Co nás čeká nového díky NIS2?

Radek Vostřez, Manager

Management Consulting Cyber Security, KPMG

23.9. 2024

Prezentující

Radek Vostřez

Manager, Management Consulting

Radek má více než 14 let zkušeností v oblasti IT a IT bezpečnosti. Svou kariéru zahájil v akademickém prostředí, kde měl klíčovou roli při založení nového týmu zaměřeného na kybernetickou bezpečnost. Vedl různé projekty týkající se IT sítí a kybernetické bezpečnosti, spolupracoval na projektech v oblasti stavebních investic a vědeckého výzkumu a řídil provoz komplexní datové infrastruktury. V současné době se v KPMG specializuje na komplexní projekty v oblastech kybernetické bezpečnosti a IT technologií. Díky svým znalostem a zkušenostem dokáže poskytnout klientům cenné poznatky a řešení v kritických IT technology and cybersecurity výzvách.

E-mail: rvostrez@kpmg.cz

KPMG

NIS2 a Nový zákon o kybernetické bezpečnosti

Jaká jsou základní fakta NIS2?

Cíl NIS2: Zlepšit odolnost veřejných a soukromých subjektů, příslušných orgánů a EU jako celku v oblasti kybernetické bezpečnosti a schopnost reagovat na bezpečnostní incident.

- 27.12. 2022 bylo **zveřejněno finální přijaté znění směrnice NIS2** (jedná se o revizi směrnice NIS z roku 2016).
- NIS2 stanovuje **minimální pravidla** týkající se regulačního rámce a mechanismy účinné spolupráce mezi příslušnými subjekty v každém členském státě.
- **Zpřísňuje** a zefektivňuje požadavky na kybernetickou bezpečnost.
- Zavádí přísnější opatření dohledu pro vnitrostátní orgány a přísnější požadavky na vymáhání a usiluje o harmonizaci sankčních režimů mezi členskými státy.
- Každý členský stát má povinnost přijmout národní strategii kybernetické bezpečnosti, ve které vymezí strategické cíle a příslušná politická a regulační opatření s cílem dosáhnout vysoké úrovně kybernetické bezpečnosti a udržovat ji.

NIS 2 nabyla účinnosti 16. ledna 2023

- Požadavky, které NIS2 přináší, budou promítnuty v **novém zákoně o kybernetické bezpečnosti** (NZoKB) a v s ním souvisejících **vyhláškách**.

Jaká jsou základní fakta NZoKB?

Cíl NZoKB : Transpozice směrnice NIS 2; fungující systém kybernetické bezpečnosti v ČR; stanovení minimálních požadavků na standardní zabezpečení poskytovatelů regulovaných služeb; zavedení funkčního a efektivního mechanismu prověřování bezpečnosti dodavatelského řetězce.

- V ČR je problematika KB komplexně řešena od roku 2015 (účinnost 1. znění ZoKB).
- 2017 - 2 stěžejní novelizace (nový institut tzn. provozovatele systému; komplexní novela transponující do zákona obsah směrnice NIS).
- Po novele regulováno přibližně 400 orgánů a osob.
- NZoKB odstraňuje dosavadní rozlišování povinných osob – nově pouze **poskytovatel regulované služby.**
- V souhrnu nárůst povinných osob minimálně 15násobný oproti současnému stavu.
- Poskytovatelé RS jsou **povinni dodržovat bezpečnostní opatření** (organizační a technická), v režimu vyšších či nižších povinností.
- Posiluje se řízení bezpečnosti a **odpovědnosti vedoucích pracovníků podniku –** nově např. povinnost vzdělávání vrcholového vedení organizace.

Předpoklad účinnosti NZoKB léto 2025

(dle NIS2 od 18. 10. 2024)

Na koho NZoKB dopadá?

