NOVÝ ZÁKON O KYBERNETICKÉ BEZPEČNOSTI AKTUÁLNĚ

Jindřich Kalíšek, advokát

18. 4. 2024

PŘEDNÁŠEJÍCÍ

- JUDr. Ing. Jindřich Kalíšek, Ph.D., CIPP/E CIPM
  - Advokát a zapsaný mediátor
  - Zakladatel & CEO cysensic & #CYBERLAWYER
  - Vysokoškolský učitel
  - Člen odborných organizací a spolků
    - Odborná sekce pro právo IT a ochranu osobních údajů (ČAK)
    - Spolek pro ochranu osobních údajů
    - Evropská federace pověřenců pro ochranu OÚ (EFDPO)
    - Český institut manažerů informační bezpečnosti (ČIMIB)
  - 14 let praxe v oblasti práva IP/IT, ochrany OÚ a kybernetické bezpečnosti

cysensic

#CY83RL4WY3R

OBSAH PŘEDNÁŠKY

1. AKTUÁLNÍ SITUACE NOVÉ EVROPSKÉ REGULACE KYBERBEZPEČNOSTI
2. AKTUÁLNÍ SITUACE NOVÉ ČESKÉ REGULACE KYBERBEZPEČNOSTI (KB)
3. STAV LEGISLATIVNÍHO PROCESU
4. DOPADY NZKB DO ORGANIZACE A POŽADAVKŮ NA BEZPEČNOST JEJÍHO EKOSYSTÉMU
5. SHRNUTÍ A DOPORUČENÍ
6. Q & A

NOVÁ EVROPSKÁ REGULACE KYBERBEZPEČNOSTI

- Směrnice Evropského parlamentu a Rady (EU) č. 2022/2555, o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148 (Network Infrastructure Security Directive 2 – NIS2)
  - Účinnost k 16. 1. 2023
  - Transpoziční lhůta k 17. 10. 2024

- Související legislativa EU
  - Směrnice Evropského parlamentu a Rady (EU) č. 2022/2557, o odolnosti kritických subjektů (CER)
  - Nařízení Evropského parlamentu a Rady (EU) č. 2022/2554, o digitální provozní odolnosti finančního sektoru (DORA)
  - Návrh nařízení o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky (Akt o kybernetické odolnosti – CRA)

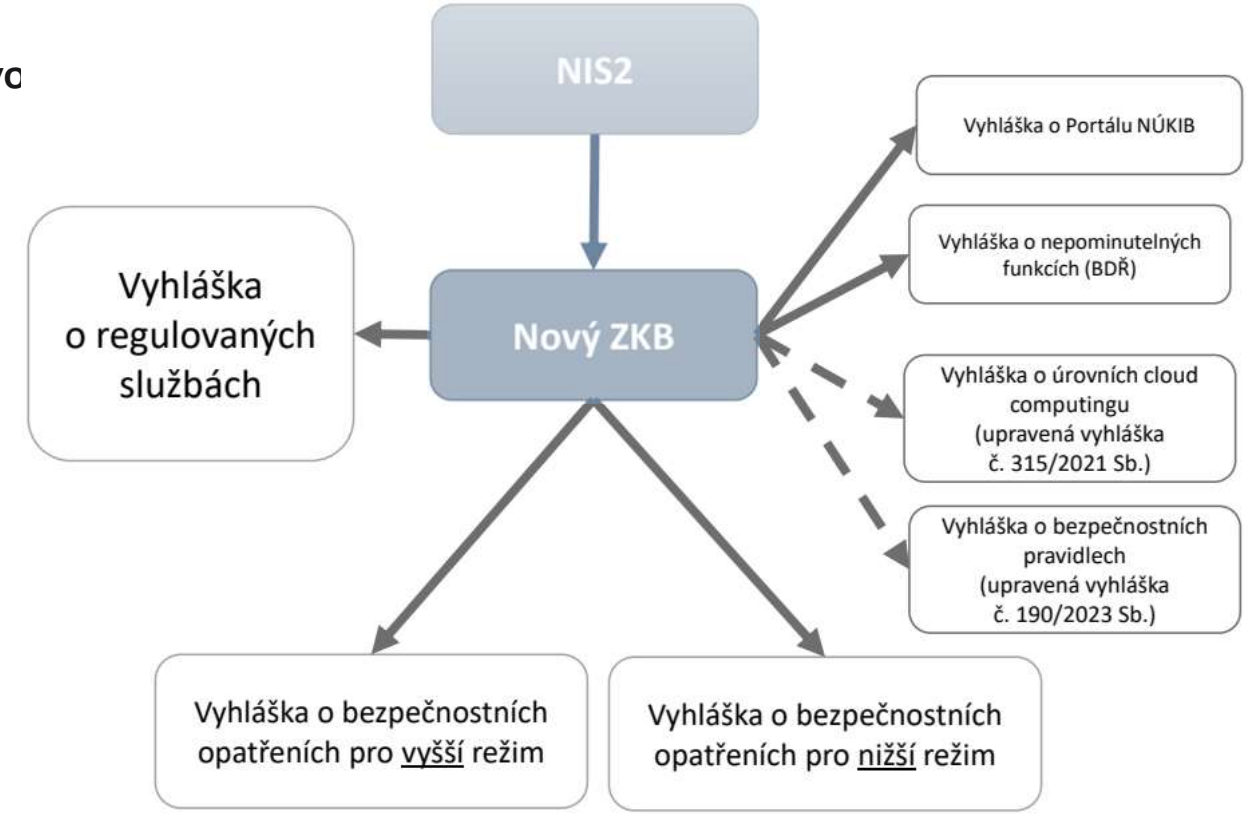
KONCEPCE ČESKÉ REGULACE KYBERBEZPEČNOSTI

