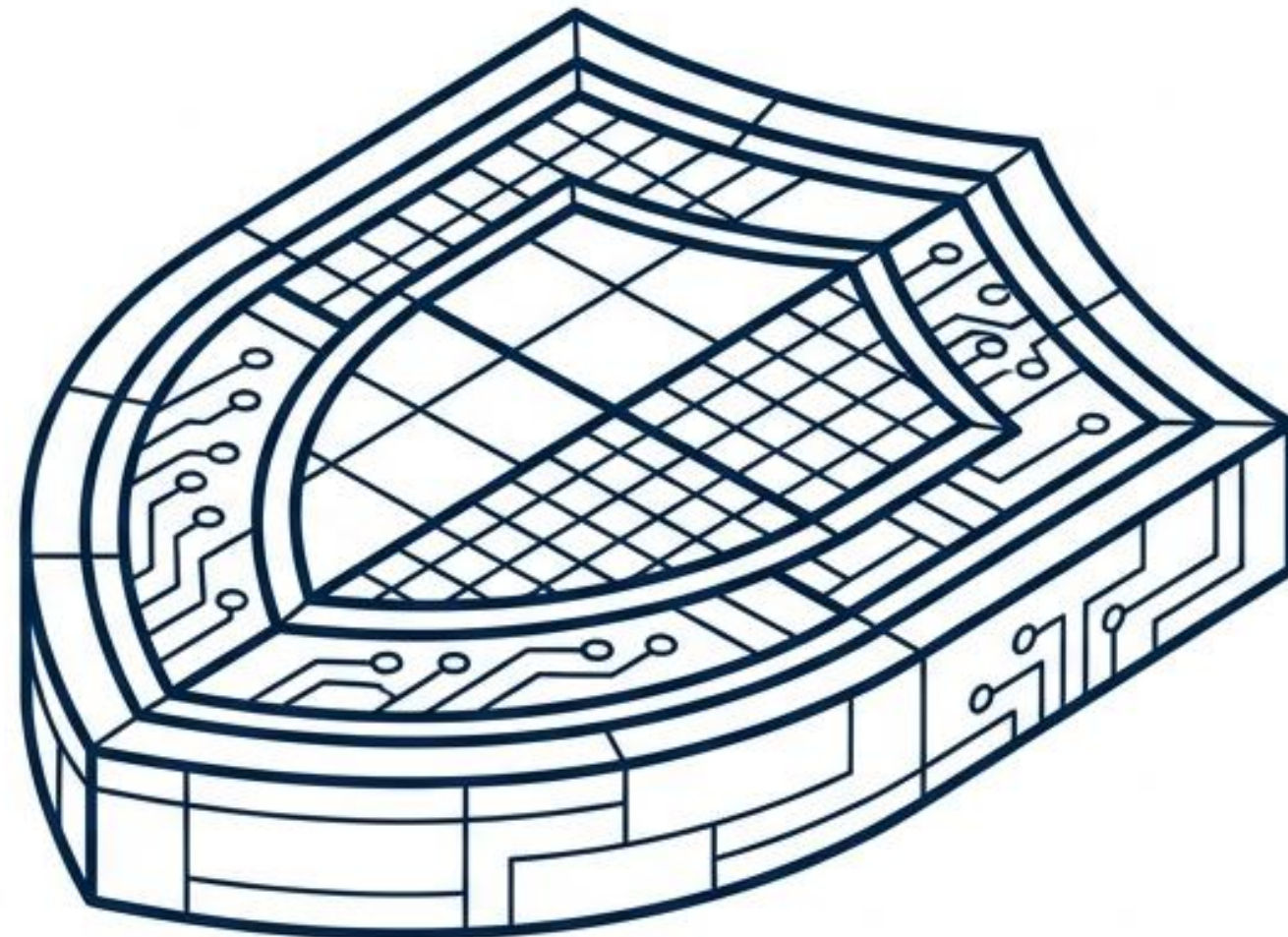




NIS2 CHECKLIST

PRO JEDNATELE A CEO

Zákon č. 264/2025 Sb. — účinný od 1. 11. 2025



ROI ARGUMENT PRO VEDENÍ FIRMY



GAP analýza stojí méně než 0,04% maximální pokuty.

A to počítáme jen pokutu – bez ztráty zakázek, reputační škody nebo dokonce zákazu výkonu funkce

OSOBNÍ ODPOVĚDNOST NELZE DELEGOVAT



Zákon přenáší odpovědnost za kybernetickou bezpečnost přímo na statutární orgán.