Na subjekty, které poskytují službu/y v některém z následujících odvětví a splňují kritérium významnosti:

- Veřejná správa a výkon veřejné moci
- Energetika – Elektřina
- Energetika – Ropa a ropné produkty
- Energetika – Plynárenství
- Energetika – Teplárenství
- Energetika – Vodík
- Obranný průmysl
- Výrobní průmysl
- Potravinářský průmysl
- Chemický průmysl
- Vodní hospodářství
- Vesmírný průmysl
- Letecká doprava
- Drážní doprava
- Vodní doprava
- Silniční doprava
- Odpadové hospodářství
- Digitální infrastruktura a služby
- Finanční trh
- Zdravotnictví
- Věda, výzkum a vzdělávání
- Poštovní a kurýrní služby

Jaká jsou požadovaná bezpečnostní opatření RS?

Vyšší povinnosti

Organizační opatření

- systém řízení bezpečnosti informací,
- požadavky na vrcholné vedení,
- stanovení bezpečnostních rolí,
- řízení bezpečnostní politiky a bezpečnostní dokumentace,
- řízení aktiv,
- řízení rizik,
- řízení dodavatelů,
- bezpečnost lidských zdrojů,
- řízení změn,
- akvizice, vývoj a údržba,
- řízení přístupu,
- zvládání kybernetických bezpečnostních událostí a incidentů,
- řízení kontinuity činností a
- provádění auditu kybernetické bezpečnosti,

Technická opatření

- fyzická bezpečnost,
- bezpečnost komunikačních sítí,
- správa a ověřování identit,
- řízení přístupových práv a oprávnění,
- detekce kybernetických bezpečnostních událostí,
- zaznamenávání událostí,
- vyhodnocování kybernetických bezpečnostních událostí,
- aplikační bezpečnost,
- kryptografické algoritmy,
- zajišťování dostupnosti regulované služby a
- zabezpečení průmyslových, řídících a obdobných specifických technických aktiv.

