Zajištění kybernetické bezpečnosti a požadavků nového ZoKB

KPMG

Aktuality z tábora interního auditu

1-2. listopadu 2023,Tábor

LH Hotel Dvořák Tábor

Základní fakta o NIS2

Cíl NIS 2: Zvýšit odolnost veřejných a soukromých subjektů, příslušných orgánů a EU jako celku v oblasti kybernetické bezpečnosti a zlepšit schopnost reagovat na bezpečnostní incident.

- **Úřední věstník Evropské unie zveřejnil finální přijaté znění směrnice NIS2 dne 27. 12. 2022** (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 i požadavky na vymáhání. Usiluje také 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. Cílem je dosažení a následné udržení vysoké úrovně kybernetické bezpečnosti.
- Požadavky NIS2 se promítnou v **novém zákoně o kybernetické bezpečnosti** a s ním souvisejících **vyhláškách**.

NIS 2 nabyla účinnosti 16. ledna 2023

Základní fakta nový ZoKB

Cíl NZoKB : Transpozice směrnice NIS2; 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 – dvě stěžejní novelizace (nový institut tzn. provozovatele systému; komplexní novela transponující do zákona obsah směrnice NIS).
- Po novele zákon reguluje přibližně 400 orgánů a osob.
- NZoKB odstraňuje dosavadní rozlišování povinných osob a sdružuje je pouze do jedné – **poskytovatel regulované služby.**
- Souhrnně narostl počet povinných osob minimálně patnáctinásobně oproti současnému stavu.
- Poskytovatelé RS jsou povinni dodržovat bezpečnostní opatření (organizační a technická), v režimu vyšších či nižších povinností.
- NZoKB dále definuje povinnosti pro poskytovatele strategicky významné služby (narušení by mohlo způsobit závažný dopad na bezpečnost ČR nebo vnitřní či veřejný pořádek).
- Posiluje se řízení bezpečnosti a **odpovědnosti vedoucích pracovníků podniku –** nově např. povinnost vzdělávání vrcholového vedení organizace.

Předpokládaný termín nabytí účinnosti: 18. říjen 2024

KPMG

Bezpečnostní opatření dle vyhlášek

Bezpečnostní opatření

Vyšší povinnosti

Organizační opatření:

- systém řízení bezpečnosti informací,
- povinnosti vrcholného vedení,
- bezpečnostní role,
- 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 kybernetických bezpečnostních incidentů,
- řízení kontinuity činností,
- audit kybernetické bezpečnosti.

Technická opatření:

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

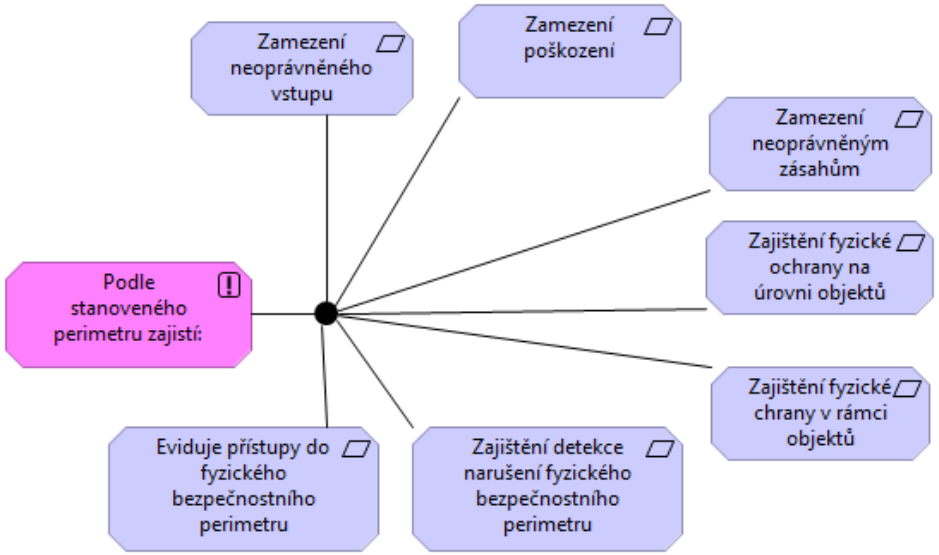
Nižší povinnosti

Organizační a technická opatření

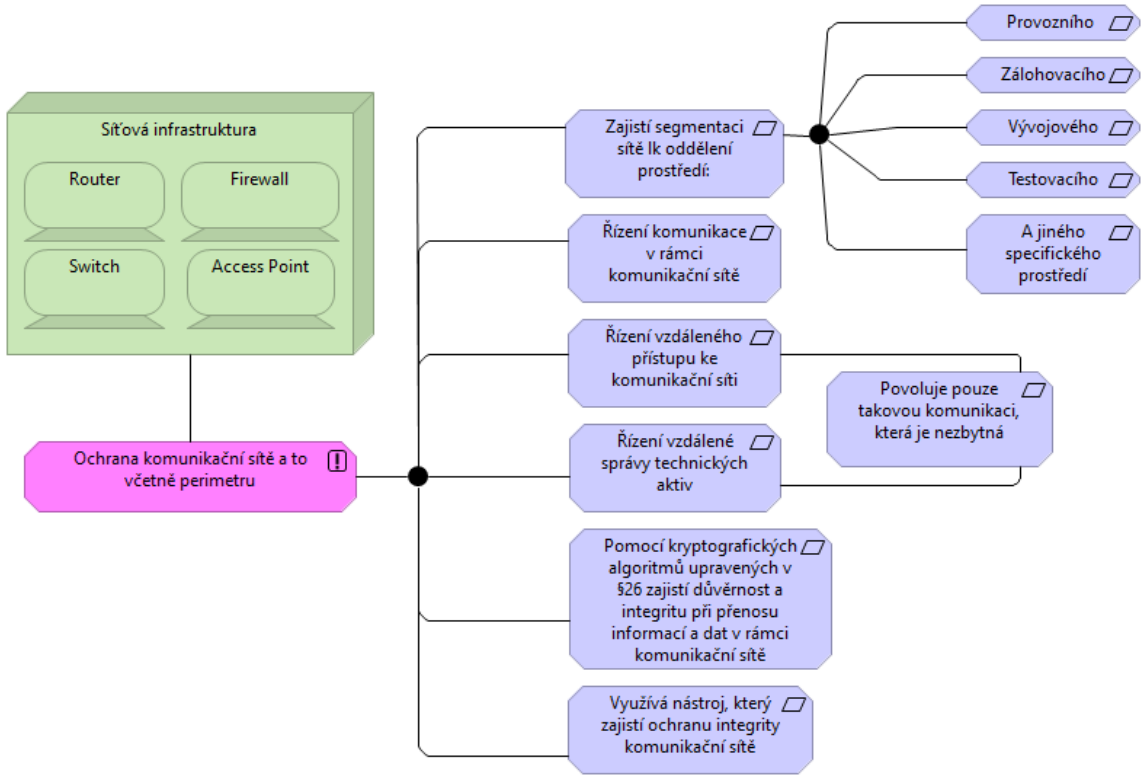
- zajišťování minimální úrovně kybernetické bezpečnosti,
- povinnosti vrcholného vedení,
- řízení aktiv,
- řízení rizik,
- bezpečnost lidských zdrojů,
- řízení kontinuity činností,
- řízení přístupu,
- řízení identit a jejich oprávnění,
- detekce a zaznamenávání kybernetických bezpečnostních událostí,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

Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností Hlava II, Technická opatření