- Návrh legislativního balíku
  - Gestorem Národní úřad kybernetické a informační bezpečnost (NÚKIB; nis2.nukib.cz)
  - Legislativní balíček složený ze zákonné a podzákonné regulace (vyhlášky, nařízení vlády ?)
  - Regulace kyberbezpečnosti organizací soukromého a veřejného sektoru
  - Kombinace požadavků NIS2 s vybranými existujícími instituty a novými instituty
- Další výhled
  - Nařízení NIS3? → 2026 + ~5 let

- Nejvýznamnější dopady
  - Rozšíření počtu povinných osob
    - V ČR z 490 na 6 000 (až 10 000 – 12 000?)
  - Povinné vzdělávání vrcholového vedení organizace
  - Větší důraz na sdílení informací mezi povinnými organizacemi
  - Prohloubení spolupráce mezi regulátorem a povinným organizacemi
  - Podrobnější požadavky na vedení registru internetových domén nejvyšší úrovně a činnost registrátorů
  - Řádové zvýšení pokut za nedodržení uložených povinností
    - Dnes max. 5 mil. Kč → 2 % z celosvětového obratu anebo 10 mil. €

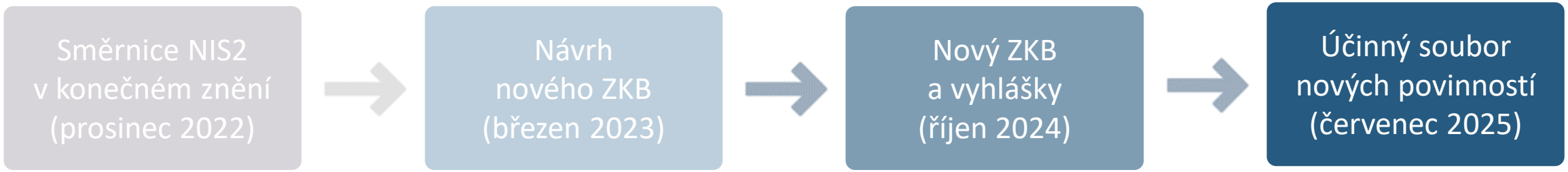
KONCEPCE ČESKÉ REGULACE KYBERBEZPEČNOSTI

- Návrh legislativního balíku
  - Změn proti ZKB je u nZKB tolik, že bylo potřeba vytvo nový zákon
  - Zcela nová úprava (cca 70 paragrafů)
  - Aktuální verze legislativního balíku
    - Zákon
    - Doprovodný zákon
    - 7 vyhlášek



Upraveno podle oficiálních publikací NÚKIB v režimu TLD: CLEAR, 2022-2024 (https://osveta.nukib.cz/)

