Raport audytu bezpieczeństwa domeny firma-przyklad.pl

Skan z 10.11.2026, reguły 2026.11.6. Audytor SecVault, secvault.pl/audytor
PRZYKŁAD: firma-przyklad.pl to fikcyjna domena, a ustalenia pochodzą ze spreparowanych danych.

65/100

ocena D

Sprawdziliśmy z zewnątrz 67 ustawień w obszarach: poczta i podszywanie, powierzchnia ataku, ochrona marki, strona WWW, domena i DNS, prywatność i RODO. Tak samo widzi je każdy w internecie, bez logowania i bez dostępu do serwera. 2 sprawdzeń nie dało się wykonać, więc nie wchodzą do wyniku.

Co to znaczy dla firmy

Z publicznych źródeł widać elementy infrastruktury, które ułatwiają wybór celu ataku.
Poczta firmowa jest słabiej chroniona: łatwiej wysłać wiadomość, która wygląda na wysłaną przez firmę, a prawdziwe wiadomości częściej trafiają do spamu.

Co widzi atakujący

- Może wysłać wiadomość z adresem nadawcy w Twojej domenie, a serwer odbiorcy nie dostaje polecenia, żeby ją odrzucić.
- Widzi subdomenę wskazującą na usługę, której już nie ma; taką nazwę bywa da się przejąć i wystawić pod nią własną treść.
- Może użyć zarejestrowanej już domeny z literówką w Twojej nazwie, żeby podszyć się pod firmę w poczcie albo na stronie.

Najważniejsze poprawki

1. Ryzyko przejęcia subdomeny

1 rekord DNS wskazuje na nieistniejącą nazwę (np. stary-sklep.firma-przyklad.pl → firma-przyklad-sklep.hostingsklepow.example). Ktoś może zarejestrować cel i podstawić treść pod Twoją subdomenę. Usuń porzucone rekordy DNS.
Dlaczego: Jeśli subdomena wskazuje (CNAME) na nieistniejącą nazwę albo nieaktywną usługę, ktoś obcy może ją zarejestrować i serwować własną treść pod Twoim adresem (phishing, złośliwe skrypty).
Jak naprawić: Usuń z DNS rekordy wskazujące na usługi, których już nie używasz.

2. DMARC: rekord

Brak rekordu DMARC - każdy może wysyłać wiadomości "od" tej domeny, a odbiorcy nie dostają polecenia, co z nimi robić.
Dlaczego: DMARC łączy SPF i DKIM i mówi odbiorcom, co robić z podszywaniem. Bez niego ktoś może wysyłać faktury "od Ciebie".
Jak naprawić: Dodaj TXT _dmarc.<domena>: v=DMARC1; p=none; rua=mailto:... - zacznij od monitorowania.

3. Czy da się podszyć pod firmę

Każdy może wysłać wiadomość wyglądającą na "od Twojej firmy" i trafi ona do skrzynki odbiorcy (klienta, kontrahenta). Brakuje skutecznej polityki DMARC. To główny mechanizm oszustw "na fakturę".
Dlaczego: Bez skutecznego DMARC każdy może wysłać e-mail wyglądający na "od Twojej firmy" do Twoich klientów i kontrahentów. To mechanizm oszustw na fałszywą fakturę i zmianę numeru konta.
Jak naprawić: Doprowadź SPF i DKIM do porządku, a politykę DMARC ustaw na quarantine, potem reject.

Następny krok

Zacznij od pierwszej poprawki z listy. Po zmianie uruchom skan ponownie: wynik pokaże, czy zmiana zadziałała.

Wynik w obszarach

Obszar	Wynik	Waga	Do poprawy
Poczta i podszywanie	77/100	24	3
Powierzchnia ataku	51/100	22	3
Ochrona marki	20/100	14	3
Strona WWW	90/100	18	3
Domena i DNS	65/100	14	2
Prywatność i RODO	86/100	8	1
Widoczność w Google	87/100	poza oceną	2
Dostępność strony	93/100	poza oceną	1

Rekordy DNS do wklejenia

Propozycje policzone z wyników skanu. Przed wklejeniem przeczytaj uwagę pod każdym rekordem; zmiany w DNS rób w panelu dostawcy DNS domeny.

