Raport Bezpieczeństwa Poczty

Audyt uwierzytelniania SPF, DKIM i ochrony przed podszywaniem DMARC

Dominik Rudkowski
Audyt bezpieczeństwa poczty | +48 536 028 166
kontaktrudkowski@gmail.com | rudkowski.netlify.app

30/100

Klasa E

Domena: kancelaria.example

Data badania: 2026-11-08 20:10:38
Dostawca poczty: Własny / Nierozpoznany serwer
Czas odpowiedzi DNS: 897 ms | Metodologia: Pasywny audyt RFC DNS

Protokół	Status	Podsumowanie konfiguracji
SPF RFC 7208	POPRAWNY (-all)	Mechanizm kończący: `-all` | Liczba lookupów DNS: 5/10
DKIM RFC 6376	NIE WYKRYTO (HEUR.)	Przetestowano 23 popularnych selektorów. Możliwy unikalny selektor.
DMARC RFC 7489	BRAK POLITYKI	Domena bezbronna wobec podszywania się (e-mail spoofing).
MX / Transport	POCZTA AKTYWNA	Dostawca: Nieznany | MTA-STS: NIE | TLS-RPT: NIE

Kluczowe ustalenia i ocena ryzyka dla firmy

[DMARC] Brak wdrożonej polityki DMARC

Domena nie posiada opublikowanego rekordu DMARC w DNS (_dmarc).

Konsekwencje biznesowe: Brak DMARC oznacza, że serwery pocztowe na świecie nie wiedzą, co zrobić ze sfałszowanymi wiadomościami. Dowolny przestępca może wysyłać e-maile z adresem Twojej firmy jako nadawcy (spoofing), przeprowadzając ataki phishingowe na klientów i pracowników.

Zalecenie: Wdróż politykę DMARC na serwerze DNS. Zacznij od trybu monitoringu (p=none) z adresem do raportów rua=, a po weryfikacji legalnych wysyłek przejdź na p=quarantine lub p=reject.

```
Wpis DNS do dodania: TXT _dmarc.kancelaria.example "v=DMARC1; p=none;
rua=mailto:dmarc-reports@kancelaria.example; pct=100"
```

[SPF] Rygorystyczny mechanizm końcowy SPF (-all / HardFail)

Tylko jawnie wymienione serwery są uprawnione do nadawania poczty. Cała reszta jest bezwzględnie odrzucana.

Konsekwencje biznesowe: Brak ryzyka, o ile wszystkie legalne systemy (np. newsletter, CRM, fakturowanie) zostały uwzględnione w rekordzie.

Zalecenie: Upewnij się, że każde nowe narzędzie wysyłkowe jest dodawane do SPF przed rozpoczęciem wysyłki.

[DKIM] Nie wykryto selektora DKIM na podstawie popularnych wzorców

Przeskanowano 23 typowych selektorów (m.in. domyślne dla popularnych platform). Selektory DKIM nie są indeksowane w DNS, więc mogą działać pod unikalną, niestandardową nazwą.

Konsekwencje biznesowe: Jeśli DKIM rzeczywiście nie jest skonfigurowany, odbiorcy nie mogą zweryfikować integralności treści listu, a wskaźnik DMARC Alignment opiera się wyłącznie na SPF.

Zalecenie: Sprawdź w panelu administracyjnym swojego serwera pocztowego, czy funkcja podpisywania wiadomości (DKIM) jest aktywna i jaki selektor został jej przypisany.

Szczegóły Techniczne Audytu: kancelaria.example

Data: 2026-11-08 20:10:38
Dominik Rudkowski

Dokumentacja dla administratora systemów i personelu IT

1. Konfiguracja SPF (Sender Policy Framework)

Opublikowany rekord SPF:
```
v=spf1 a mx include:spf.hosting-przyklad.pl -all
```

• Liczba mechanizmów generujących zapytania DNS: 5 (maksymalny limit wg RFC 7208: 10)
• Mechanizm domyślny / końcowy: -all
• Zgodność z RFC 7208: ZGODNY
• Drzewo ewaluacji zapytań DNS:
→ a (+1 lookup)
→ mx (+1 lookup)
→ include:spf.hosting-przyklad.pl (+1 lookup)
→ a (+1 lookup)
→ mx (+1 lookup)

2. Podpis kryptograficzny DKIM (DomainKeys Identified Mail)

```
Nie wykryto publicznych kluczy DKIM pod 22 popularnymi selektorami.
```

• Sprawdzone selektory: default, selector1, selector2, google, k1, k2, s1, s2, dkim, mail, smtp, mandrill, mxvault, zoho, cm...
• Rekomendacja: Standard bezpieczeństwa nakazuje stosowanie klucza RSA o długości minimum 2048 bitów.

3. Polityka DMARC (Domain-based Message Authentication)

Opublikowany rekord DMARC (_dmarc.kancelaria.example):
```
BRAK REKORDU DMARC W DNS
```

• Polityka główna (p=): Brak | Polityka dla subdomen (sp=): Domyślna (dziedziczy p)
• Adresy raportowania zagregowanego (rua=): Brak
• Adresy raportowania kryminalistycznego (ruf=): Brak

4. Rekordy MX i Bezpieczeństwo Transportu

```
MX priorytet 10: poczta.kancelaria.example
```

Plan Naprawczy - Gotowe Wpisy DNS do Wdrożenia

Typ	Host / Nazwa	Wartość rekordu
TXT	_dmarc	v=DMARC1; p=quarantine; rua=mailto:dmarc-reports@kancelaria.example; pct=100

Raport poufny przygotowany dla: kancelaria.example | Wszelkie prawa zastrzeżone © Dominik Rudkowski