STAV LEGISLATIVNÍHO PROCESU

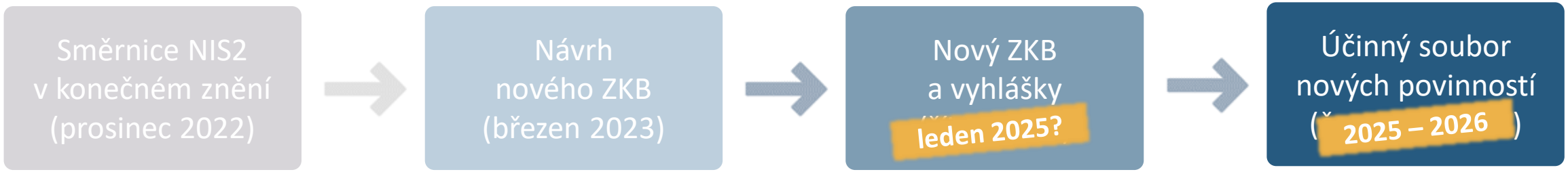


Upraveno podle oficiálních publikací NÚKIB v režimu TLD: CLEAR, 2022-2024 (https://osveta.nukib.cz/)

STAV LEGISLATIVNÍHO PROCESU

- 18 měsíců na národní legislativní proces → NÚKIB začal v předstihu
  - Leden – březen 2023 – Veřejné konzultace → 1 144 unikátních připomínek
  - Červenec 2023 – Oficiální ukončení MPŘ
  - 22. 12. 2023 – Předloženo LRV
  - 4. 4. 2024 – Proběhla Velká LRV, která jednání přerušila a vrátila zákon předkladateli k dopracování
- Nabírá se zpoždění (aktuálně asi 5 měsíců) → Účinnost patrně od 1. 1. 2025, možná dokonce později
  - Vyhlášky do LP v každém případě později!

STAV LEGISLATIVNÍHO PROCESU



Upraveno podle oficiálních publikací NÚKIB v režimu TLD: CLEAR, 2022-2024 (https://osveta.nukib.cz/)

STAV LEGISLATIVNÍHO PROCESU

- Mezirezortní připomínkové řízení
  - Celkem NÚKIB obdržel 886 připomínek od 51 připomínkových míst
  - 518 připomínek zásadních
  - 368 připomínek doporučujících

- Rozpor přetrvává u 4 připomínkových míst
  - Český telekomunikační úřad
  - Svaz měst a obcí
  - Asociace krajů
  - Svaz průmyslu a dopravy

Upraveno podle oficiálních publikací NÚKIB v režimu TLD: CLEAR, 2022-2024 (https://osveta.nukib.cz/)

STAV LEGISLATIVNÍHO PROCESU

- Hlavní kritizované a sporné oblasti
  - Nedostatečné zpracování dopadové analýzy RIA
  - Mechanismus prověřování bezpečnosti dodavatelského řetězce (BDŘ)
    - Zrušit, omezit jen na kritická aktiva anebo do určité hloubky DŘ
    - Kompenzace
    - Nemělo by se vztahovat na přístupovou část sítí (RAN)
  - Určovací kritéria RS ve vyhlášce a nikoliv v zákoně (nebo v nařízení vlády)
    - LRV: Není neústavní
  - Regulace obcí s rozšířenou působností
    - Buď úplné vypuštění obcí nebo vynětí z přestupkové odpovědnosti, popř. plošné snížení pokut

- Připomínky a návrhy jejich vypořádání lze dohledat ve vypořádací tabulce v eKLEP

- **Motivace kritiků? × Motivace NÚKIB**

POVINNÉ SUBJEKTY

Vyšší režim bezpečnosti

- Provozovatelé kritické infrastruktury (včetně informační)
- Provozovatelé základních služeb
- Provozovatelé některých významných informačních systémů
- Energetika – elektřina, dálkové vytápění a chlazení, ropa, zemní plyn, vodík
- Doprava – letecká, železniční, vodní silniční
- Bankovnictví – úvěrové instituce
- Infrastruktury finančních trhů – obchodní systémy (burzy), ústřední protistrany
- Zdravotnictví – poskytovatelé zdravotní péče, referenční laboratoře EU, subjekty provádějící výzkum a vývoj týkající se léčivých přípravků, subjekty vyrábějící základní farmaceutické výrobky a farmaceutické přípravky, subjekty vyrábějící zdravotnické prostředky považované za kritické v případě ohrožení veřejného zdraví
- Pitná a odpadní voda
- Digitální infrastruktura – výměnné uzly internetu, DNS, TLD, cloud computing, datová centra, sítě pro doručování obsahu, služby vytvářející důvěru, veřejné sítě a služby elektronických komunikací
- Veřejná správa – ústřední subjekty veřejné správy, subjekty veřejné správy územních jednotek (NUTS 1 + 2)
- Vesmír