§18 - Fyzická bezpečnost

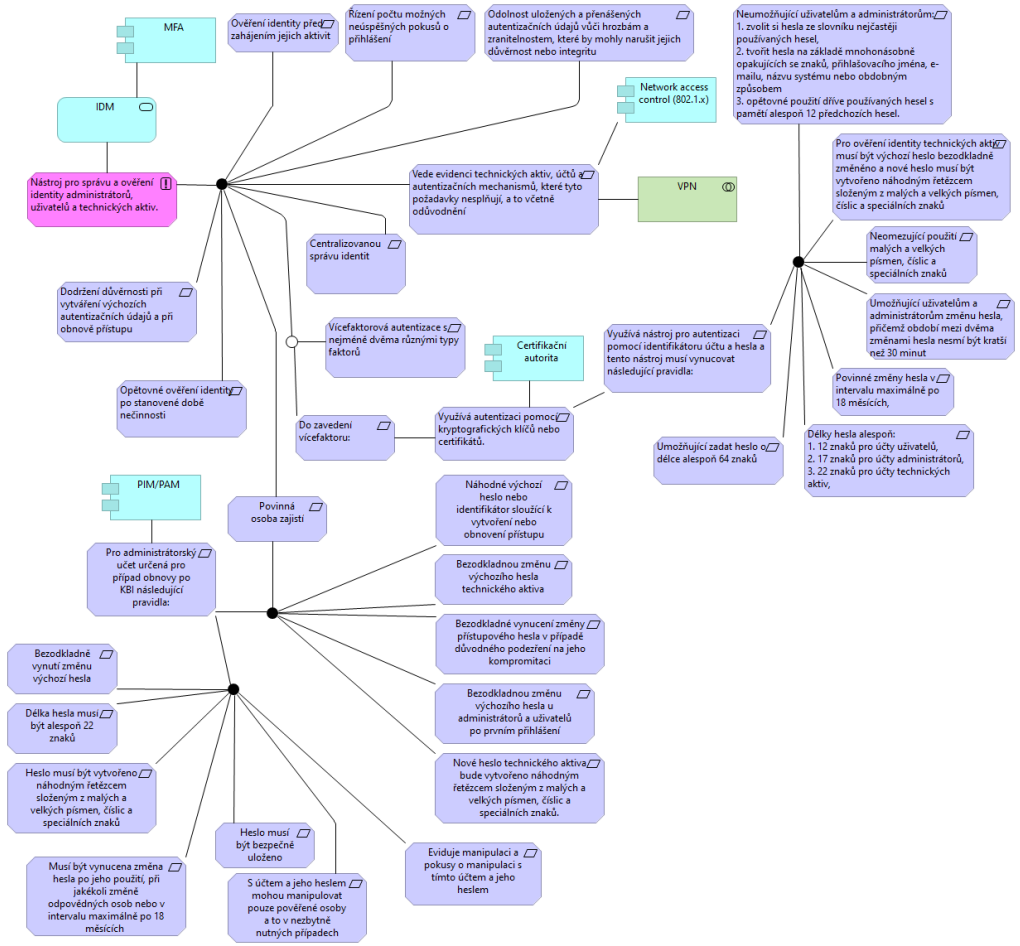


§19 - Bezpečnost komunikačních sítí

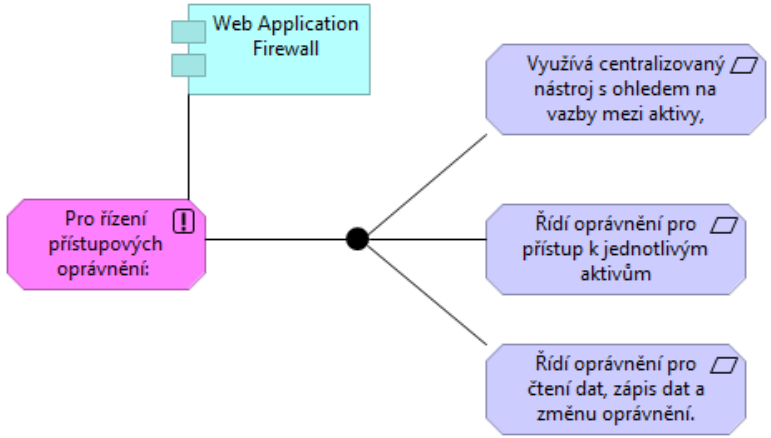


Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností Hlava II, Technická opatření