- ✗ Nelze plně delegovat na IT oddělení.
- ✗ Nelze plně delegovat na externího správce.

HROZBA: Dočasný zákaz výkonu funkce statutárního orgánu (při závažném/opakovaném porušení).

Průvodce regulací: Spadá vaše firma pod nový zákon o kybernetické bezpečnosti? (Vyhláška č. 408/2025 Sb.)

ZÁKLADNÍ KLÍČ K URČENÍ REGULACE



VELKÝ PODNIK

Podle doporučení Komise 2003/361/ES

Velikost podniku jako hlavní měřítko

Mikropodniky a malé podniky jsou většinou mimo regulaci, pokud nesplňují specifické výjimky.

Vyšší povinnosti dopadají na strategické subjekty s přísnějším dohledem, zatímco nižší povinnosti jsou pro méně kritická odvětví s mírnějším dohledem.



STŘEDNÍ PODNIK

Podle doporučení Komise 2003/361/ES

Rozhodné datum účinnosti: 1. listopadu 2025

SEKTORY A SPECIFICKÉ LIMITY (KDO JE REGULOVÁN?)



ENERGETIKA
(Elektřina)

Režim vyšších povinností

Výroha elektřiny nad 100 MW
nebo velký podnik

Režim nižších povinností

Střední podnik;
Výrobní pod 1 MW z OZE vyjmuty



DIGITÁLNÍ
INFRASTRUKTURA
A TELEKOMUNIKACE

Poskytovatelé s více než
350 000 SIM kartami nebo
100 000 povnými přípojkami
(bez ohledu na velikost)



ZDRAVOTNICTVÍ

Poskytovatelé zdravotní péče
jako velký podnik;
Výrobci kriticky důležitých
zdravotnických prostředků
(střední/velký podnik)



VEŘEJNÁ SPRÁVA

Ministerstva, kraje, ČNB, Policie,
zdravotní pojišťovny

Obce s rozšířenou působností
(ORP), vysoké školy,
Akademie věd



POTRAVINÁŘSTVÍ
A VÝROBA

—

Průmyslová výroba, zpracování,
velkoobchodní distribuce potravin
(střední/velký podnik)

ROZHODOVACÍ TABULKA PRO VYBRANÉ SLUŽBY

Regulovaná služba	Režim vyšších povinností	Režim nižších povinností
Cloud computing	Velký podnik / Státní cloud	Střední podnik
Datová centra	Velký podnik	Střední podnik
Vodní hospodářství	Velký podnik (příjmy > 5 % obratu)	Střední podnik (příjmy > 5 % obratu)
Odpadové hospodářství	—	Střední a velký podnik (> 5 % obratu)
Bankovníctví (Úvěrové inst.)	Velký podnik	Střední podnik
Sociální sítě / On-line tržiště	—	Střední a velký podnik
Letecká doprava	Velký podnik	Střední podnik

SPECIÁLNÍ PŘÍPADY (VŽDY POD REGULACÍ)



KRITICKÁ INFRASTRUKTURA STÁTU

Bez ohledu na velikost do vyššího režimu: Správa železnic, ČEPS, Národní CERT, Elektroenergetické datové centrum