TXT _dmarc.firma-przyklad.pl

```
v=DMARC1; p=none; rua=mailto:dmarc@firma-przyklad.pl
```

Skrzynka dmarc@firma-przyklad.pl musi istnieć (albo podaj inny adres w tej domenie). Po 2-4 tygodniach raportów: p=quarantine, potem p=reject.

TXT _smtp._tls.firma-przyklad.pl

```
v=TLSRPTv1; rua=mailto:tlsrpt@firma-przyklad.pl
```

Raporty o nieudanych połączeniach szyfrowanych do Twojej poczty. Skrzynka tlsrpt@firma-przyklad.pl musi istnieć.

Szczegóły: co poprawić

Poczta i podszywanie

DMARC: rekord [krytyczne]

Brak rekordu DMARC - każdy może wysyłać wiadomości "od" tej domeny, a odbiorcy nie dostają polecenia, co z nimi robić.

Dlaczego: DMARC łączy SPF i DKIM i mówi odbiorcom, co robić z podszywaniem. Bez niego ktoś może wysyłać faktury "od Ciebie".
Jak naprawić: Dodaj TXT _dmarc.<domena>: v=DMARC1; p=none; rua=mailto:... - zacznij od monitorowania.

MTA-STS [do poprawy]

Brak MTA-STS - szyfrowanie przy odbiorze poczty nie jest wymuszane (zalecane dla firm).

Dlaczego: Wymusza szyfrowanie TLS przy dostarczaniu poczty do Twojej domeny; bez tego atakujący w sieci może zdegradować połączenie do zwykłego tekstu.
Jak naprawić: Opublikuj rekord _mta-sts TXT i plik polityki pod https://mta-sts.<domena>/.well-known/mta-sts.txt (mode: enforce). Linie mx: muszą obejmować wszystkie serwery z rekordów MX.

TLS-RPT [do poprawy]

Brak TLS-RPT (raporty o błędach TLS przy dostarczaniu).

Dlaczego: Raporty o nieudanych połączeniach TLS do Twoich serwerów pocztowych.
Jak naprawić: Dodaj TXT _smtp._tls.<domena>: v=TLSRPTv1; rua=mailto:...

Powierzchnia ataku

Ryzyko przejęcia subdomeny [krytyczne]
1 rekord DNS wskazuje na nieistniejącą nazwę (np. stary-sklep.firma-przyklad.pl → firma-przyklad-sklep.hostingsklepow.example). Ktoś może zarejestrować cel i podstawić treść pod Twoją subdomenę. Usuń porzucone rekordy DNS.
Dlaczego: Jeśli subdomena wskazuje (CNAME) na nieistniejącą nazwę albo nieaktywną usługę, ktoś obcy może ją zarejestrować i serwować własną treść pod Twoim adresem (phishing, złośliwe skrypty).
Jak naprawić: Usuń z DNS rekordy wskazujące na usługi, których już nie używasz.

Subdomeny w logach certyfikatów [do sprawdzenia]
W publicznych logach certyfikatów są subdomeny (4), w tym o nazwach typowych dla środowisk testowych albo paneli: test.firma-przyklad.pl. Sprawdź, czy mają być dostępne z internetu i czy są chronione.
Dlaczego: Każdy certyfikat trafia do publicznych logów Certificate Transparency, więc adresy jak dev., test. czy admin. są widoczne dla wszystkich, a bywają zapomniane i słabiej chronione.
Jak naprawić: Przejrzyj listę, wyłącz albo zabezpiecz środowiska testowe i panele, których nie powinno być widać z internetu.

Integralność skryptów (SRI) [do poprawy]
1 skrypt ładowany z obcych serwerów (cdn.przyklad-widget.example) bez zabezpieczenia integralności (SRI). Jeśli któryś serwer zostanie przejęty, może podmienić skrypt na Twojej stronie.
Dlaczego: Skrypt ładowany z obcego serwera bez atrybutu integrity działa na Twojej stronie z pełnym zaufaniem; przejęcie tamtego serwera pozwala podmienić kod u Ciebie.
Jak naprawić: Dodaj atrybut integrity (SRI) do skryptów z obcych serwerów albo hostuj je u siebie.