§20 - Správa a ověřování identit

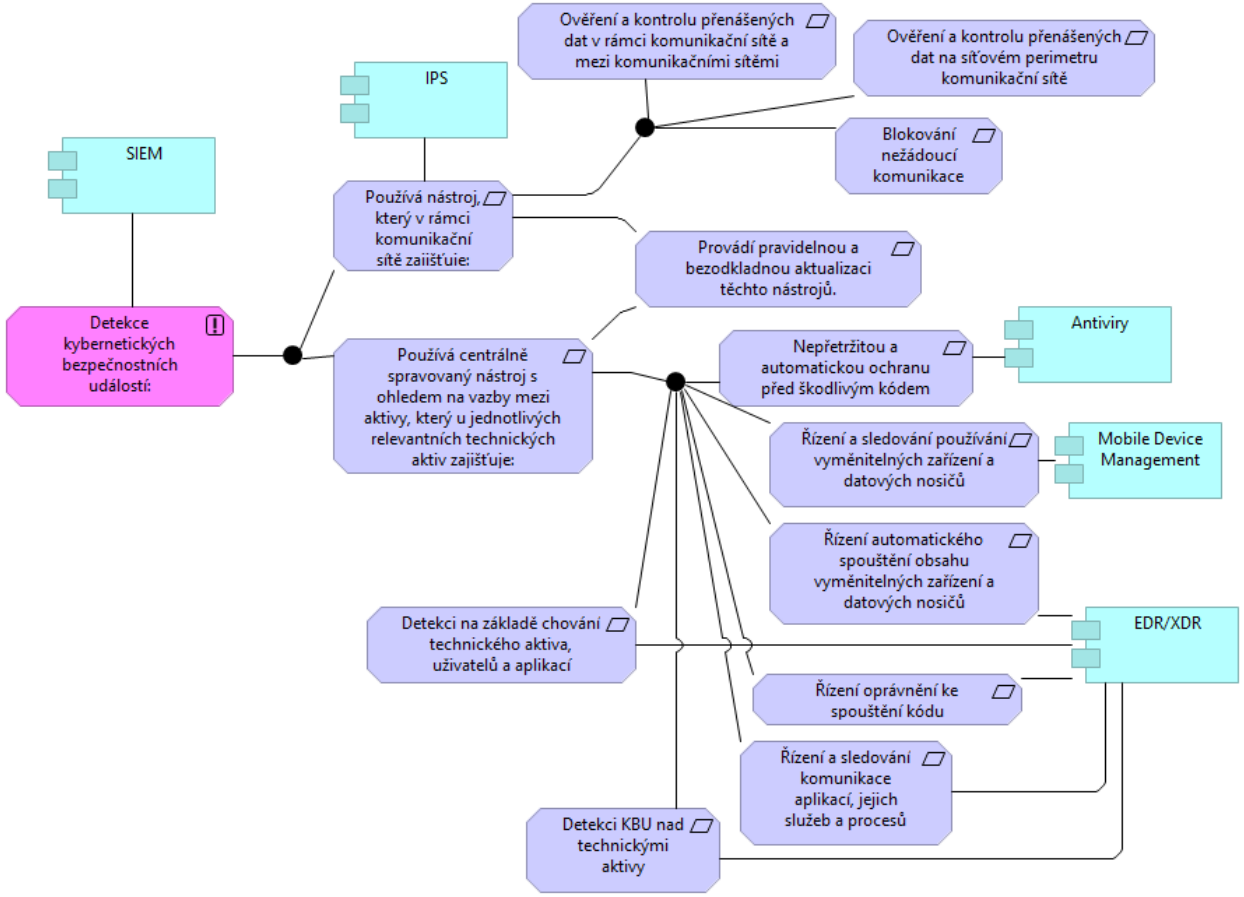


§21 - Řízení přístupových oprávnění



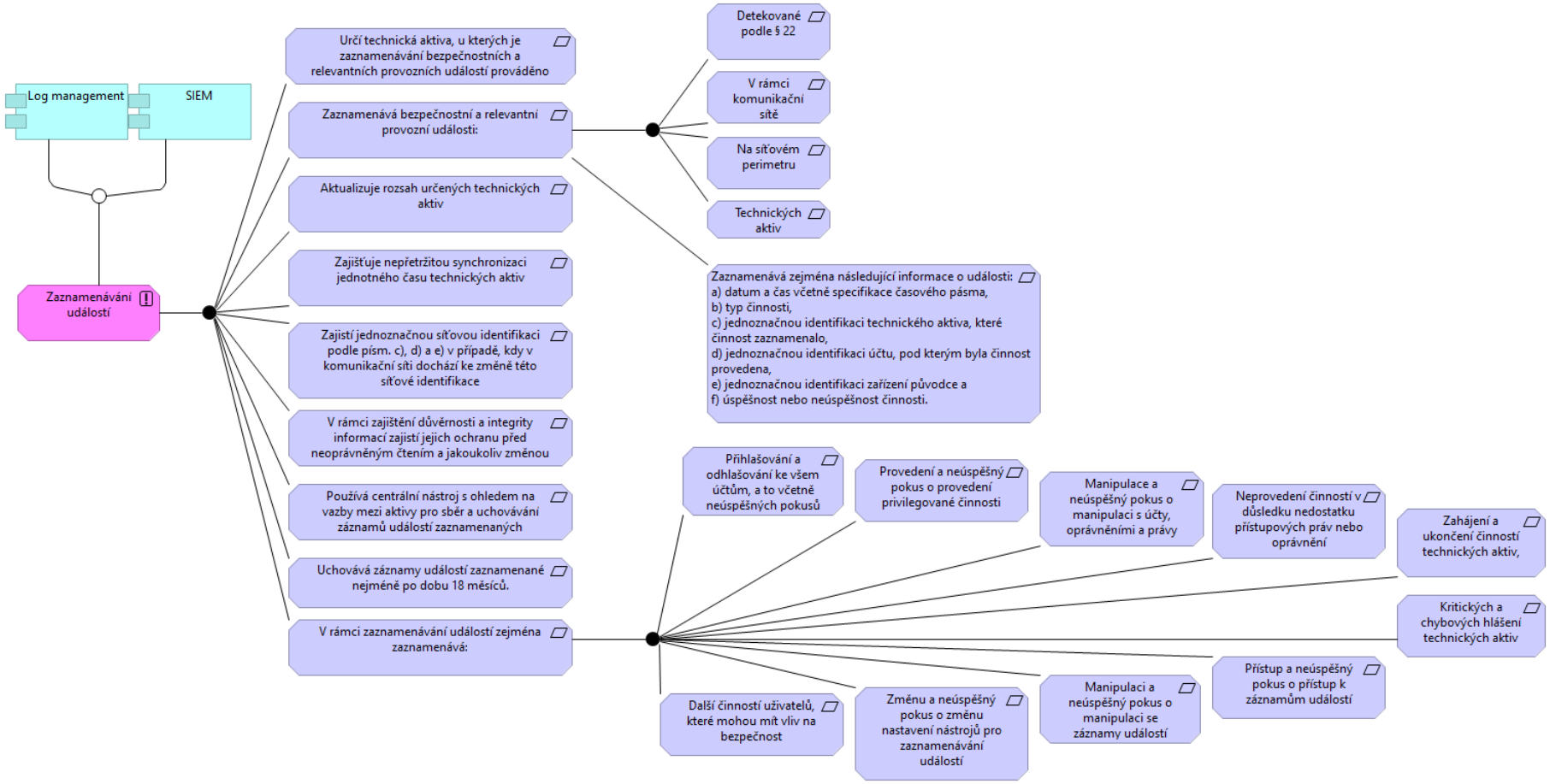
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností Hlava II, Technická opatření

§22 - Detekce kybernetických bezpečnostních událostí



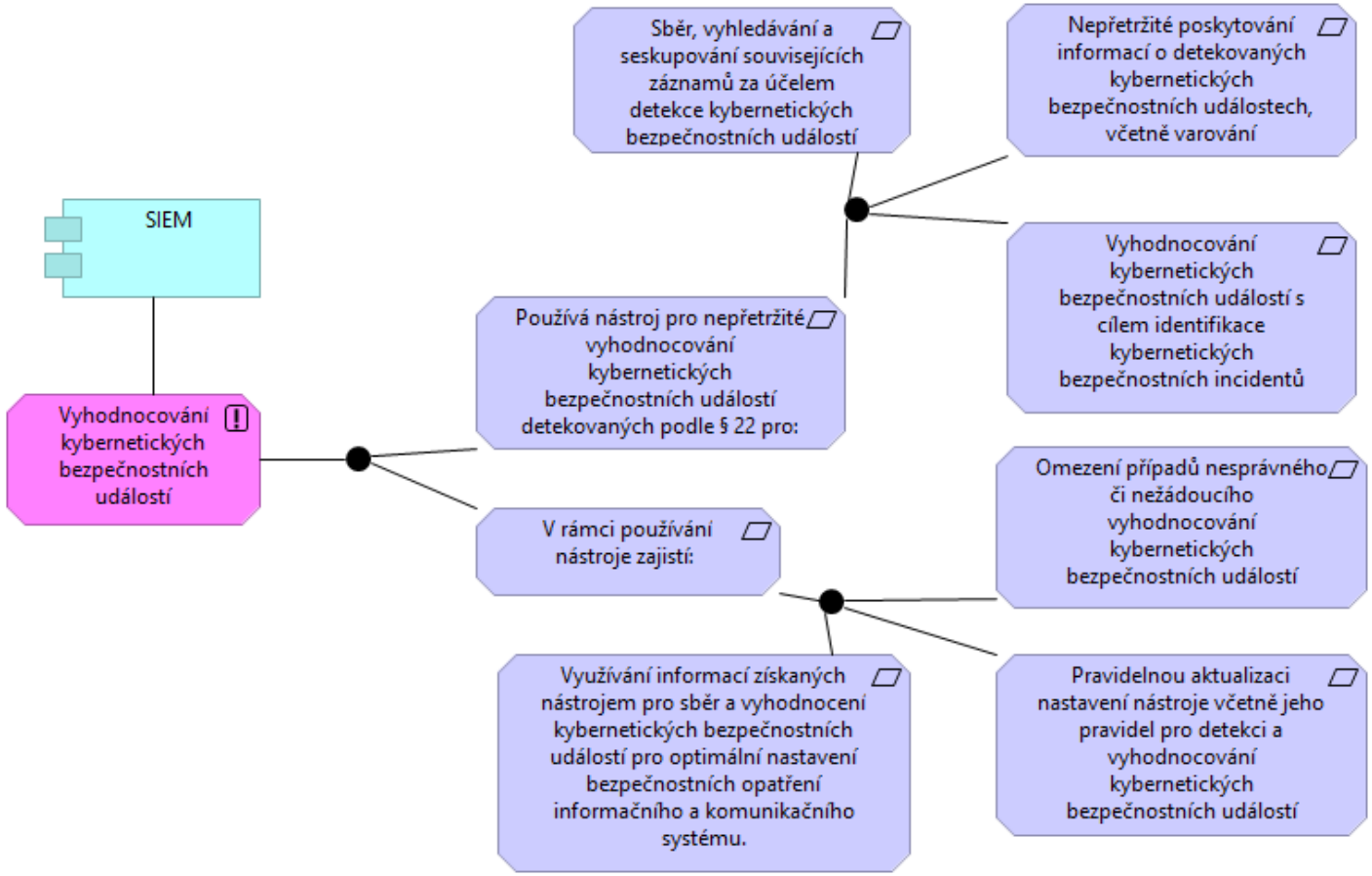
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností Hlava II, Technická opatření