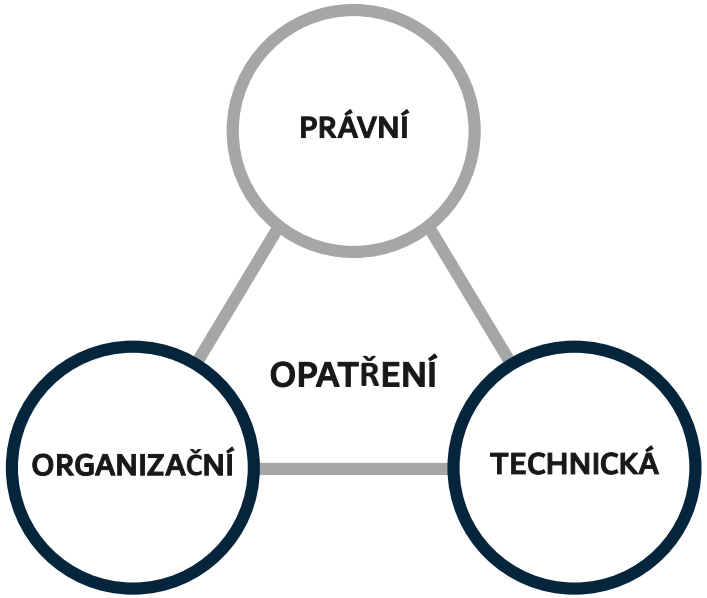
Nižší režim bezpečnosti

- Provozovatelé významných informačních systémů
- Poštovní a kurýrní služby
- Nakládání s odpady
- Výroba, produkce a distribuce chemických látek
- Výroba, zpracování a distribuce potravin
- Další výroba – výroba zdravotnických prostředků a diagnostických zdravotnických prostředků, výroba počítačů, elektronických a optických přístrojů, výroba elektrických zařízení, výroba strojů a zařízení, výroba motorových vozidel, přívěsů a návěsů, výroba ostatních dopravních prostředků a zařízení
- Poskytovatelé digitálních služeb – online tržiště, internetové vyhledávače, platformy služeb sociálních sítí

- Dopadá na nás regulace?
  - Podléháme současné regulaci?
  - Co z nové regulace na nás dopadá?
- Plníme velikostní kritéria?
  - Počet zaměstnanců (roční pracovní jednotka ≥ 50)
  - Objem aktiv (bilanční suma rozvahy > 43 mil. €)
  - Roční obrat (> 50 mil. €)
- Plníme věcná kritéria?

IMPLEMENTACE POŽADAVKŮ NOVÉ REGULACE I

- Požadavky NIS2 → Požadavky nZKB
- Vhodná, přiměřená a odpovídající technická a organizační opatření k řízení bezpečnostních rizik a incidentů
  - Analýza rizik a politiky bezpečnosti informačních systémů
  - Řešení a zvládání incidentů (prevence, odhalování a reakce)
  - Zotavení a kontinuity činností (*business continuity*) → krizové řízení
  - Bezpečnost dodavatelského řetězce
  - Bezpečnost lidských zdrojů
  - Řízení přístupů k aktivům a zabezpečení proti jejich zneužití
  - Metodiky, politiky a postupy pro hodnocení účinnosti bezpečnostních opatření → testování a audit
  - Praktiky základní počítačové hygieny
  - Vzdělávání v oblasti kybernetické bezpečnosti → povinné vzdělávání vrcholového vedení



- Máme dostatečné technické, finanční a lidské zdroje na rozvoj a posilování IS/CS?

