PRÁVNÍ PROSTOR

ODBORNÝ KONGRES

Ing. Bc. Adam Kučínský

Národní úřad pro kybernetickou
a informační bezpečnost

Aktuální změny v oblasti regulace kybernetické bezpečnosti

Aktuální změny v oblasti regulace kybernetické bezpečnosti

Nový zákon o kybernetické bezpečnosti

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Právní prostor
10. dubna 2024
TLP: CLEAR

Adam Kučínský
ředitel
Odbor regulace

Shrnutí situace

Prezentace má informační a osvětových charakter a informace v ní obsažené se mohou se v čase změnit.

Základem změn je nově přicházející **směrnice NIS2**, ale také potřeba zákon o kybernetické bezpečnosti aktualizovat.

Do návrhu zákona jsou promítnuty také vnitrostátní instituty a požadavky.

Směrnice obecně je legislativní akt Evropské unie, který není* sám o sobě aplikovatelný **(= musí nejdříve vzniknout národní úprava).**

Národní úřad pro kybernetickou a informační bezpečnost **připravil návrh nového zákona o kybernetické bezpečnosti.**

Návrh zákona byl 22. 12. 2023 předložen Legislativní radě vlády. Velká LRV proběhla 4. 4. 2024

Nová pravidla by měla platit v druhé polovině roku 2024 (do 17. října 2024 podle požadavku směrnice NIS2).

*zpravidla

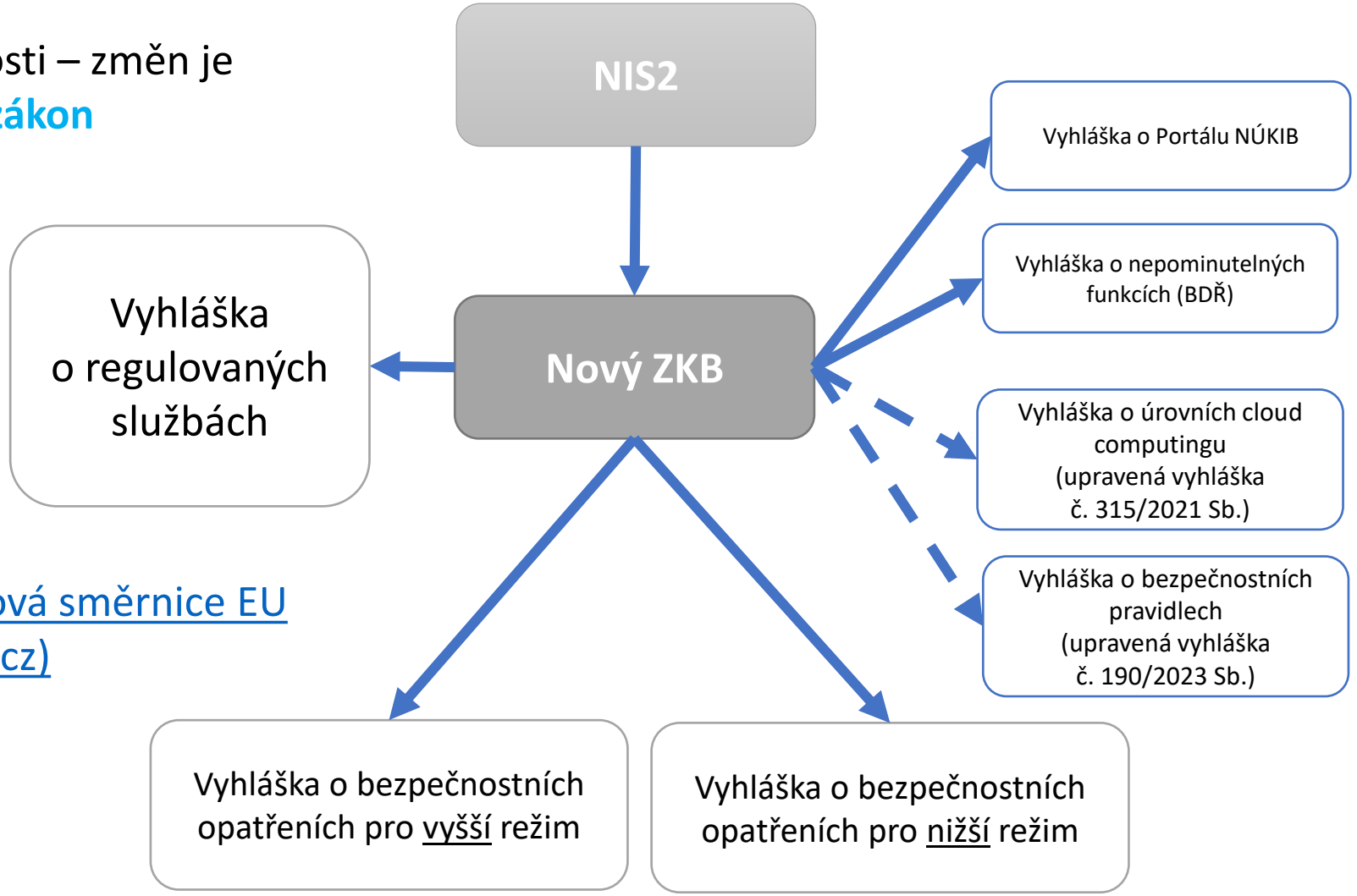
Nový zákon o kybernetické bezpečnosti v LRV