§23 - Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů



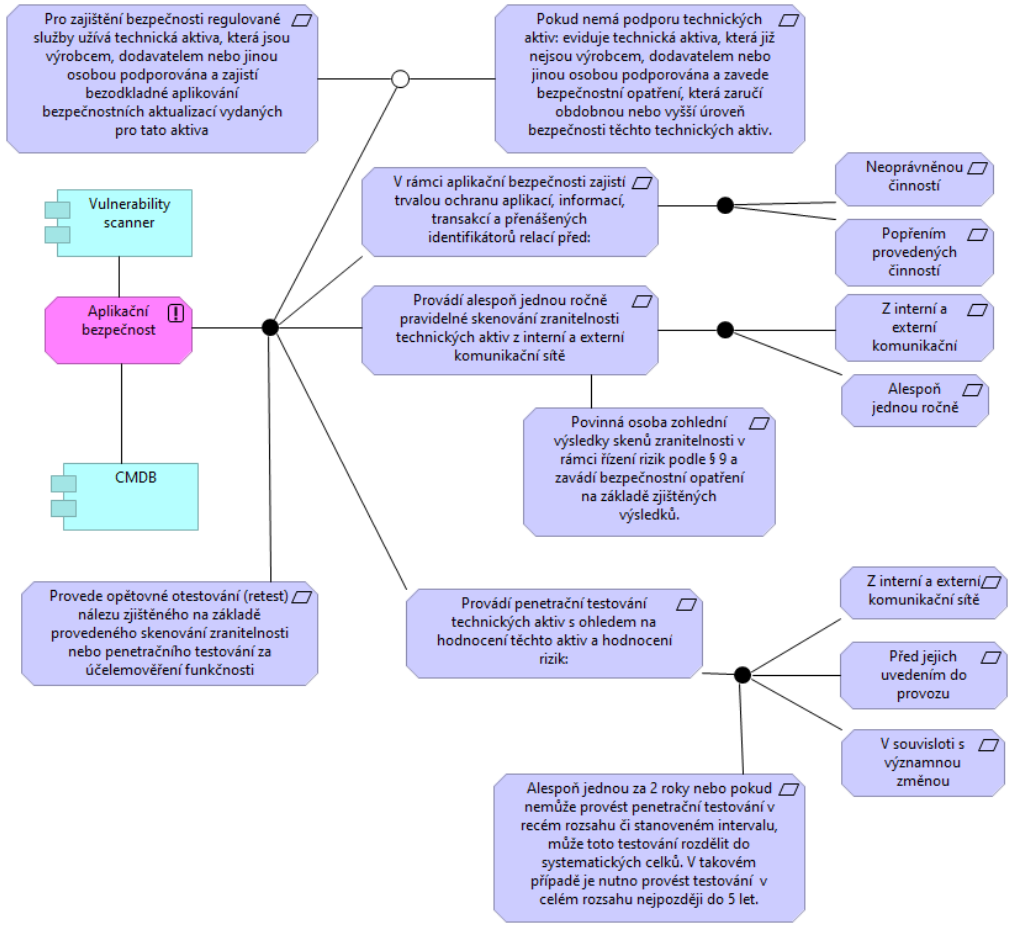
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností Hlava II, Technická opatření

§24 - Sběr a vyhodnocování kybernetických bezpečnostních událostí



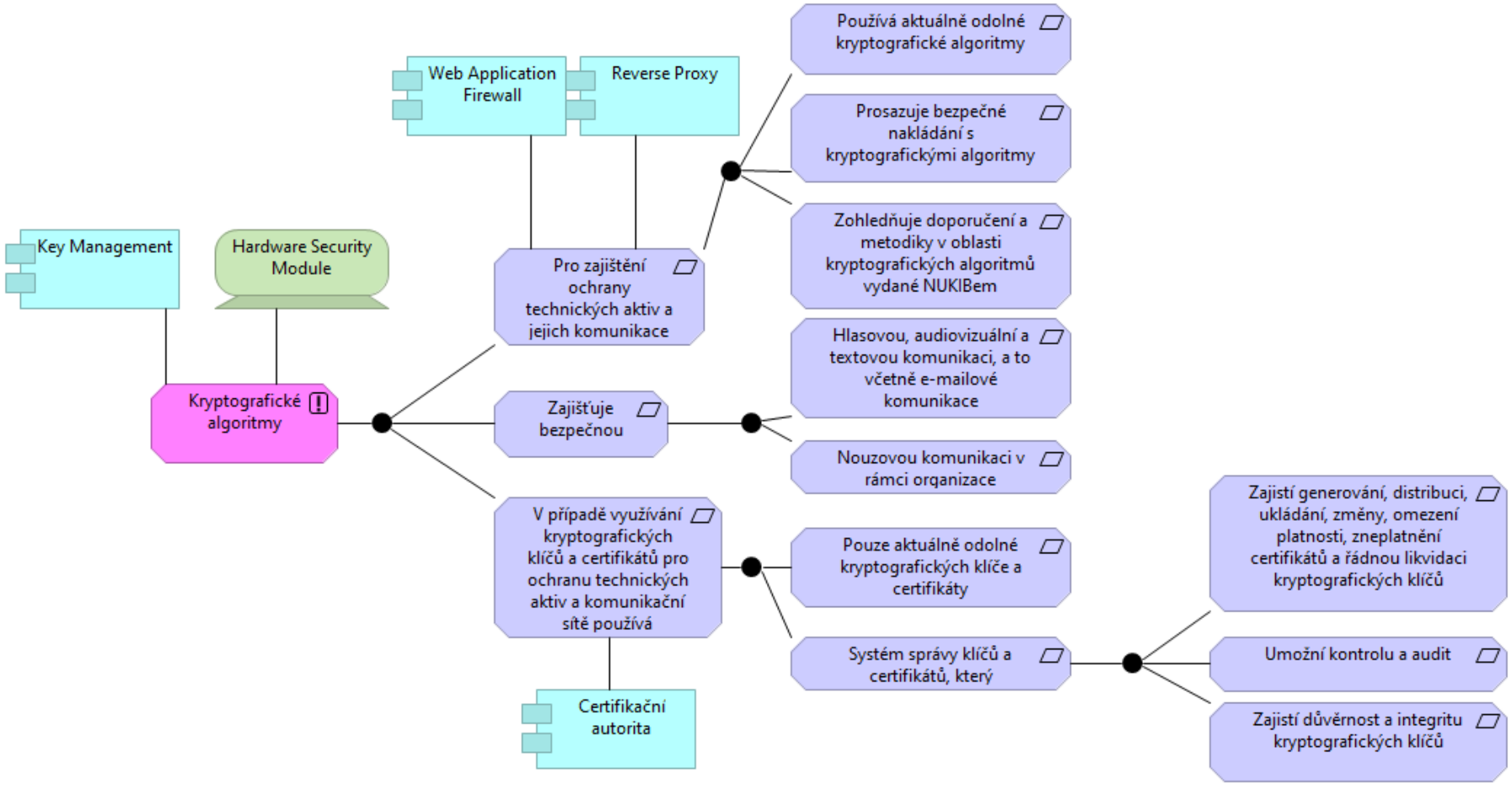
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností Hlava II, Technická opatření

