



NIS2: Od registrace k realitě

Praktický průvodce pro **CISO & Compliance Officers** – Březen 2026

Blue Partners – NIS2 Whitepaper

Je březen 2026. NÚKIB ví, kdo jste. Teď musíte prokázat, že jste zabezpečení.



Registrace

Formální krok



Compliance

Funkční opatření

Ne papírová bezpečnost, ale funkční, prokazatelná a kontrolovatelná opatření.



10 pilířů compliance podle NIS2

1. Řízení (Governance)



Odpovědnost vedení



Aktiva, BIA



Řízení rizik

2. Odolnost (Resilience)



Zvládání incidentů



BCP/Krizové řízení



Bezpečnost dodavatelského řetězce

3. Hygiena (Hygiene)



Kryptografie



IAM & MFA



DevSec



Školení

Řízení rizik a odpovědnost vedení

Řízení rizik

Živý proces, ne dokument pro auditory.



Inventář aktiv



Matice rizik



Plán zvládání rizik

Toto je váš nejsilnější
argument pro board.



Odpovědnost vedení

Odpovědnost nelze delegovat – lze delegovat výkon, nikoli odpovědnost.

**Vysoká pokuta
+ osobní odpovědnost
statutárních orgánů.**

Incidenty a kontinuita: Hra o čas



BCP & Disaster Recovery



Netestovaný plán v šuplíku je při kontrole bezcenný.

- Pravidelné testování obnovy (RTO/RPO).



Technická hygiena a dodavatelský řetězec

Dodavatelský řetězec

Nejčastější slabé místo.

- Hodnocení dodavatelů
- Bezpečnostní požadavky ve smlouvách



Zero Trust & MFA

Nikdy nedůvěřuj, vždy ověřuj.

- MFA na kritických systémech
- Šifrování dat v klidu i při přenosu



Cesta k implementaci: Harmonogram



Fáze 0 & 1: Diagnostika a Prioritizace

Týden 1–6



Gap Analýza

Zjistěte, kde skutečně stojíte.

Výstup: Gap report (Splněno / Částečně / Nesplněno).

Analýza rizik

Prioritizovaný akční plán + Rozpočet.

Pro-Tip: Nezačínejte implementovat, dokud nevíte, co chybí.

