INNOVIX

RAPORT 2026 · BADANIE PASYWNE

Nagłówki bezpieczeństwa i TLS w serwisach polskich spółek

Strony główne 140 spółek z indeksów WIG20, mWIG40 i sWIG80 · pomiar 2026-10-08

NAJWAŻNIEJSZE WYNIKI

Pięć liczb z badania

50,4%	stron wymusza bezpieczne połączenie nagłówkiem HSTS
35,2%	ma politykę Content-Security-Policy w nagłówku
51,2%	chroni się przed osadzaniem w cudzych ramkach
2,4%	publikuje plik security.txt z kontaktem dla badaczy
96%	negocjuje TLS 1.3 (strony z danymi o połączeniu)

Lista: 140 serwisów; wykluczone przez robots.txt: 0; problem z połączeniem HTTPS: 9; odpowiedź inna niż 200 (np. strona blokady ruchu automatycznego): 6. Odsetki nagłówków liczone od 125 stron z odpowiedzią 200.

Wnioski

- Szyfrowanie jest standardem, ale jego wzmocnienie - nie: 95,2% stron przekierowuje z HTTP na HTTPS, a nagłówek HSTS wysyła tylko połowa (50,4%); czas obowiązywania co najmniej rok ma 36,8%.
- Polityka Content-Security-Policy to wciąż mniejszość (35,2%), a połowa z tych polityk (17,6% wszystkich stron) dopuszcza skrypty inline ('unsafe-inline'), co osłabia ochronę przed atakami XSS.
- Prawie co druga strona (48,8%) nie chroni się przed osadzaniem w cudzych ramkach - ani nagłówkiem X-Frame-Options, ani dyrektywą frame-ancestors.
- Co trzecia strona (34,4%) nie wysyła żadnego z sześciu podstawowych nagłówków bezpieczeństwa; komplet ma 10,4%.
- Kontakt dla osób zgłaszających podatności to rzadkość: plik security.txt z polem Contact publikuje 2,4% serwisów.
- Konfiguracja TLS wypada dobrze: 96% stron z danymi wynegocjowało TLS 1.3; problem z połączeniem HTTPS miało 9 ze 140 serwisów (6,4%), najczęściej certyfikat nieobejmujący adresu z www albo niepełny łańcuch certyfikatów.

WYNIKI SZCZEGÓŁOWE

Nagłówki i konfiguracja

Wskaźnik	Odsetek
HTTP przekierowuje na HTTPS	95,2%
HSTS (Strict-Transport-Security)	50,4%
HSTS na co najmniej rok	36,8%
HSTS z dyrektywą preload	17,6%
Content-Security-Policy (nagłówek)	35,2%
CSP z 'unsafe-inline' w script-src	17,6%
Ochrona przed osadzaniem w ramkach	51,2%
X-Content-Type-Options: nosniff	49,6%
Referrer-Policy	33,6%
Permissions-Policy	14,4%
Cross-Origin-Opener-Policy	3,2%
Wersja oprogramowania w nagłówku Server	15,2%
Nagłówek X-Powered-By	15,2%
security.txt z polem Contact	2,4%



Wskaźniki "wersja w nagłówku Server", "X-Powered-By" i "CSP z 'unsafe-inline'" są niepożądane - im niższy odsetek, tym lepiej.

TLS i certyfikaty

Wynegocjowana wersja protokołu (serwisy z działającym HTTPS): TLS 1.2 - 5, TLS 1.3 - 120, brak danych - 6. Brak danych wynika z ograniczenia narzędzia pomiarowego (poprawione na kolejną edycję).

Problem z połączeniem HTTPS miało 9 z 140 serwisów: certyfikat nie obejmuje adresu (np. z www) - 3; niepełny łańcuch certyfikatów - 2; przekroczony czas odpowiedzi - 1; połączenie HTTPS odrzucone (port 443) - 1; certyfikat samopodpisany - 1; zbyt słaby klucz DH w konfiguracji TLS - 1. Niepełny łańcuch certyfikatów część przeglądarek uzupełnia sama; certyfikat bez adresu z www oznacza ostrzeżenie dla osób wpisujących adres w tej formie.