§25 - Aplikační bezpečnost



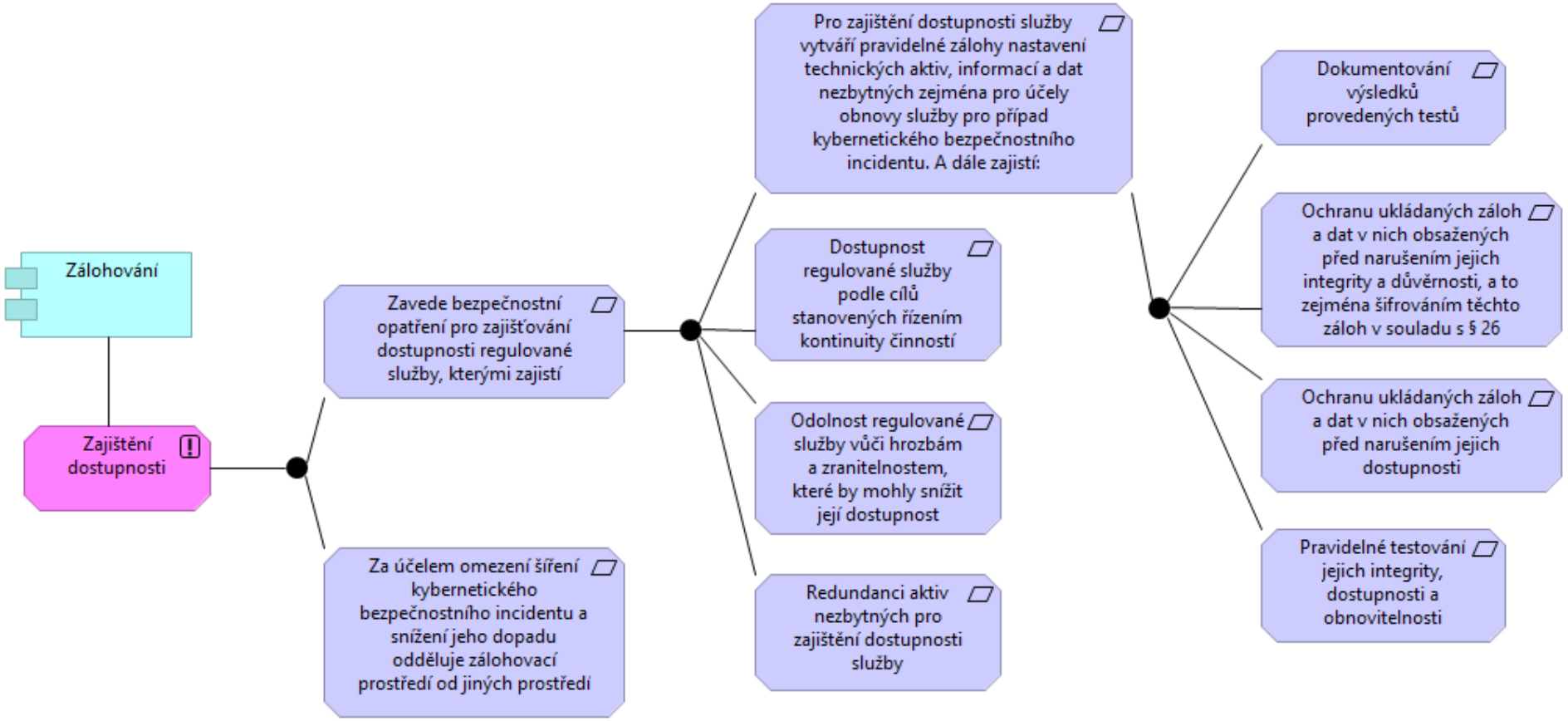
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností Hlava II, Technická opatření

§26 - Kryptografické algoritmy



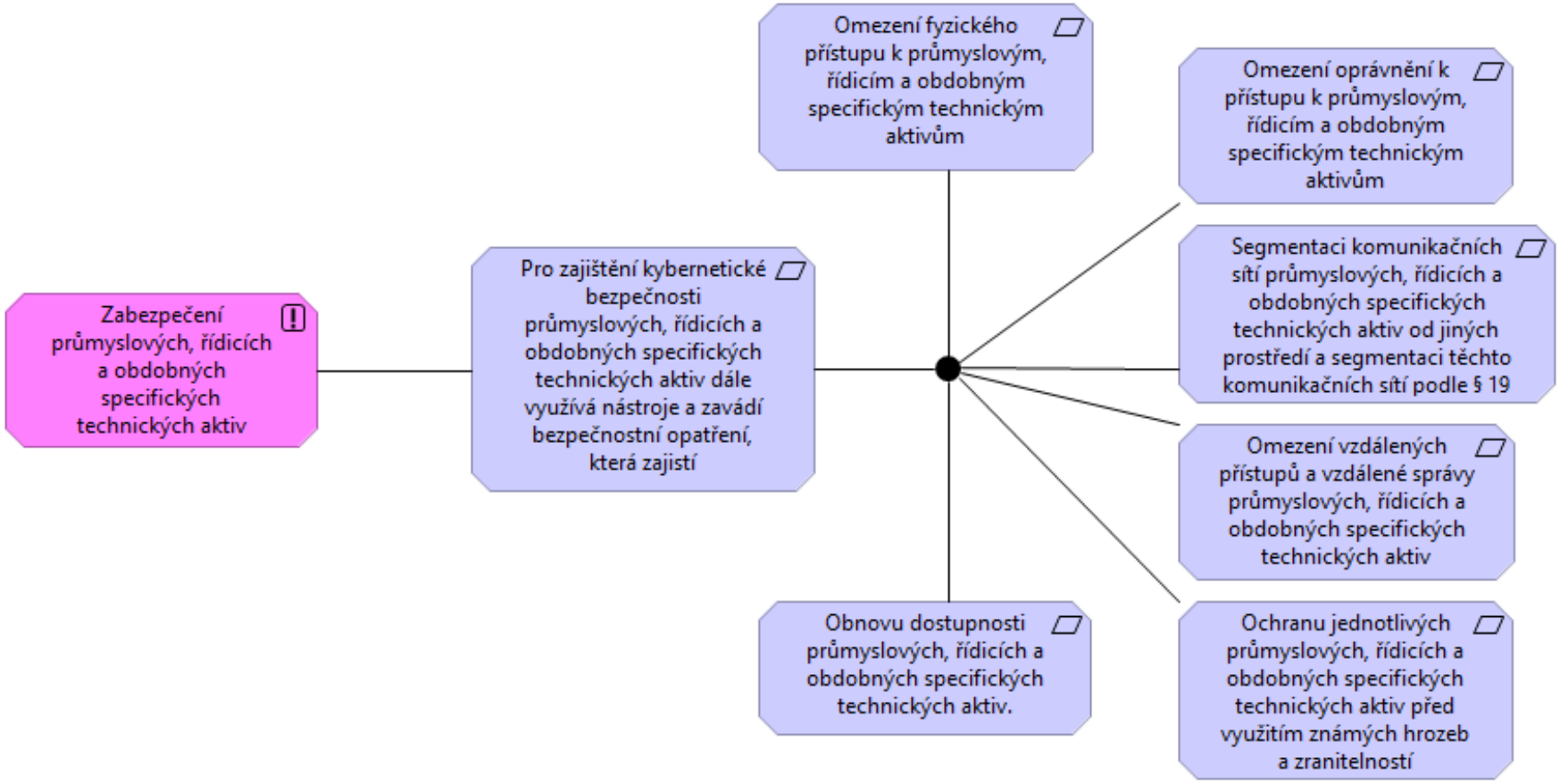
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností Hlava II, Technická opatření

§27 - Zajištění dostupnosti regulované služby



Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností Hlava II, Technická opatření

§28 - Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv



KPMG

Dopady do organizace aneb na co se především zaměřit?

Na co se především zaměřit?

Zpřísněná pravidla pro řízení kybernetické bezpečnosti

- identifikace všech primárních aktiv v rámci celé organizace (včetně jejich evidence);
- určení, která primární aktiva souvisejí s poskytováním RS, a určení jejich podpůrných aktiv;
- stanovení rozsahu SŘBI (+ pravidelné přezkoumávání a aktualizace);
- alespoň 1x ročně vyhodnocení cílů SŘBI;
- řízení přístupu k aktivům;
- tvorba/aktualizace bezpečnostních politik a bezpečnostní dokumentace;
- komplexnější přístup k řízení rizik;
- povinnost identifikovat rizika, vyhodnocovat a přijímat opatření ke snížení rizik, posuzovat naplňování plánu zvládání rizik;
- analýza rizik stěžejní před jakoukoliv změnou ve společnosti;
- posuzování účelnosti opatření k řízení rizik v oblasti KB;
- zabezpečení pořizování, vývoje a údržby sítí a informačních systémů;
- důraz na bezpečnost lidských zdrojů, pravidelná školení a kybernetická hygiena;
- prosazování politik a postupů týkajících se používání kryptografie a případně šifrování;
- využívání více faktorového ověření identity;
- zajištění provedení auditu kybernetické bezpečnosti;
- provádění penetračních testování technických aktiv.

Protiopatření

- povinnost provádění výstrah, varování a reaktivních opatření;
- následné oznámení o provedení a výsledku opatření NÚKIB.