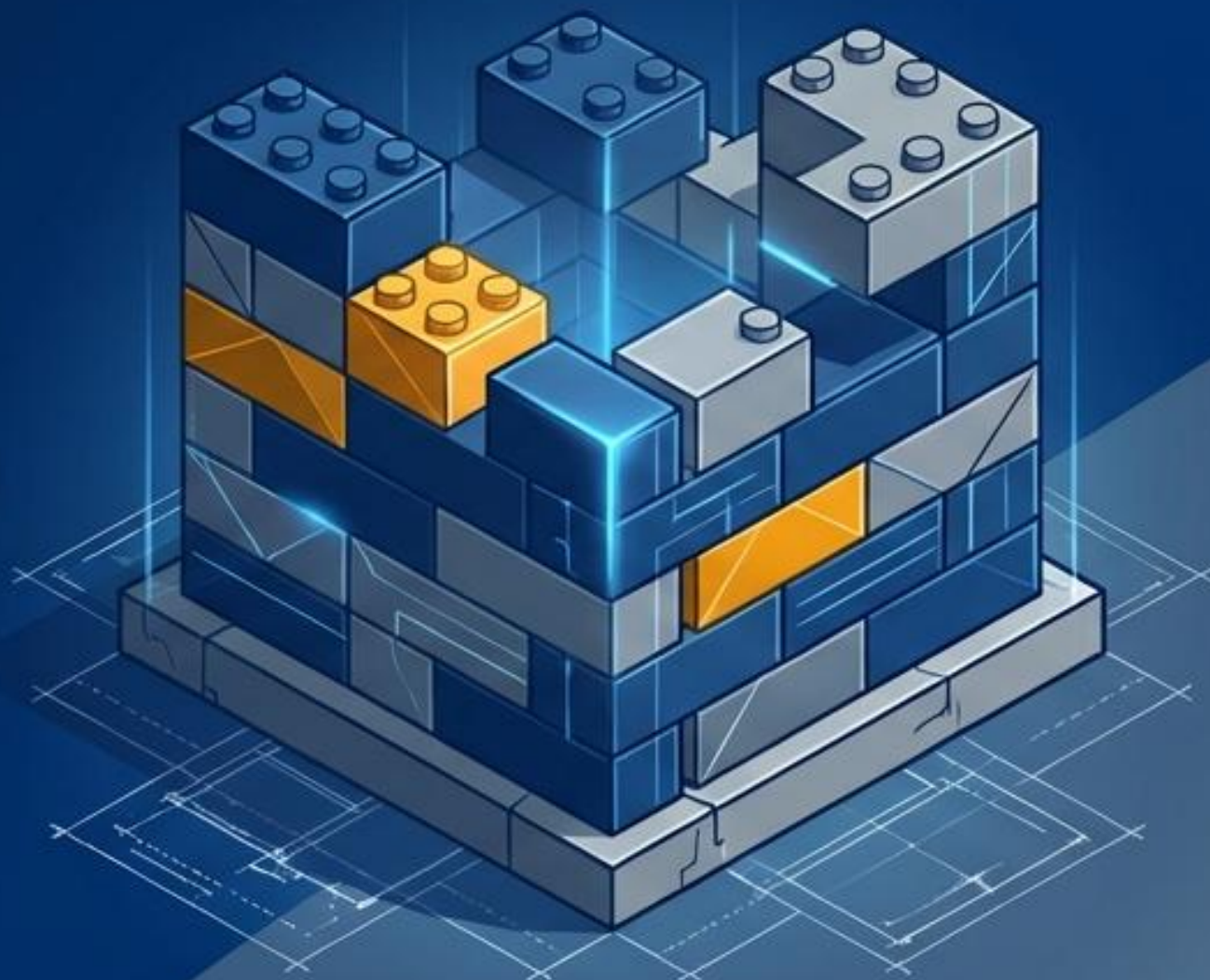


Fáze 2 & 3: Implementace a Dokumentace

Měsíc 2–5

ISMS Strategie

- ISO 27001 jako základ (~70% shoda).
- Doplnění specifik NIS2 (Hlášení incidentů, sankce).



Dokumentace

- Musí odrážet realitu (Zdola nahoru).
- Incident Response Plan, Politika řízení přístupu.

Dokumentace bez evidence = Nesplněno.



Fáze 4 & 5: Lidský faktor a Testování

Měsíc 5–6



Školení

- Statutární orgán: Povinné školení o odpovědnosti.
- Zaměstnanci: Awareness programy, Phishing.



Ověření

- Tabletop cvičení: Simulace ransomware.
- Penetrační testy.
- Test obnovy ze záloh.



Nejčastější chyby (A jak se jim vyhnout)



Dokumentace vs. Realita

Politiky v šuplíku, které nikdo nezná.



Ignorování dodavatelů

50 dodavatelů s přístupem, žádné hodnocení.



Nezájem vedení

Board vnímá bezpečnost jen jako IT problém.



Jednorázový projekt

Čekání na 'hotovo' místo kontinuálního procesu.



Fáze 6: Průběžné udržování



Jak vám pomůže Blue Partners?

Důvěryhodnost a Odbornost

- ✓ Certifikovaní ISMS Lead Auditori
- ✓ 15 let na trhu
- ✓ 150+ klientů

Nabídka

Konzultace zdarma (30 min)

K ničemu se nezavazujete

Zavolejte ještě dnes



+420 602 177 433

Kontaktujte nás ještě dnes pro bezpečnější zítřek.

Registrace byla začátek. Bezpečnost je cíl.

Nejsme jen konzultanti.
Implementujeme, školíme a zůstáváme.

