Mail: DMARC – Ochrona przed Spoofingiem i Phishingiem

Co to jest DMARC?

DMARC (Domain-based Message Authentication, Reporting, and Conformance) to **protokół uwierzytelniania e-maili**, który chroni domeny przed:

- podszywaniem się pod adresy e-mail (spoofingiem),
- atakami phishingowymi,
- nieautoryzowanym użyciem domeny do wysyłki e-maili.

DMARC współpracuje z dwoma innymi mechanizmami uwierzytelniania wiadomości:

- **SPF** (Sender Policy Framework) – określa, które serwery mogą wysyłać maile w imieniu domeny.
- **DKIM** (DomainKeys Identified Mail) – podpis kryptograficzny w wiadomości, potwierdzający autentyczność nadawcy.

Jak działa DMARC?

1. Serwer odbiorcy (np. Gmail, Outlook) otrzymuje wiadomość e-mail. 2. Sprawdza, czy wiadomość:

- przeszła test **SPF**,
- przeszła test **DKIM**,
- i czy **nadawca jest zgodny z domeną** (czyli tzw. „alignment”).

3. Na podstawie wyniku, serwer sprawdza **politykę DMARC**, którą ustawiła domena nadawcy. 4. W zależności od polityki (`none`, `quarantine`, `reject`), wiadomość jest:

- zaakceptowana,
- oznaczona jako spam,
- lub całkowicie odrzucona.

Rekord DMARC w DNS

Rekord DMARC to **rekord TXT**, dodany do strefy DNS domeny, np.:

```
_dmarc.ostrowski.net.pl. IN TXT "v=DMARC1; p=quarantine;
rua=mailto\:kacper\@ostrowski.net.pl
```

Składnia rekordu DMARC

Parametr	Opis
`v=DMARC1`	Wersja protokołu (zawsze `DMARC1`)
`p=`	Polityka DMARC (`none`, `quarantine`, `reject`)
`rua=`	Adres e-mail do raportów zbiorczych (aggregate reports)
`ruf=`	Adres e-mail do raportów szczegółowych (forensic reports – rzadko używane)
`fo=`	Kiedy generować raporty (np. `fo=1` = każda porażka SPF/DKIM)

Polityki DMARC

p=none

* Tryb monitorowania. * Nie podejmuje żadnych działań wobec nieautoryzowanych wiadomości. * Służy do zbierania raportów i weryfikacji konfiguracji SPF/DKIM. * Zalecany jako pierwszy krok.

p=quarantine

* Wysyła podejrzane wiadomości do folderu **SPAM/JUNK**. * Ochrona przed phishingiem – ale nie blokuje wiadomości całkowicie. * Dobry kompromis pomiędzy bezpieczeństwem a ryzykiem fałszywych alarmów. * Zwykle używany jako drugi krok przed pełnym odrzucaniem (`reject`).

p=reject

* Najsilniejsza polityka – całkowicie **odrzuca** wiadomości, które nie przejdą testów. * Zapewnia maksymalną ochronę przed spoofingiem. * Zalecana **tylko wtedy**, gdy:

- SPF i DKIM są poprawnie skonfigurowane,
- Masz pełną kontrolę nad wszystkimi serwerami wysyłającymi wiadomości w imieniu domeny.

Przykładowe Rekordy DMARC

Tryb monitorowania

```
v=DMARC1; p=none; rua=mailto\:kacper\@ostrowski.net.pl
```

Tryb kwarantanny

```
v=DMARC1; p=quarantine; rua=mailto\:kacper\@ostrowski.net.pl; fo=1
```

Tryb odrzucania

```
v=DMARC1; p=reject; rua=mailto\:kacper\@ostrowski.net.pl; fo=1
```

Raportowanie (rua, ruf)

- **rua** – raporty zbiorcze (raz dziennie), w formacie XML, pokazujące statystyki SPF/DKIM/DMARC.
- **ruf** – raporty szczegółowe (jeśli wspierane przez odbiorcę), zawierające kopie problematycznych wiadomości.

Raporty można analizować ręcznie lub za pomocą narzędzi takich jak:

- https://dmarcian.com/
- https://easydmarc.com/
- https://mail-tester.com/
- https://mxtoolbox.com/

Zalecana kolejność wdrażania

1. **Utwórz i zweryfikuj SPF i DKIM**. 2. **Dodaj rekord DMARC z `p=none` i monitoruj raporty**. 3. Po kilku dniach/tygodniach:

- jeśli legalne wiadomości przechodzą testy,
- a raporty nie pokazują błędów,

4. **Zmień politykę na `p=quarantine`**. 5. Po kolejnej fazie testów, przejdź do **`p=reject`** (pełna ochrona).

Podsumowanie

DMARC to kluczowy element bezpieczeństwa poczty e-mail. Umożliwia właścicielowi domeny:

- ochronę reputacji,
- zapobieganie spoofingowi i phishingowi,
- zbieranie danych diagnostycznych,
- kontrolę nad sposobem obsługi nieautoryzowanych wiadomości.

Pełna ochrona wymaga poprawnej konfiguracji **SPF**, **DKIM** oraz dobrze dobranej **polityki DMARC**.