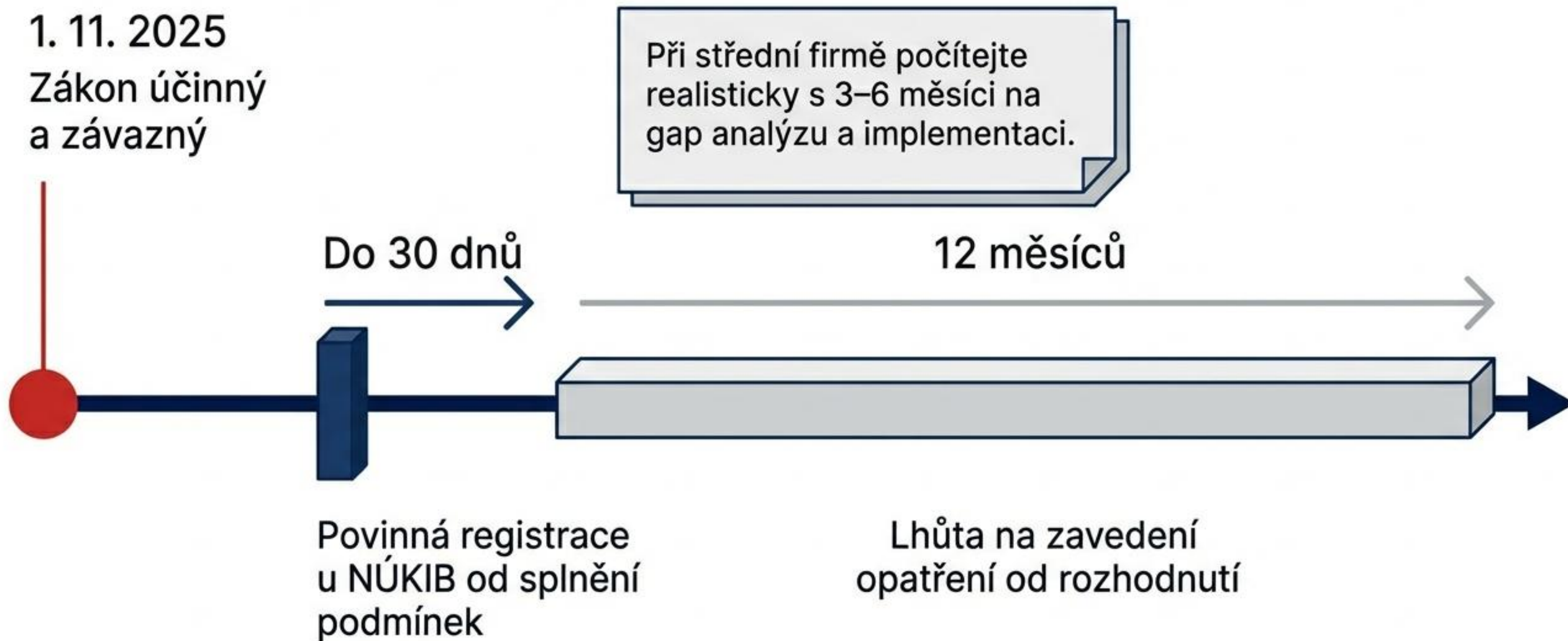
VÝZKUM A VÝVOJ V KRITICKÝCH OBLASTECH

Institute zabývající se AI, kvantovými technologiemi, biotechnologiemi nebo polovodích 5 letech spadají do vyššího (vojenský materiál) nebo nižšího režimu

ORIENTAČNÍ ČASOVÁ OSA



1. 11. 2025
Zákon účinný
a závazný



ÚKOL PRO VEDENÍ: GOVERNANCE A ZDROJE

Priorita: Kritické



Schválit a podepsat bezpečnostní politiku (s datem a podpisem).



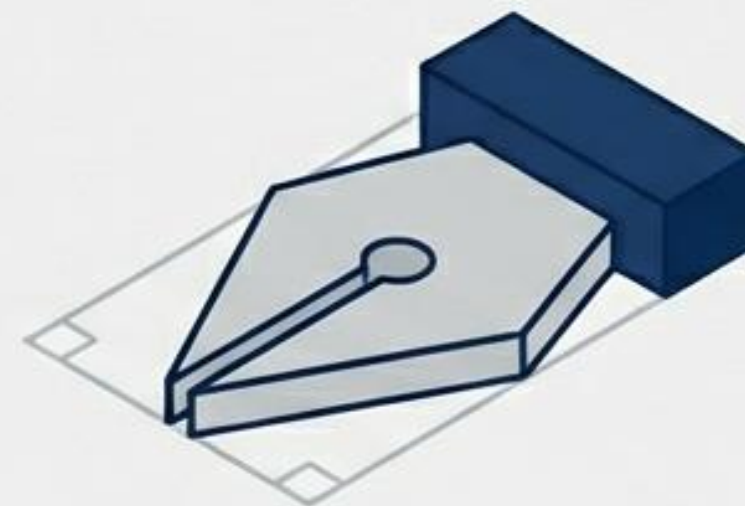
Zajistit alokaci budgetu a lidí (zahrnout do rozpočtu na příští rok).



Jmenovat manažera kybernetické bezpečnosti (CISO) — interní nebo outsourcovaný.