Zpřísněná pravidla pro dodavatele

- povinnost zajistit bezpečnost celého dodavatelského řetězce, včetně bezpečnostních aspektů týkajících se vztahů mezi každým subjektem a jeho přímými dodavateli nebo poskytovateli služeb;
- povinnost zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro svůj stanovený rozsah;
- zohlednění zranitelností specifických pro každého přímého dodavatele a poskytovatele služeb;
- zohlednění celkové kvality produktů a postupů v oblasti kybernetické bezpečnosti svých dodavatelů a poskytovatelů služeb, včetně postupů bezpečného vývoje.

Zpřísněné povinnosti vrcholného vedení

- odpovědnost vrcholného vedení za kybernetickou bezpečnost;
- školení vedoucích orgánů;
- prokazatelné seznamování se s výsledky a zprávami z oblasti KB;
- zajištění dostupnosti zdrojů potřebných pro zajišťování kybernetické bezpečnosti;
- účast zástupce vrcholného vedení, nebo jím pověřená osoba na výboru pro řízení kybernetické bezpečnosti.

Incident management

- důraz na řešení incidentů (prevence a odhalování KBI a reakce na ně) a stanovení nutných bezpečnostních opatření;
- prošetření a určení příčin kybernetického bezpečnostního incidentu;
- vedení záznamů o KBI a o jejich zvládání.

Na co se především zaměřit?

Dohled orgánu
- kontroly ve společnosti (včetně namátkových) i externí dohled;
- pravidelné audity;
- cílené bezpečnostní audity na základě posouzení rizik, nebo dostupných informací týkajících se rizik;
- požadavky na přístup k údajům, dokumentům nebo veškerým informacím potřebným pro výkon dohledových úkolů;
- požadavky na doložení provádění zásad KB či na přístup k údajům, dokumentům anebo veškerým informacím potřebným pro výkon dohledových úkolů;
- povinnost provést uložená nápravná opatření;
- dodržování vydaných varování, závazných pokynů nebo příkazů požadujících, aby subjekty napravily zjištěné nedostatky nebo porušení povinností.

Sdílení informací
- hlášení registračních, kontaktních a dalších doplňujících údajů NÚKIB;
- hlášení kybernetických bezpečnostních incidentů (prvotní hlášení do 24h);
- informování uživatelů regulované služby (v případě KBI);
- vzájemné sdílení podstatných informací o KB včetně informací týkajících se kybernetických hrozeb, zranitelností, indikátorů narušení, taktiky, technik a postupů, varování při ohrožení kybernetické bezpečnosti a konfiguračních nástrojů.

Řízení kontinuity
- analýza dopadů;
- správa zálohování a obnova provozu po havárii;
- krizové řízení;
- nastavení plánů kontinuity podle kritičnosti aktiv;
- pravidelné testování kontinuity a plánů obnovy;
- zpracování plánu obnovy/migrace kritických dodávek;
- testování plánů kontinuity a plánů obnovy musí zahrnovat dodavatelské řetězce.

Sankce, tresty
- za přestupek lze uložit pokutu až 250 milionů korun či do 2 % z čistého celosvětového ročního obratu v předchozím rozpočtovém roce (záleží, která z částek je vyšší);
- pořádkové pokuty až do výše 100 tisíc korun;
- donucovací pokuty až do výše 10 milionů korun nebo 1 % z čistého celosvětového ročního obratu v předchozím rozpočtovém roce (záleží, která z částek je vyšší);
- další sankční režimy;
- pozastavení platnosti certifikace;
- pozastavení výkonu řídící funkce.

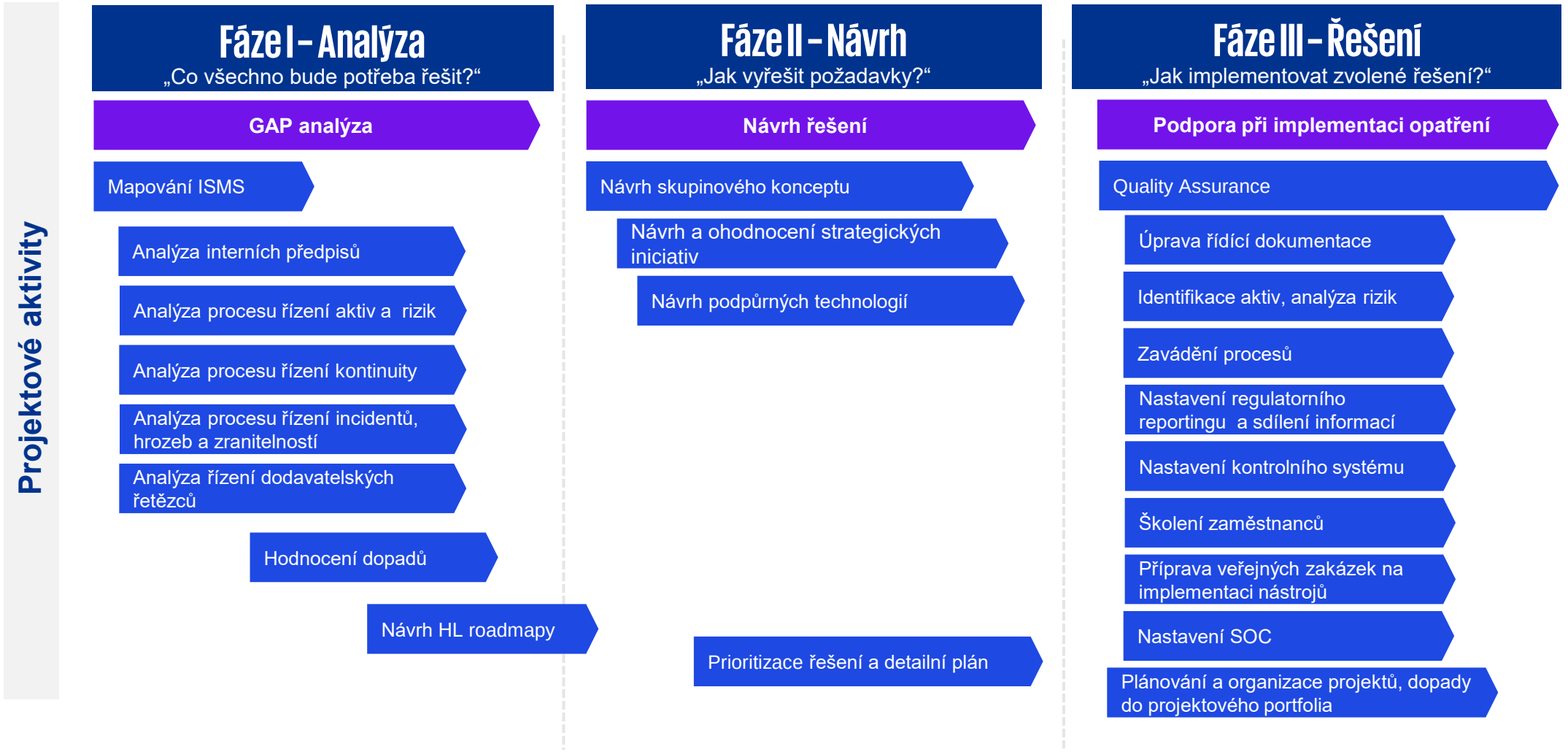
Přesná podoba těchto opatření v rámci ČR je aktuálně v legislativním procesu.