Ochrona marki

Czy da się podszyć pod firmę [krytyczne]
Każdy może wysłać wiadomość wyglądającą na "od Twojej firmy" i trafi ona do skrzynki odbiorcy (klienta, kontrahenta). Brakuje skutecznej polityki DMARC. To główny mechanizm oszustw "na fakturę".
Dlaczego: Bez skutecznego DMARC każdy może wysłać e-mail wyglądający na "od Twojej firmy" do Twoich klientów i kontrahentów. To mechanizm oszustw na fałszywą fakturę i zmianę numeru konta.
Jak naprawić: Doprowadź SPF i DKIM do porządku, a politykę DMARC ustaw na quarantine, potem reject.

Domeny łudząco podobne [do sprawdzenia]
Zarejestrowane są nazwy różniące się od Twojej literówką, podobnym znakiem albo dopiskiem: frma-przyklad.pl. Sprawdź, czy są Twoje. Cudza domena tego typu nadaje się do podszywania się pod firmę. Ta sama nazwa z inną końcówką jest zarejestrowana: firma-przyklad.com. To mogą być Twoje domeny albo inne firmy o tej samej nazwie.
Dlaczego: Oszuści rejestrują nazwy z literówką albo inną końcówką, żeby podszywać się pod markę i łowić klientów.
Jak naprawić: Sprawdź, czy podobne domeny są Twoje; kluczowe warianty warto zarejestrować samemu, a cudze podszywające się zgłosić. Przy krótkiej nazwie domeny różniące się jedną literą to zwykle inne marki i nie wpływają na wynik.

Podobne domeny z pocztą [do sprawdzenia]
Poczta jest skonfigurowana (rekord MX) na podobnych domenach: frma-przyklad.pl, firma-przyklad.com. Jeśli nie są Twoje, mogą posłużyć do korespondencji udającej Twoją firmę. Sam rekord MX nie dowodzi złych zamiarów.
Dlaczego: Podobna domena z rekordem MX może odbierać pocztę zaadresowaną z pomyłką i prowadzić korespondencję w imieniu firmy o łudząco podobnej nazwie.
Jak naprawić: Ustal, do kogo należą te domeny. Własne zostaw. Przy cudzej, która podszywa się pod Twoją firmę, zgłoś nadużycie do jej rejestratora i podaj klientom oficjalny adres.

Strona WWW

Content-Security-Policy [do poprawy]
Brak Content-Security-Policy (ochrona przed wstrzykiwaniem skryptów).
Dlaczego: Ogranicza, skąd strona może ładować skrypty - główna ochrona przed wstrzykniętym kodem (XSS).
Jak naprawić: Zacznij od Content-Security-Policy-Report-Only, potem wdróż politykę bez unsafe-inline (skrypty w plikach albo ze skrótem sha256). Politykę wysyłaj w nagłówku HTTP, nie tylko w znaczniku <meta>.

security.txt [do poprawy]
Brak /.well-known/security.txt (jak zgłosić Ci lukę w bezpieczeństwie).
Dlaczego: Standardowy plik z kontaktem dla osób, które znajdą lukę.
Jak naprawić: Umieść /.well-known/security.txt z polem Contact: (RFC 9116).

Permissions-Policy [do poprawy]
Brak Permissions-Policy.
Dlaczego: Wyłącza nieużywane funkcje przeglądarki (kamera, mikrofon, lokalizacja) dla osadzonych treści.
Jak naprawić: Dodaj Permissions-Policy: camera=(), microphone=(), geolocation=().

Domena i DNS

DNSSEC [do poprawy]
Brak DNSSEC - odpowiedzi DNS domeny nie są podpisane (możliwe podstawienie adresu w sieciach bez ochrony).
Dlaczego: Podpisane odpowiedzi DNS uniemożliwiają podstawienie fałszywego adresu strony lub serwera poczty.
Jak naprawić: Włącz DNSSEC u operatora DNS i dodaj rekord DS u rejestratora (Cloudflare: DNS → Settings → DNSSEC).

Rekord CAA [do poprawy]
Brak rekordu CAA (każdy urząd certyfikacji może wystawić certyfikat dla domeny).
Dlaczego: Ogranicza, które urzędy certyfikacji mogą wystawić certyfikat dla domeny.
Jak naprawić: Dodaj rekord CAA: 0 issue "letsencrypt.org" (plus urząd Twojego hostingu/CDN).