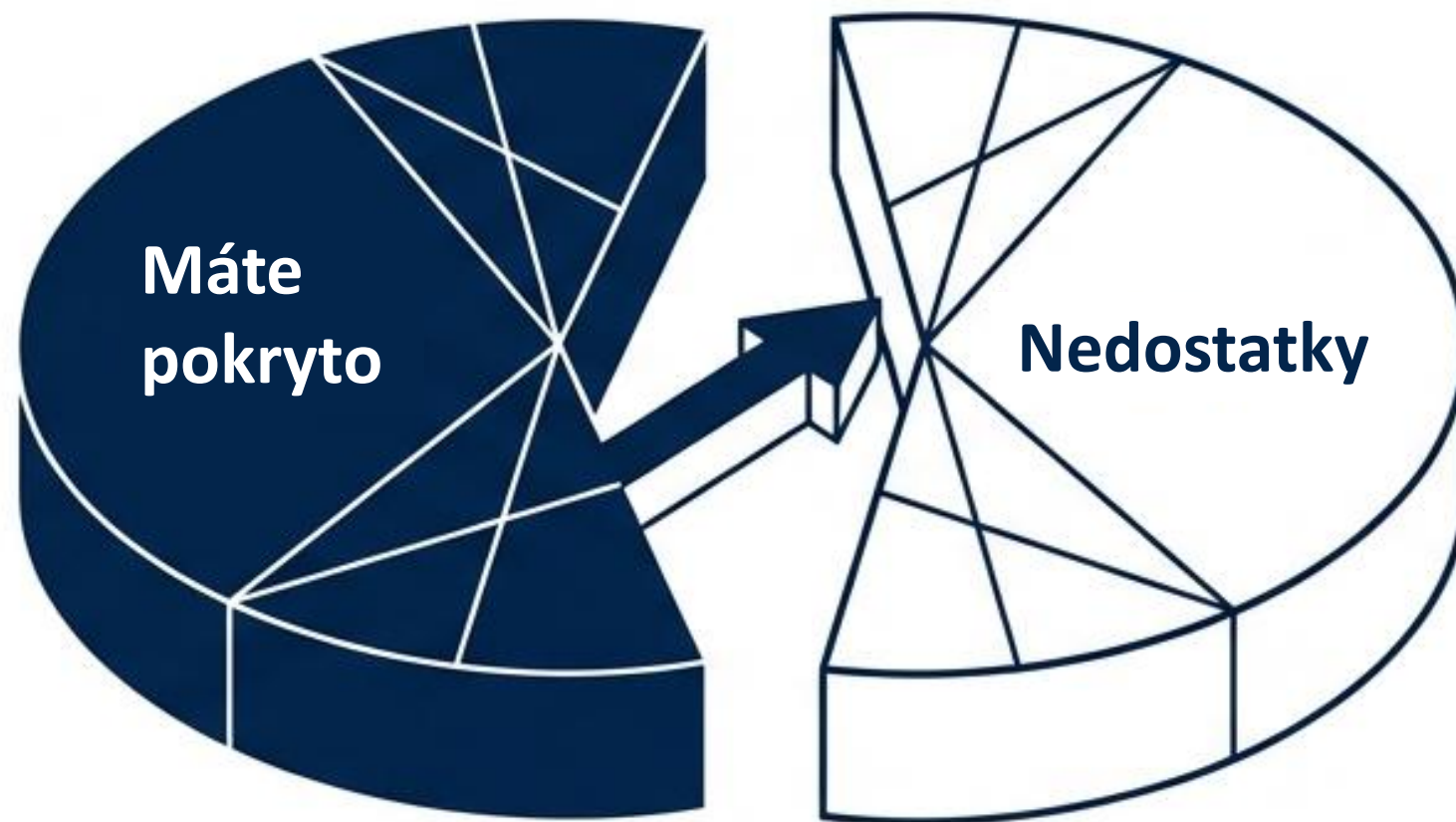
Absolvovat školení kybernetické bezpečnosti pro vedení.





KDE JSME A CO NÁM CHYBÍ? (GAP ANALÝZA)

System řízení bezpečnosti informací (ISMS) je páteří compliance.



- ☐ Provést gap analýzu vůči zákonu a vyhlášce **410/2025 Sb.**
- ☐ Sestavit registr aktiv (HW, SW, data, procesy).
- ☐ Analýza rizik a dopadů na provoz (BIA).
- ☐ Prověřit klíčové dodavatele (Supply chain).

Expert Tip: Bez gap analýzy nevíte, co přesně musíte dořešit. Doporučujeme certifikovaného auditora.



TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ



MFA:
Vícefaktorové
ověřování pro
kritické systémy
(vzdálený
přístup, cloud).



Zálohy:
Pravidlo 3-2-1,
testovat obnovu
min. 2x ročně.



Šifrování:
Přenosy dat a
citlivá data v
klidu (TLS 1.2+,
šifrování disků).