Nižší povinnosti

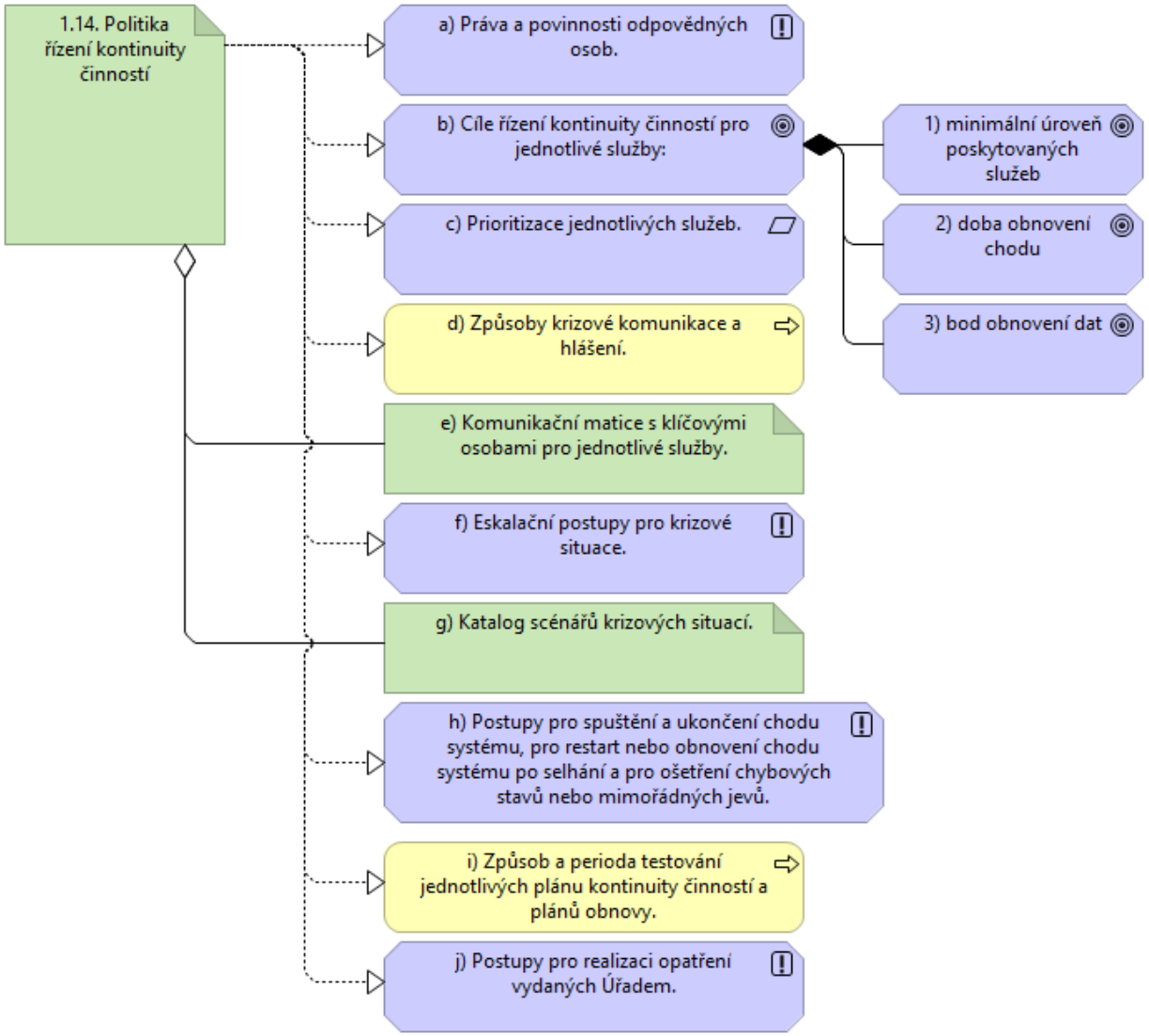
Organizační a technická opatření

- systém zajišťování minimální kybernetické bezpečnosti,
- požadavky na vrcholné vedení,
- řízení aktiv,
- řízení rizik,
- bezpečnost lidských zdrojů,
- řízení kontinuity činností,
- řízení přístupu,
- řízení identit a jejich oprávnění,
- detekce a zaznamenávání kybernetických bezpečnostních událostí,
- řešení kybernetických bezpečnostních incidentů,
- bezpečnost komunikačních sítí,
- aplikační bezpečnost a
- kryptografické algoritmy.