Dni do wygaśnięcia certyfikatu w dniu pomiaru: poniżej 30 - 8, 30-90 - 77, powyżej 90 - 40. Krótki termin nie musi oznaczać problemu - certyfikaty odnawiane automatycznie mają zwykle 90 dni ważności.

Ciasteczka strony głównej

Ciasteczka ustawia 65 stron głównych (razem 160). Atrybut Secure ma 50%, HttpOnly - 50%, SameSite - 40,6% ciasteczek. Część ciasteczek musi być czytelna dla skryptów (np. zgody), więc brak HttpOnly nie zawsze jest błędem.

CO ZROBIĆ

Lista kontrolna dla zespołu

- Przekierowanie stałe (301 lub 308) z http:// na https:// dla domeny i www.
- Strict-Transport-Security: max-age co najmniej 31536000, includeSubDomains; po sprawdzeniu subdomen - preload.
- Content-Security-Policy: zacznij od trybu Report-Only, usuń skrypty i style inline, unikaj 'unsafe-inline' w script-src (nonce albo hash).
- frame-ancestors 'self' (albo 'none') w CSP - ochrona przed osadzaniem w cudzych ramkach; X-Frame-Options dla starszych przeglądarek.
- X-Content-Type-Options: nosniff, Referrer-Policy: strict-origin-when-cross-origin, Permissions-Policy z wyłączeniem nieużywanych funkcji.
- Usuń wersje oprogramowania z nagłówków Server i X-Powered-By.
- Ciasteczka sesyjne: Secure, HttpOnly, SameSite=Lax lub Strict.
- Plik /.well-known/security.txt (RFC 9116) z polami Contact i Expires - kontakt dla osób zgłaszających podatności.
- Monitoruj ważność certyfikatów i automatyzuj ich odnawianie.

Nagłówki to higiena konfiguracji widocznej z zewnątrz, a nie pełna ocena bezpieczeństwa. Test penetracyjny sprawdza, czy zabezpieczenia aplikacji i infrastruktury działają w praktyce.

Metodyka i ograniczenia

Lista: spółki z indeksów WIG20, mWIG40 i sWIG80 według portfeli GPW Benchmark po korekcie z 18 września 2026 r.; adresy stron z kart spółek na gpw.pl. Najwyżej 4 żądania na serwis (robots.txt, strona główna przez HTTPS z najwyżej trzema przekierowaniami, strona główna przez HTTP, security.txt), robots.txt szanowany, jawny identyfikator robota InnovixHeaderSurvey, co najmniej 3 sekundy przerwy między żądaniami. Bez skanowania, podstron, formularzy i prób dostępu.

Ograniczenia: jeden pomiar w jednym dniu; strona główna nie reprezentuje całego serwisu; nagłówki mogą różnić się między podstronami i zależeć od sieci CDN; wynik nie ocenia zgodności z ustawą o krajowym systemie cyberbezpieczeństwa ani innymi przepisami. Wyniki publikujemy wyłącznie zbiorczo; dane per serwis przechowujemy lokalnie przez 12 miesięcy.

Pełna metodyka: innovix.pl/wiedza/badanie-naglowkow-bezpieczenstwa/

O Innovix

Innovix sp. z o.o. to software house z Wrocławia z własnym zespołem testów bezpieczeństwa. Tworzy oprogramowanie dedykowane dla firm z sektorów regulowanych i wykonuje testy penetracyjne aplikacji, API, infrastruktury i chmury. Kontakt: audyty@innovix.pl, +48 575 621 877, innovix.pl. Wyniki można cytować z podaniem źródła (Innovix, innovix.pl).