Skrócone sprawozdanie z audytu PQC

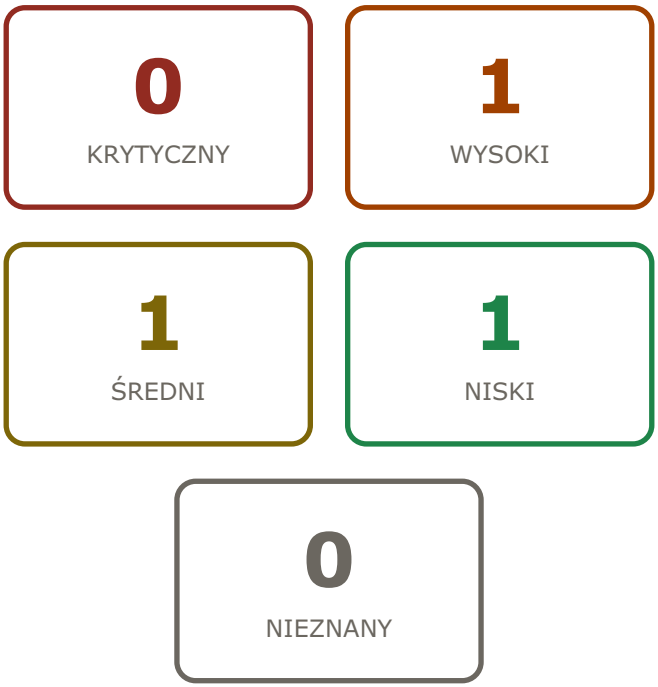
Klient: **InvestPro MVP Sp. z o.o.**

ID audytu: `00000000-0000-0000-0003-000000000003`

Wygenerowano: 2026-06-03 19:30 UTC

Pewność modelu: **94%**

Podsumowanie ryzyka



Gotowość regulacyjna

71/100 **N/D**

Wskaźnik gotowości NIS2

Wskaźnik gotowości DORA

Niewystarczające dane skanu do oceny zbiorczej. Sprawdzono jedynie publiczne punkty końcowe TLS; kontrole wewnętrzne, polityki zarządzania i procesy ICT są poza zakresem. Pełny wynik wymaga ręcznej sesji audytora.

Orientacyjny termin remediacji: **180** dni

Obserwacje

WYSOKI REQUIRES_REVIEW:X25519 (classical only, no PQC hybrid) → REQUIRES_REVIEW:X25519+ML-KEM-768 hybrid — enable via Vercel Edge TLS settings or Cloudflare proxy

TLS 1.3 is correctly deployed with modern AEAD cipher suites — an excellent baseline for an 8-person startup. However, key exchange uses classical X25519 only, without ML-KEM-768 hybrid (FIPS 203). Client financial portfolios and personal authentication data transmitted over these sessions are at risk of Harvest-Now-Decrypt-Later attack. Vercel's Edge Network has announced PQC hybrid TLS support; enabling it is a configuration change, not an engineering project.

Komponent: TLS 1.3 key exchange on investpro.pl and app.investpro.pl | **Nakład pracy:** trywialny | **Ryzyko HNDL:** tak

NISKI Ed25519 → REQUIRES_REVIEW:ML-DSA-65 JWT signing (FIPS 204) — available via liboqs Python bindings in Supabase edge functions

JWT session tokens use EdDSA (Ed25519) — currently the strongest available classical signature for this use case. Ed25519 is quantum-vulnerable via Shor's algorithm but has shorter-term risk than RSA/ECDSA due to key size dynamics. Session tokens typically expire within hours, reducing HNDL exposure. Migration to ML-DSA-65 (FIPS 204) can be scheduled within the 12-24 month window.

Komponent: JWT EdDSA (Ed25519) — user session tokens | **Nakład pracy:** średni | **Ryzyko HNDL:** nie

ŚREDNI ECDSA-P256 → REQUIRES_REVIEW:When public CAs support ML-DSA: request ML-DSA-65 certificate (FIPS 204). Interim: HSTS + certificate pinning monitoring.