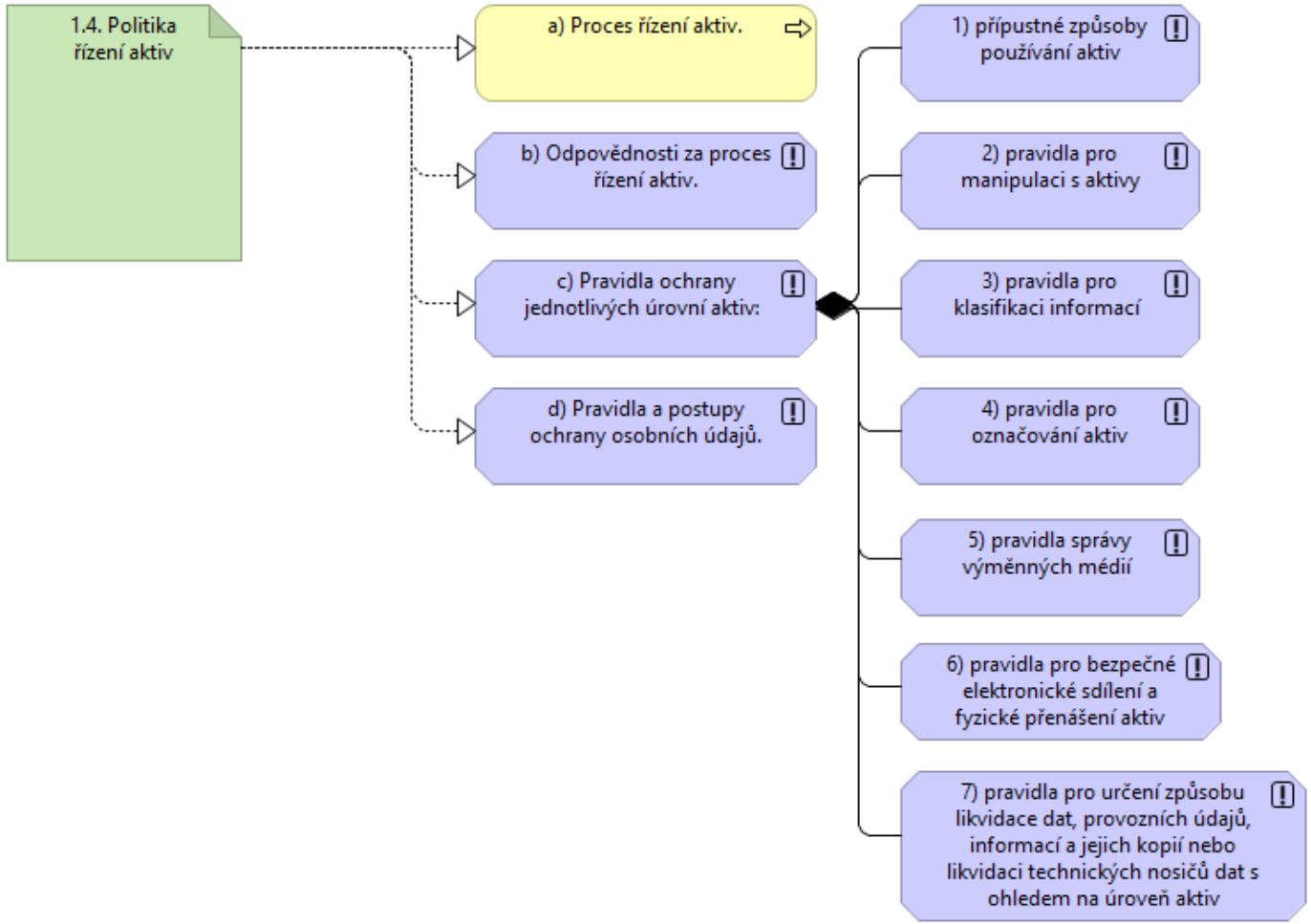
Typické dopady NZoKB do organizace

- Identifikace aktiv, posouzení souvislostí aktiv s RS, určení podpůrných aktiv u primárních aktiv souvisejících s RS, **stanovení rozsahu řízení kybernetické bezpečnosti dle zákona**
- Přezkum a aktualizace bezpečnostních politik a bezpečnostní dokumentace, zavedení nových procesů vycházejících z aktualizovaných bezpečnostních opatření
- Aktualizace procesu řízení aktiv a rizik – aktualizace analýzy rizik a plánu zvládání rizik
- Zapojení vedení společnosti, zajištění školení zaměstnanců a vrcholového vedení
- Nové nastavení procesu kontinuity, komplexnější plány kontinuity a plány obnovy, řízení kontinuity a obnovy i u dodavatelů
- Revize systému a procesu řízení bezpečnostních incidentů a nastavení reportingu
- Aktualizace procesu řízení bezpečnosti dodavatelů/subdodavatelů – bezpečnostní prověrky/hodnocení rizik souvisejících s dodavateli, nová smluvní ujednání/aktualizace, provádění kontroly zavedení bezpečnostních opatření

