * `Wartość`: deklaracja SPF (szczegóły poniżej).

Składnia rekordu SPF

```
v=spf1 [elementy] [mechanizmy końcowe]
```

Najczęstsze elementy SPF

Element	Opis
`ip4:x.x.x.x`	Pozwala na wysyłkę z adresu IPv4
`ip6:xxxx::xxxx`	Pozwala na wysyłkę z adresu IPv6
`include:domena`	Uznaje rekord SPF innej domeny (np. dostawcy usług e-mail)
`a`	Zezwala na serwery wskazane w rekordzie A domeny
`mx`	Zezwala na serwery MX zdefiniowane dla domeny
`exists:`	Zezwolenie w oparciu o istnienie DNS
`all`	Pasuje do wszystkich — używane na końcu jako domyślne zachowanie

Modyfikatory mechanizmów

Symbol	Znaczenie
`+`	Pass (domyślnie — nie trzeba pisać)
`-`	Fail – odrzucić
`~`	SoftFail – zaakceptuj, ale oznacz jako podejrzane
`?`	Neutral – żadnego wyraźnego wyniku

Przykłady Rekordów SPF

1. Prosty rekord tylko dla jednego IP

```
v=spf1 ip4:192.0.2.1 -all
```

Tylko IP `192.0.2.1` może wysyłać maile z tej domeny. Wszystko inne jest odrzucane (`-all`).

2. SPF dla serwerów OVH

```
v=spf1 include:mx.ovh.com -all
```

Zezwala wszystkim serwerom OVH (zdefiniowanym w `mx.ovh.com`) na wysyłanie maili.

3. Kombinacja IP + serwerów mailowych + fallback

```
v=spf1 ip4:203.0.113.0/24 include:_spf.google.com ~all
```

Zezwala:

- adresom IP z zakresu `203.0.113.0/24`
- serwerom Gmaila

Wszystko inne dostaje **softfail** (trafia np. do spamu, ale nie jest odrzucane).

Rekomendacje Bezpieczeństwa

1. **Zawsze kończ rekord SPF mechanizmem `all`**:

- `-all` → wszystko poza listą = odrzuć
- `~all` → wszystko poza listą = oznacz jako podejrzane

2. **Unikaj nadmiaru `include:`** – każde z nich to dodatkowe zapytanie DNS (limit: 10). 3. **Nie używaj SPF bez `all`** – to otwarte zaproszenie dla spamerów. 4. **Testuj po każdej zmianie** – np. na https://mxtoolbox.com.

Narzędzia do testowania SPF

- https://mxtoolbox.com/spf.aspx
- https://dmarcian.com/spf-survey/
- https://www.kitterman.com/spf/validate.html
- https://dnschecker.org/spf-record-checker.php

Co się stanie, gdy SPF zawiedzie?

To zależy od polityki serwera odbiorczego. Możliwe reakcje:

- zaakceptowanie, ale oznaczenie jako SPAM (softfail),
- odrzucenie wiadomości (fail),
- całkowita neutralność – traktowanie jak każdą inną wiadomość.

Częste problemy z SPF

- Brak `all` → rekord nieskuteczny
- Zbyt wiele `include:` → przekroczenie limitu zapytań DNS
- Błąd składni (np. podwójne `v=spf1`)
- Nieaktualne wpisy dostawców (np. po migracji serwera)

Podsumowanie

SPF jest prostym, ale bardzo skutecznym narzędziem zabezpieczającym Twoją domenę e-mail przed nadużyciami. Prawidłowo skonfigurowany:

- ogranicza możliwość podszywania się pod Twój adres e-mail,
- poprawia reputację domeny,
- zwiększa dostarczalność wiadomości.

SPF powinien być stosowany **razem z DKIM i DMARC** dla pełnej ochrony poczty.