Typické dopady nZoKB do organizace

- Identifikace aktiv, stanovení rozsahu řízení kybernetické bezpečnosti dle zákona, přezkum a aktualizace bezpečnostních politik a bezpečnostní dokumentace
- Zavedení nových procesů vycházejících z aktualizovaných bezpečnostních politik
- Aktualizace procesu řízení aktiv a rizik – aktualizace analýzy rizik a plánu zvládání rizik
- Změna/obsazení bezpečnostních rolí, 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 (SOC, CSIRT) 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 výstupů

Příklad KPMG přístupu k řešení nového ZoKB v organizaci



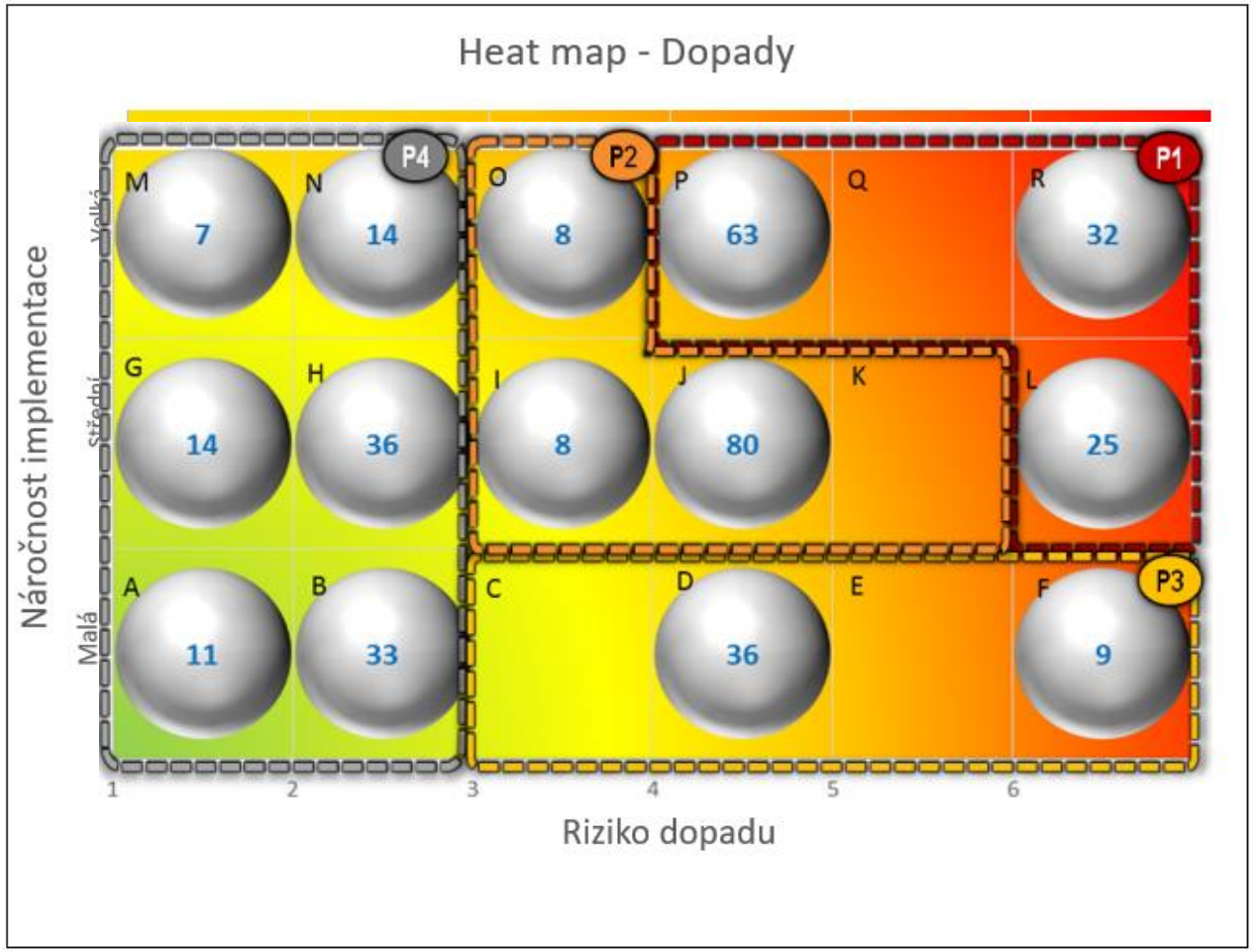
Příklad auditního výstupu – checklist povinností dle vyhlášek

Oblast	Identifikace ustanovení	Obsah ustanovení vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností	Míra splnění	Poznámka	Odkaz na dokument	Kapitola / Odstavec
Systém řízení bezpečnosti informací	HLAVA I §4 odst. 1 písm. i	2. výsledků vyhodnocení účinnosti SŘBI,	Splněno			
Systém řízení bezpečnosti informací		3. dopadů kybernetických bezpečnostních incidentů na poskytované služby a	Splněno			
Systém řízení bezpečnosti informací		4. v souvislosti s prováděnými významnými změnami.	Nesplněno			
Systém řízení bezpečnosti informací	HLAVA I §4 odst. 1 písm. j	Povinná osoba v rámci SŘBI řídí provoz a zdroje SŘBI a zaznamenává činnosti spojené se systémem řízení bezpečnosti informací a řízením rizik.	Částečně splněno			
Systém řízení bezpečnosti informací	HLAVA I §4 odst. 1 písm. k	Povinná osoba v rámci SŘBI stanoví proces řízení výjimek z pravidel stanovených podle písm. e).	Splněno			
Systém řízení bezpečnosti informací	HLAVA I §4 odst. 2 písm. a	Povinná osoba v případě neplnění povinnosti řízení rizik podle odstavce 1 písm. c) zavede všechna bezpečnostní opatření požadovaná touto vyhláškou				
Systém řízení bezpečnosti informací	HLAVA I §4 odst. 2 písm. b	Povinná osoba v případě neplnění povinnosti řízení rizik podle odstavce 1 písm. c) zpracuje o bezpečnostních opatřeních podle písm. a),				
Systém řízení bezpečnosti informací		1. prohlášení o aplikovatelnosti podle § 9 odst. 1 písm. f) a	Splněno			
Systém řízení bezpečnosti informací		2. plán zvládání rizik přiměřeně podle § 9 odst. 1 písm. g),	Splněno			

Příklad heatmapy k prioritizaci kroků

Zhodnocení a prioritizace kroků

- **P1** – Realizace je potřebná ASAP
- **P2** – Je potřebná detailnější analýza pro návrh řešení
- **P3** – „Quick wins“ realizace je možná okamžitě
- **P4** – Realizace dopadu je možná později



Příklad karty iniciativ

* Priorita — Vysoká — Střední — Normální

Název	Revize procesu identifikace, řešení a hlášení incidentů
Stručný popis iniciativy	Cílem iniciativy je zajištění SOC, jeho začlenění do organizace a jejího ISMS, a to včetně definice konceptu a katalogu služeb, vytvoření strategie SOC (vize a cíle, operační model SOC) a popisu procesů/činností SOC (včetně potřeby personálních zdrojů). Organizace může SOC vybudovat a provozovat vlastními silami, nebo může poptat SOC jako službu poskytovanou externím dodavatelem včetně potřebných kapacit bezpečnostních specialistů. Zajištění SOC jako služby je pro organizaci doporučená varianta. SOC pro organizaci by měl být zajišťován v režimu 24/7 s nepřetržitým dohledem a s vysokou dostupností služeb (včetně geograficky odděleného záložního pracoviště), procesy a provoz SOC by měly splňovat standard ISO 27001 a požadavky Zákona 181/2014 Sb. a Vyhlášky 82/2018 Sb. o kybernetické bezpečnosti a vyhlášky NIS2. Součástí služeb SOC by měl být certifikovaný tým CSIRT, podporující provozy IT a OT při rychlém vyšetření a vyřešení incidentů. Při popisu hodnocení a hlášení incidentů je vhodné využít techniky MITRE ATT&CK. Výstupem iniciativy je návrh architektury SOC, zavedené procesy SOC a implementace potřebných nástrojů.
Řešené gapy	7, 8, 13, 14
Řešitel	Jan Novák

Doba implementace	10-12 měsíců	**CAPEX**	750 000 Kč
Dodatečná FTE	3	**OPEX**	400 000 Kč

Příklad rozpočtu – finální přehled, podkladové výpočty

Odhady implementace opatření

Odhady nákladů (podle zkušenosti KPMG) na implementaci jednotlivých opatření v závislosti na velikosti společnosti