Prywatność i RODO

Klauzula przy formularzu [do poprawy]
Formularz bez klauzuli informacyjnej RODO i bez pola zgody.
Dlaczego: Przy zbieraniu danych przez formularz trzeba spełnić obowiązek informacyjny.
Jak naprawić: Dodaj krótką klauzulę informacyjną pod formularzem (administrator, cel, prawa) i link do polityki.

Widoczność w Google

Open Graph [do poprawy]
Brak znaczników Open Graph - link do strony nie ma ładnego podglądu.
Dlaczego: Decyduje o podglądzie linku w komunikatorach i mediach społecznościowych.
Jak naprawić: Dodaj og:title, og:description i og:image.

Dane strukturalne [do poprawy]
Brak danych strukturalnych JSON-LD (Organization albo LocalBusiness dla firmy, Person dla strony osoby, SoftwareApplication albo Product dla produktu).
Dlaczego: JSON-LD daje wyszukiwarce uporządkowane dane: firmy (Organization, LocalBusiness: adres, godziny), osoby (Person) albo produktu (SoftwareApplication, Product).
Jak naprawić: Dodaj blok JSON-LD z typem pasującym do strony: Organization albo LocalBusiness dla firmy, Person dla strony osoby, SoftwareApplication albo Product dla produktu.

Dostępność strony

Link "przejdź do treści" [do poprawy]
Brak linku "przejdź do treści" dla klawiatury.
Dlaczego: Pozwala użytkownikom klawiatury ominąć menu.
Jak naprawić: Dodaj na początku strony link do kotwicy z treścią (np. #tresc) z tekstem "Przejdź do treści", widoczny po fokusie.

Bez uwag

Serwery pocztowe (MX), SPF: rekord, SPF: polityka "all", SPF: limit odwołań DNS, DKIM: podpis wiadomości, Szyfrowanie na serwerze MX (STARTTLS), Rekord odwrotny (PTR) serwera MX, Sekrety w kodzie strony, HTTPS działa, Przekierowanie HTTP → HTTPS, Certyfikat TLS, Stare wersje TLS, HSTS, X-Content-Type-Options, Ochrona przed clickjackingiem, Referrer-Policy, Flagi ciasteczek, Ujawnianie wersji oprogramowania, Mixed content, Rozmiar strony głównej, Czas odpowiedzi serwera, Adres z www. i bez, IPv6, Termin ważności domeny, Serwery nazw, Polityka prywatności, Zgoda na cookies i trackery, Dane firmy na stronie, Tytuł strony, Meta description, Nagłówek H1, Link canonical, Język strony, Wersja mobilna (viewport), Indeksowanie strony głównej, robots.txt, Mapa strony (sitemap), Opisy obrazów (alt), Język dokumentu, Etykiety pól formularza, Struktura nagłówków, Tytuł strony, Powiększanie na telefonie.

Nie sprawdzono (poza wynikiem)

DMARC: polityka (Bez rekordu DMARC nie ma czego ocenić.); DMARC: raporty (Bez rekordu DMARC nie ma czego ocenić.).

NIS2: co widać z zewnątrz

Mapowanie ustaleń na środki z art. 21 ust. 2 dyrektywy NIS2. Środki organizacyjne potwierdzasz wewnątrz firmy.

Środek	Stan

a) Analiza ryzyka i polityki bezpieczeństwa informacji	poza zasięgiem skanu
b) Obsługa incydentów (wykrywanie, reagowanie, zgłaszanie)	braki
c) Ciągłość działania i kopie zapasowe	bez uwag
d) Bezpieczeństwo łańcucha dostaw	braki
e) Bezpieczeństwo systemów i obsługa podatności	braki
f) Ocena skuteczności środków bezpieczeństwa	częściowo
g) Higiena cyberbezpieczeństwa i szkolenia	braki
h) Kryptografia i szyfrowanie	częściowo
i) Kontrola dostępu i zarządzanie aktywami	częściowo
j) Uwierzytelnianie wieloskładnikowe i bezpieczna łączność	poza zasięgiem skanu

Metoda

Skan był pasywny i zewnętrzny: zapytania DNS, kilka żądań do strony głównej, jedno połączenie z serwerem pocztowym, publiczne rejestry (RDAP, logi certyfikatów). Nie skanowaliśmy portów i nie próbowaliśmy się logować. Raport opisuje stan z dnia skanu. Sprawdzenia oznaczone jako niesprawdzone nie wchodzą do wyniku.