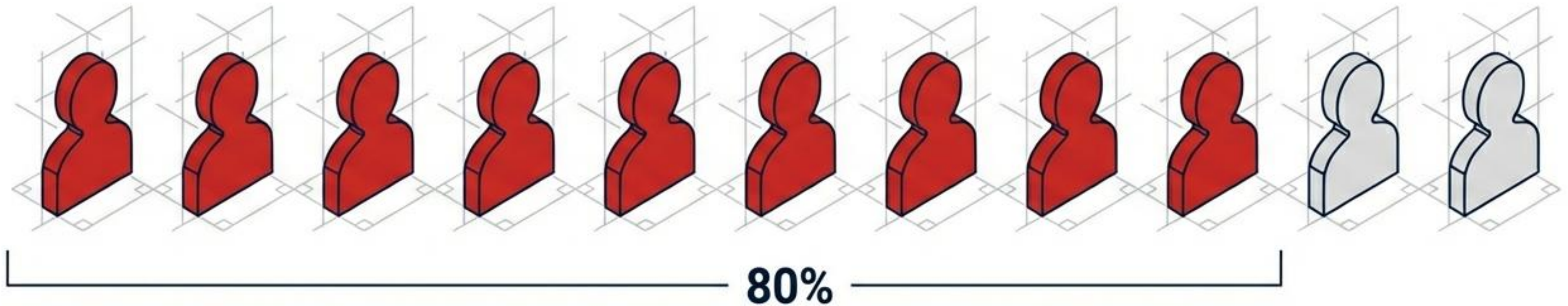
Monitoring:
Logy, SIEM nebo
alternativa pro
detekci
incidentů.



Audit:
Penetrační testy
min. 1x ročně.



LIDSKÝ FAKTOR: 80 % INCIDENTŮ ZAČÍNÁ CHYBOU



Phishing, slabá hesla, neúmyslný únik dat. Školení je efektivní obrana.

- Vstupní školení pro všechny (s certifikátem).
- Pravidelná opakovací školení (min. 1x ročně).
- Simulace phishingových útoků (měřit rizikové skupiny).
- Specializované školení pro IT tým a vedení.



HLÁŠENÍ INCIDENTŮ NÚKIB



◆ **Requirement:** Mít zdokumentovaný proces detekce a klasifikace incidentů.

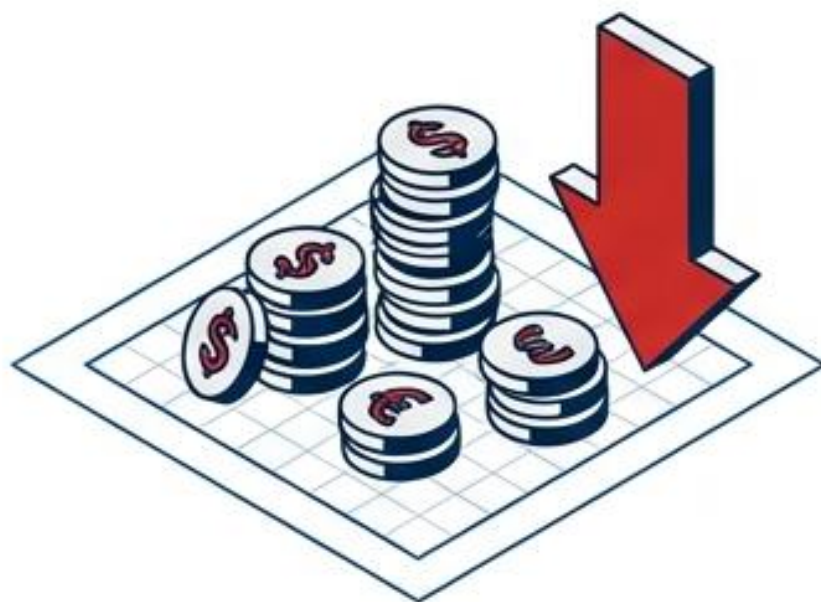
◆ **Note:** Hlášení je povinné i u incidentů dodavatelů.

CO HROZÍ PŘI ZANEDBÁNÍ?



POKUTA

Až 250 000 000 Kč
nebo 2 % celosvětového
obratu (platí vyšší
částka).



ZÁKAZ FUNKCE

Osobní odpovědnost
a zákaz výkonu funkce
pro statutární orgán.