IMPLEMENTACE POŽADAVKŮ NOVÉ REGULACE II

- Registrovat regulovanou službu
- Hlásit kontaktní a další údaje
- Stanovit rozsah řízení kybernetické bezpečnosti
- Zavádět bezpečnostní opatření
  - Vyšší režim
  - Nižší režim
- Hlásit kybernetické bezpečnostní incidenty
  - Vyšší režim
  - Nižší režim
- Reagovat na protiopatření
  - Výstraha × Varování × Reaktivní opatření
- Plnit informační povinnost poskytovatele regulované služby
- Oznamovat KBI s významnými dopady
  - NÚKIB
  - Uživatelé → včetně informace o krocích, které zmenšují dopady
- **Máte dostatečné technické, finanční a lidské zdroje na rozvoj a posilování IS/CS?**

IMPLEMENTACE POŽADAVKŮ NOVÉ REGULACE III

- Ustanovení ZKB *Seznam bezpečnostních opatření provozovatelů regulovaných služeb* +
- Účinné znění příslušných vyhlášek
  - § 4–17 + 18–28 vyhlášky o bezpečnostních opatřeních PRS v režimu vyšších povinností
  - Vyhláška o bezpečnostních opatřeních PRS v režimu nižších povinností (check-list) ?

Režim vyšších povinností – Organizační opatření	Režim vyšších povinností – Technická opatření
1. Systém řízení bezpečnosti informací	1. Fyzická bezpečnost
2. Povinnosti vrcholového vedení	2. Bezpečnost komunikačních sítí
3. Bezpečnostní role	3. Správa a ověřování identit
4. Řízení bezpečnostní politiky a dokumentace	4. Řízení přístupových oprávnění
5. Řízení aktiv	5. Detekce KBU
6. Řízení rizik	6. Zaznamenávání událostí
7. Řízení dodavatelů	7. Vyhodnocování KBU
8. Bezpečnost lidských zdrojů	8. Aplikační bezpečnost
9. Řízení změn	9. Kryptografické algoritmy
10. Akvizice, vývoj a údržba	10. Zajišťování dostupnosti regulované služby
11. Řízení přístupu	11. Zabezpečení průmyslových, řídící a obdobných specifických aktiv
12. Zvládání KBU a KBI	
13. Řízení kontinuity činností	
14. Audit kybernetické bezpečnosti	

Režim nižších povinností – Organizační opatření
1. Zajišťování minimální úrovně kybernetické bezpečnosti
2. Povinn[illegible] vrcholového [illegible]dení
3. Říz[illegible]ní aktiv
4. [illegible]vládání KBU a KBI

Režim nižších povinností – Technicka opatření
1. [illegible]yzická bezpečn[illegible]st
2. B[illegible]zpečnost komunikačních sítí
3. Dete[illegible]e KBU
4. Aplikační bez[illegible]
5. Zajišťování dostupnosti regulované služby

SHRNUTÍ A DOPORUČENÍ

- **#NIS2 už je #buzzword → Pozor na obchodníky se strachem, teplou vodou a mlhou**
- Zavést komplexní procesy a participativní systémy pro průběžné i ad-hoc vyhodnocování rizik
- Začít sledovat bezpečnostní profil všech částí dodavatelských řetězců (PZS s vyšším režimem)
- Zpracovat bezpečnostní dokumentaci organizace a udržovat ji aktuální
- Zahájit kontinuální vzdělávání zaměstnanců i vedoucích osob
- Posílit či reorganizovat oddělení IT / CS a/nebo získat externisty
  - **Lidi nejsou! A ani v roce 2025 nebudou!**

SHRNUTÍ A DOPORUČENÍ

- S čím ne/může pomoci externista?
  - Identifikace a právní ochrana strategických informačních aktiv
  - Participace na přípravě bezpečnostní politiky / IS-CS SP
  - Participace na zavedení bezpečnostních opatření
  - Příprava na různé typy KBU / KBI (BCM, IS/CS IRP)
  - Vzdělávání, sdílení know-how a (přiměřený) outsourcing
  - Kyberbezpečnost na klíč / bez práce / koupí dokumentů a zařízení
  - Kyberbezpečnost bez pravidelné spolupráce s interními lidmi

DĚKUJI ZA POZORNOST

Jindřich Kalíšek, advokát
2024 © Nakladatelství FORUM

18. 4. 2024