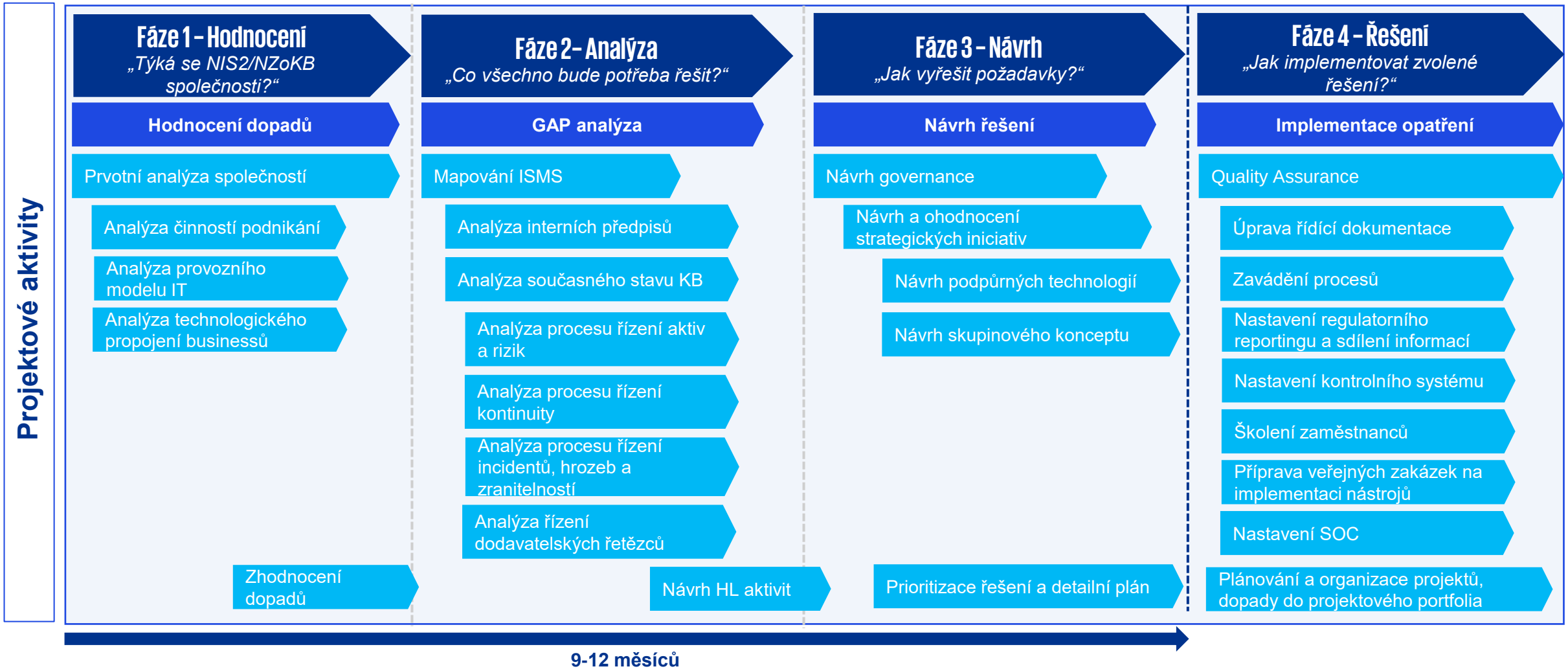
Příklady požadavků na politiky dle NZoKB (vyhlášky)