Velikost společnosti (zaměstnanců)	§3-§16	§17	§18	§19	§20	§21
Méně než 50	500 000,00 Kč	500 000,00 Kč	1 000 000,00 Kč	500 000,00 Kč	500 000,00 Kč	500 000,00 Kč
51-249	700 000,00 Kč	1 000 000,00 Kč	4 000 000,00 Kč	2 000 000,00 Kč	1 500 000,00 Kč	2 000 000,00 Kč
Nad 250	1 000 000,00 Kč	3 000 000,00 Kč	10 000 000,00 Kč	10 000 000,00 Kč	10 000 000,00 Kč	4 000 000,00 Kč
Synergie	60%	20%	50%	50%	30%	50%

Vytvoření základní sady vrcholových politik SŘBI, formulářů a vzorů reportů. Provedení analýzy aktiv a rizik,	Definice bezpečnostních úseků, implementace kontroly perimetru (EZS), kontroly vstupů (elektronické	Definice segmentace sítě a komunikačních pravidel. Upgrade síťových prvků (routery, switche, FWs), zavedení	Zavedení IDM, zavedení MFA (např. MS MFA), konfigurace bezpečné autentizace pro všechny účty ve	Definice konceptu RBAC, zavedení RBAC a nastavení rolí do všech aplikací, revize přístupových oprávnění všech	Zavedení kontroly (antispam, antivir) na e-mailové bráně (např. konfigurací Azure Outlook). Zavedení ochrany

Název	Popis	Opex (za 1 rok)	Capex	FTE
Revize procesu řízení kybernetických rizik	Aktualizace politiky a metodik, zaškoleni zaměstnanců, aktualizace analýzy rizik, aktualizace plánu zvládání rizik	400 000 Kč (externí support)	850 000 Kč (první rok)	0,2 FTE
Revize procesu řízeni bezpečnosti dodavatele	Aktualizace politiky, revize vzoru smluv, zaškolení zaměstnanců, aktualizace klasifikace dodavatelů, přesmluvnění kritických dodavatelů	-	850 000 Kč (první rok)	-
Revize procesu řízení kontinuity činností	Aktualizace politiky a metodik, zaškolení zaměstnanců, aktualizace byznys impakt analýzy, návrh vrcholového plánu kontinuity, návrh vzoru a plánu kontinuity a plánu obnovy, návrh plánu testu kontinuity	300 000 Kč (pravidelné testy s dodavateli)	1 200 000 Kč (první rok)	0,2 FTE
Revize procesu identifikace, řešení a hlášení incidentů	Výběr dodavatele SOC, napojení bezpečnostního dohledu, aktualizace politiky, příprava vzoru hlášení, zaškolení zaměstnanců	400 000 Kč (externí služby SOC)	750 000 Kč (první rok)	0,2 FTE
Celkem		**1 100 000 Kč**	**2 650 000 Kč**	**0,6 FTE**

Závěrečné shrnutí

Jak může KPMG pomoci

Jak už dnes pomáháme klientům

- zhodnocení procesu řízení aktiv a rizik, samotná analýza aktiv a rizik;
- analýza politik, příloh, metodik a vzorů;
- posouzení řízení a efektivity zvládání incidentů;
- zhodnocení plánů kontinuity podle kritičnosti aktiv;
- analýza závislosti na dodavatelích třetích stran a navázaných smluvních vztahů;
- **hodnocení dopadu NIS2** a souladu s platnou legislativou dle zjištěných informací;
- **návrh harmonogramu** a tematických okruhů, které vzešly z GAP analýzy;
- **návrh governance a strategie k zajištění souladu s NIS2 (s novým ZoKB a jeho vyhláškami);**
- **tvorba interních předpisů.**

Využíváme zkušený seniorní interní tým

- dlouholeté zkušenosti s GAP analýzou dle požadavků NIS1 v lokální implementaci;
- sledování vývoje směrnice NIS2 už v průběhu přípravy na půdě EU;
- připomínkování návrhu nového ZoKB a jeho vyhlášek na základě dlouhodobých zkušeností;
- dostatečná kapacita týmu a nabyté zkušenosti pro hladký průběh rozdílové analýzy;
- reference s dodávkami srozumitelného a přehledného vyhodnocení aktuálního stavu.

Patříme mezi přední účastníky aktivit souvisejících s aplikací NIS2

Odborné články (viz odkazy přímo v textu)

19. 12. 2022 - NIS2 bude srovnatelná s GDPR – Týdeník Euro (tydenikeuro.cz)

9. 1. 2023 - Evropa proti kyberzločinu. Nová direktiva o IT bezpečnosti ovlivní tisíce firem | Týdeník pro ekonomiku, politiku a byznys (tydenikhrot.cz)

30. 1. 2023 - Kyberbezpečnost po česku: tři řádky v Excelu a liknavý přístup vedení | Finmag.cz (penize.cz)

03/2023 - NIS2 zpřísní nároky na kyberbezpečnost firem i státu

Účast na odborných konferencích, workshopech

Cyberblog kulatý stůl: NIS 2 – co přináší nová evropská směrnice zaměřená na standardizaci v oblasti kybernetické bezpečnosti? – Cyberblog

Nová bezpečnostní směrnice NIS 2 se bude týkat mnohem více společností než jednička. - O2

Program XVIII. konference IT Governance 2022 | ISACA CRC

Způsobí NIS 2 stejný poprask jako GDPR? | Konference a události KPMG (kpmg-eventy.cz)

2023 - Virtuální konference "Směrnice NIS 2: Procesy a technologie" - NIS2.tech

Mezinárodní konference QUBIT: NIS 2 – an opportunity to increase cybersecurity importance

Tomáš Kudělka – KPMG NIS2 garant

Tomáš Kudělka

Director

Tel.: +420 724 244 944

Email: tkudelka@kpmg.cz

Tomáš v oblasti IT a IT bezpečnosti působí už 25 let. Svou kariéru zahájil v KPMG v oddělení Risk Managementu. Zaměřoval se především na informační bezpečnost – procesní i řídící frameworky (ISO 27001, COBIT, ITIL, PCI DSS) a technické zabezpečení (penetrační testy, configuration review, apod.). Později byl také zodpovědný za projekty v oblasti řízení IT a návrhu IT architektur.

Po prvních deseti letech práce v oblasti poradenství pro KPMG přešel do IT provozu. Nejdříve vystavěl a jako výkonný ředitel řídil globální provozní centrum pro mezinárodní IT společnost Diebold Nixdorf. Následně tři roky pracoval jako CTO pro mezinárodního systémového integrátora, společnost Simac Technik.

V roce 2019 se vrátil do KPMG a v současné době pracuje jako ředitel technologického týmu.

Oblasti NIS2 se aktivně věnuje v odborných kruzích a často vystupuje na konferencích a v odborných diskusích, například:

- Kulatý stůl na téma NIS 2 se zástupci NÚKIB: Cyberblog kulatý stůl: NIS 2 – co přináší nová evropská směrnice zaměřená na standardizaci v oblasti kybernetické bezpečnosti? – Cyberblog
- O2 CyberCast: O2 CyberCast #5 s Tomášem Kudělkou z KPMG: Nová bezpečnostní směrnice NIS 2 se bude týkat mnohem více společností než jednička. - O2
- Konference IT governance 2022: Program XVIII. konference IT Governance 2022 | ISACA CRC
- Konference Směrnice NIS 2: Procesy a technologie: Virtuální konference "Směrnice NIS 2: Procesy a technologie" - NIS2.tech

Na téma NIS2 publikoval řadu článků v oborných periodikách, například:

- NIS2 bude srovnatelná s GDPR – Týdeník Euro (tydenikeuro.cz)
- Na tisíce firem dopadne nová administrativa. Některé může přijít až na stovky milionů | Hospodářské noviny (HN.cz)
- Evropa proti kyberzločinu. Nová direktiva o IT bezpečnosti ovlivní tisíce firem | Týdeník pro ekonomiku, politiku a byznys (tydenikhrot.cz)
- NIS2 zpřísní nároky na kyberbezpečnost firem i státu (systemonline.cz)