Let's Encrypt issues ECDSA-P256 certificates, which are quantum-vulnerable in their signing algorithm (Shor's algorithm on elliptic curves). While Let's Encrypt does not yet issue ML-DSA certificates (industry-wide limitation — public CAs awaiting ML-DSA CA/Browser Forum policy), planning for hybrid certificate trust chains is advisable for a regulated MiFID II entity.

Komponent: X.509 certificates — Let's Encrypt ECDSA-P256 | **Nakład pracy:** mały | **Ryzyko HNDL:** nie

Kontekst regulacyjny

Regulacja	Artykuł	KRYTYCZNY	Powiązane ustalenia
NIS2	`NIS2 Art.21(2)(f)`	WYSOKI	F-001
TLS key exchange does not include post-quantum hybrid as recommended under NIS2 Art. 21(2)(f) cryptographic policy requirements (PL transposition UoKSC Art.10). As a KNF-supervised entity, InvestPro may be in scope for enhanced NIS2 essential entity obligations.			
GDPR	`GDPR Art.32`	ŚREDNI	F-001
If PII processed in Supabase (client identification, portfolio data) is transmitted over TLS without PQC hybrid protection, this may constitute indicators of insufficient technical measures under GDPR Art.32 given the quantum threat horizon.			

> *NIS2 — ogólny pułap sankcji do €10M lub 2% rocznego obrotu (stosowany przez właściwy organ w przypadkach ciężkich naruszeń). Informacja ogólna, nie ocena indywidualnej odpowiedzialności.*

> *DORA — potencjalne sankcje do 1% dziennego obrotu za każdy dzień trwającego naruszenia. Informacja ogólna, nie ocena indywidualnej odpowiedzialności.*

> *UoKSC (PL) — sankcje do 100 000 PLN i ewentualne zawieszenie usług. Informacja ogólna, nie ocena indywidualnej odpowiedzialności.*

Priorytetowy plan działań

1. **REQUIRES_REVIEW:X25519 (classical only, no PQC hybrid) → REQUIRES_REVIEW:X25519+ML-KEM-768 hybrid — enable via Vercel Edge TLS settings or Cloudflare proxy** trywialny
   TLS 1.3 is correctly deployed with modern AEAD cipher suites — an excellent baseline for an 8-person startup. However, key exchange uses classical X25519 only, without ML-KEM-768 hybrid (FIPS 203). Client financial portfolios and personal authentication data transmitted over these sessions are at risk of Harvest-Now-Decrypt-Later attack. Vercel's Edge Network has announced PQC hybrid TLS support; enabling it is a configuration change, not an engineering project.

   NIS2 Art.21(2)(f) · GDPR Art.32

Mapa drogowa

Szybkie zwycięstwa (0–3 mies.)

Termin: 0-3

- Enable X25519+ML-KEM-768 hybrid TLS on Vercel or add Cloudflare proxy with PQC enabled
- Document current cryptographic stack as CBOM — baseline for future audits

Główna migracja (3–12 mies.)

Termin: 3-12

- Evaluate Supabase roadmap for ML-DSA JWT support
- Prototype Ed25519 → ML-DSA-65 migration in staging environment

+ 1 dodatkowych szczegółowych kroków w raporcie technicznym

KLAUZULA PRAWNA

Niniejszy dokument stanowi zautomatyzowaną ocenę gotowości do kryptografii post-kwantowej (PQC readiness assessment), a NIE certyfikowany audyt bezpieczeństwa. Wszystkie ustalenia mają charakter wskazujący na potencjalne ryzyka i niezgodności na podstawie publicznie dostępnych danych technicznych i informacji dostarczonych przez klienta. Dokument nie stanowi (a) porady prawnej, (b) gwarancji bezpieczeństwa, (c) oficjalnej opinii o zgodności z NIS2 / DORA / RODO — taką opinię wydaje wyłącznie certyfikowany audytor. Rekomendacje nie mają statusu nakazu. Zaleca się uzupełnienie raportu ręcznym przeglądem wykwalifikowanego specjalisty ds. bezpieczeństwa informatycznego przed podjęciem decyzji o skutkach prawnych lub finansowych. MorozzAI dostarcza raport «tak jak jest», bez wyraźnych ani dorozumianych gwarancji dokładności, kompletności lub zastosowania w konkretnych okolicznościach, i nie ponosi odpowiedzialności za decyzje podjęte na jego podstawie.