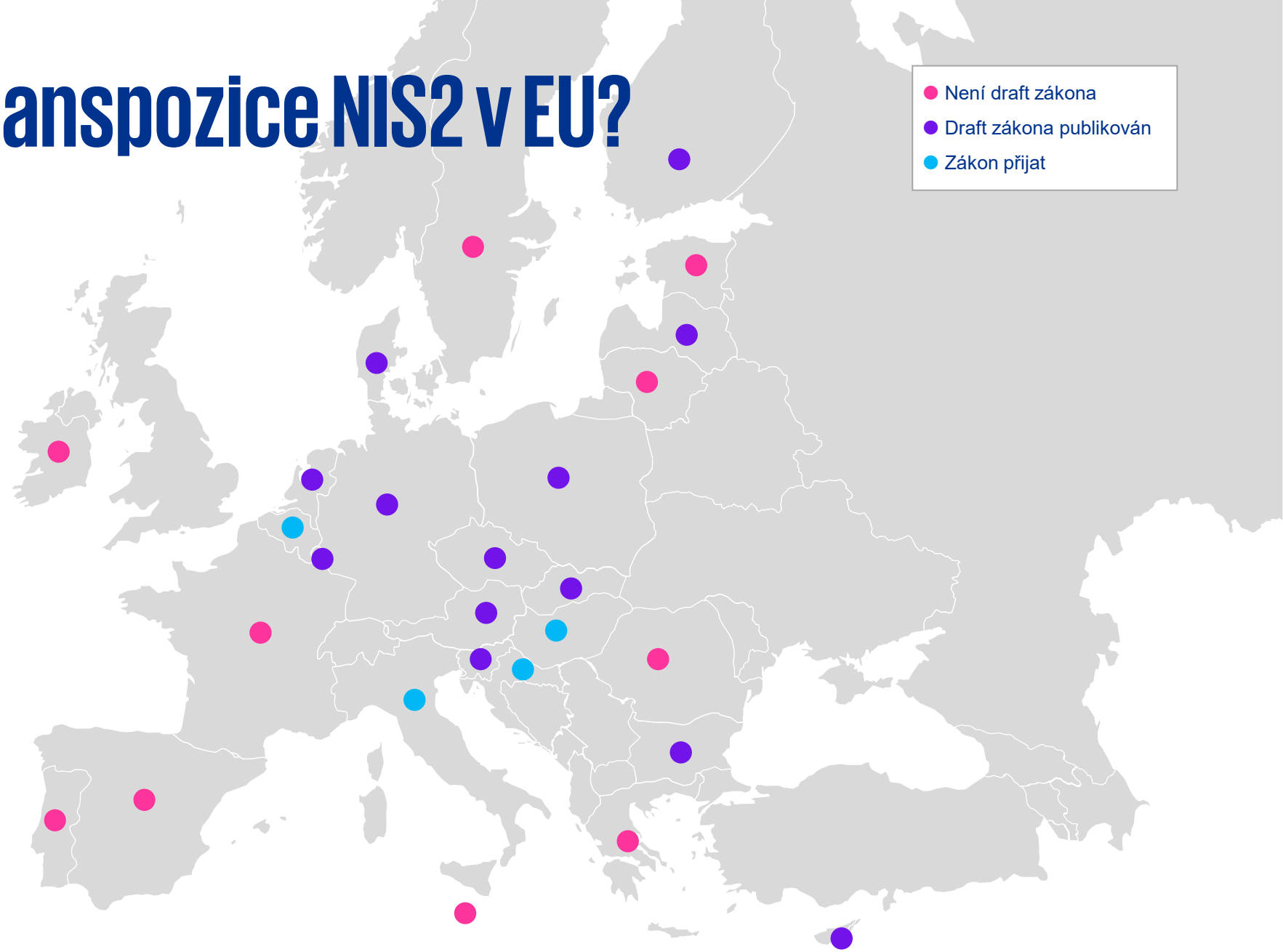
Příklady požadavků na politiky dle NZoKB (vyhlášky)



KPMG přístup k řešení NIS2/NZoKB v organizaci



Jaký je stav transpozice NIS2 v EU?



60+ NIS-2 specialistů

V KPMG vznikla nadnárodní skupina odborníků na NIS 2 spolupracující na podpoře mezinárodních společností v celé EU při plnění požadavků směrnice NIS 2.

Expertní tým

Naši specialisté NIS 2 jsou podporováni konzultanty v oblasti kybernetické bezpečnosti a řízení rizik z různých oborů, od bezpečnosti IT přes regulaci až po forenzní analýzu, kteří spolupracují na podpoře našich klientů.