PQC-Bereitschaftsbewertung — Zusammenfassung

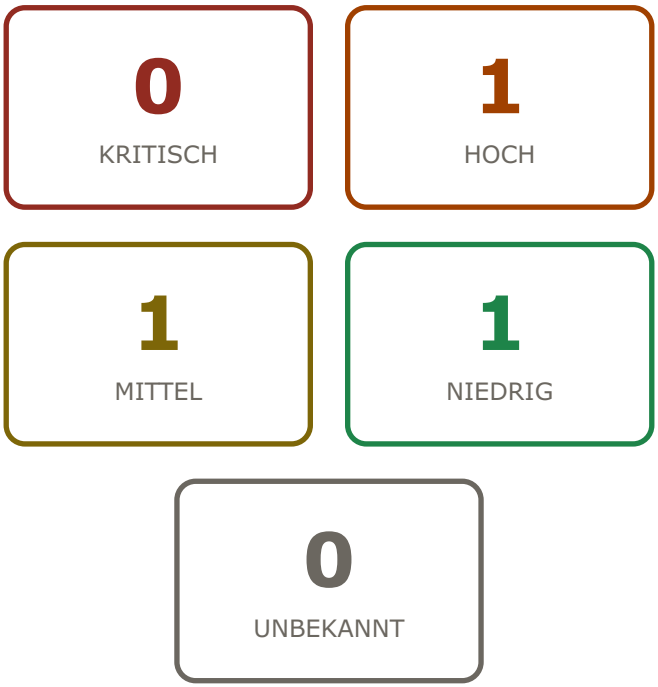
Auftraggeber: **InvestPro MVP Sp. z o.o.**

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

Erstellt am: 2026-06-03 19:30 UTC

Modellkonfidenz: **94%**

Risikoubersicht



Regulatorische Bereitschaftsindikatoren

71/100

NIS2-Bereitschaftsindikator

k.A.

DORA-Bereitschaftsindikator

Unzureichende Scandaten fur eine Gesamtbewertung. Es wurden nur offentlich erreichbare TLS-Endpunkte gescannt; interne Kontrollen, Governance und ICT-Prozesse wurden nicht bewertet. Eine vollstandige Bewertung erfordert eine manuelle Prufsitzung.

Indikativer Behebungszeitraum: **180** Tage

Feststellungen

HOCH 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.

Komponente: TLS 1.3 key exchange on investpro.pl and app.investpro.pl | **Aufwand:** trivial | **HNDL-Indikator:** ja

NIEDRIG 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.

Komponente: JWT EdDSA (Ed25519) — user session tokens | **Aufwand:** mittel | **HNDL-Indikator:** nein

MITTEL **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.

Komponente: X.509 certificates — Let's Encrypt ECDSA-P256 | **Aufwand:** gering | **HNDL-Indikator:** nein

Regulatorischer Kontext

Rechtsrahmen	Artikel	KRITISCH	Verbundene Feststellungen
NIS2	`NIS2 Art.21(2)(f)`	HOCH	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`	MITTEL	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 — illustrative Obergrenze fur Verwaltungsbussen bis zu 10 Mio. EUR oder 2 % des weltweiten Jahresumsatzes (angewendet von der zustandigen Behorde in schwerwiegenden Fallen). Allgemeine Information, keine Beurteilung Ihres spezifischen Haftungsrisikos.*

> *DORA — mogliche Zwangsgelder bis zu 1 % des taglichen Gesamtumsatzes pro Tag bei anhaltender Nichtkonformitat. Allgemeine Information, keine Beurteilung Ihres spezifischen Haftungsrisikos.*

Prioritare Massnahmen

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** trivial
   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

Massnahmenplan

Schnelle Massnahmen (0-3 Monate)

Zeitrahmen: 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

Hauptmigration (3-12 Monate)

Zeitrahmen: 3-12

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

+ 1 weitere detaillierte Schritte im technischen Bericht