BYZNYS DOPAD

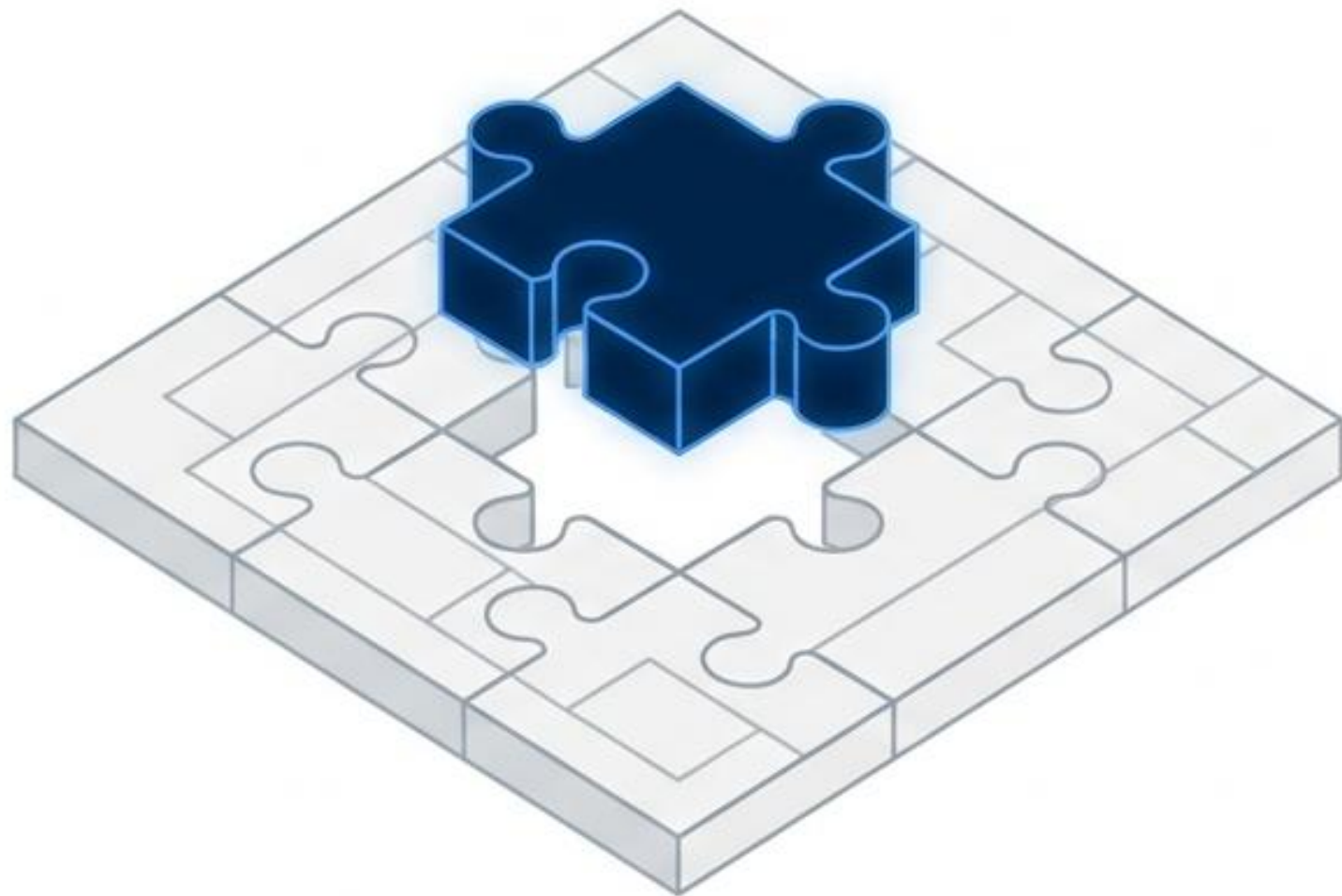
Ztráta reputace,
vyřazení ze supply
chain (banky/investoři
vyžadují compliance).





ZÍSKEJTE PŘESNÝ OBRAZ SITUACE

Tento checklist je orientační. Pro přesnou gap analýzu a plán nápravy kontaktujte certifikovaného ISMS auditora.



- ✓ Certifikovaní ISMS lead auditoři.
- ✓ Minimalizace rizika pokuty a osobní odpovědnosti.
- ✓ Přesný prioritizovaný plán nápravy.



Blue Partners

Váš partner pro NIS2 a kybernetickou bezpečnost

☎ +420 602 177 433

🌐 bluepartners.cz

30min konzultace zdarma, bez závazků.