Nový zákon o kybernetické bezpečnosti – změn je tolik, že bylo **potřeba vytvořit nový zákon**

= zcela nová úprava – cca 70 paragrafů

Verze po mez. připomínkovém řízení předpokládá navíc **7 vyhlášek.**

Celý návrh zveřejněn zde: [Course: Nová směrnice EU o bezpečnosti sítí a informací (nukib.cz)]



Nový ZKB – hlavní body

Nový zákon dopadne na minimálně 6 000 organizací

- jde téměř výhradně o požadavek směrnice
- reguluje přes **107 služeb ve 22 odvětvích** (energetika, zdravotnictví, bankovnictví, doprava, veřejná správa, digitální infrastruktura,…)
- hlavním kritériem pro zahrnutí do regulace je **velikost subjektu** (daná počtem zaměstnanců nebo jeho finanční situací)
- mění se také přístup k rozsahu regulace – **nevybírají se konkrétní systémy, ale celé služby**
- do regulace se nově navrhuje **zařadit obce (ORP)**

Regulované organizace zákon nově označuje jako **tzv. poskytovatele regulované služby** a rozděluje je do **dvou režimů – nižších povinností a vyšších povinností**

- podle režimu mají stanovené povinnosti

Vznikají nové instituty

- zajištění dostupnosti regulované služby nebo mechanismus prověřování bezpečnosti dodavatelského řetězce (BDŘ)

Mění se některé stávající instituty

- stav kybernetického nebezpečí, (proti)opatření, konkrétní lhůty pro hlášení incidentů, sankce,…

Povinné osoby – odvětví, služby

- Vše podle NIS2
- Nad rámec požadavků NIS2
  - Vybrané subjekty v odvětví letectví – po konzultaci s ÚCL
  - Vybrané subjekty v oblasti výzkumu a vývoje (nekomerční užití, veřejné financování, citlivá činnost, velké výzkumné infrastruktury; vysoké školy)
  - Vojenský průmysl – vojenský materiál, zboží a technologie dvojího užití
  - Vybrané instituce veřejné správy
- Aktuálně 107 služeb v 22 odvětvích (mírně odlišná taxonomie než NIS2)

- Sčítání velikosti podniků vychází z NIS2

Shrnutí povinností

Hlavní povinnosti

- **hlásit kontaktní a další údaje**
- **stanovit rozsah řízení kybernetické bezpečnosti** – definuje rozsah regulace v organizaci
- **zavádět bezpečnostní opatření** – podle režimu v kterém je služba určena (vyšší/nižší)
- **hlásit kybernetické bezpečnostní incidenty** – podle režimu v kterém je služba určena (vyšší/nižší)
- **informovat zákazníky** o incidentech a hrozbách
- **provádět protiopatření**
- **plnit povinnosti z tzv. Mechanismu bezpečnosti dodavatelského řetězce** u vybraných (strategicky významných) služeb
- **zajistit dostupnost z České republiky** u vybraných (strategicky významných) služeb

Zákon dále upravuje další oblasti nezbytné pro fungování regulatorního rámce

- specifické situace – poskytování informací, stav kybernetického nebezpečí
- úprava institucí – NÚKIB, CERT a jejich pravomoci, součinnost dalších orgánů státu
- sankce – přestupky, úprava horních limitů sankcí

Nelegislativní činnosti spojené s přípravou nového ZKB

Veřejné konzultace

- Neoficiální připomínkování ze strany odborné veřejnosti v 1Q 2023
- Zasláno 1144 jedinečných podnětů (od 117 jednotlivých míst), zohledněno 58 % z nich, vypořádání je zveřejněno na webu

Dotazy

- Za březen 2024 přes centrální email regulace@nukib.cz 54 dotazů ke směrnici NIS2, novému zákonu a jeho dopadům
- Další desítky dotazů telefonicky či na osobní maily jednotlivých zaměstnanců
- Stovky jednání

Osvěta

- Od začátku roku dosud - více než 30 národních i mezinárodních konferencí, řada bilaterálních zahraničních jednání
- Aktivní komunikace s 28 svazy a oborovými sdruženími

Informační podpora

- Web Nová směrnice EU o bezpečnosti sítí a informací (nukib.cz) - 351 343 přístupů k 4. 1. 2024 (AJ verze přes 5 000)
- Nově vytvořeny tzv. factsheets – shrnutí aktuálních informací k novému zákonu

Nelegislativní činnosti spojené s přípravou nového ZKB

Spolupráce na úrovni EU

- Práce na úrovni NIS2 Cooperation group
  - Oficiální konzultační orgán podle NIS2
  - Platforma formující výklad NIS2, harmonizaci regulací, řešení odlišných názorů na výklad NIS2
  - Zástupci regulátorů v jednotlivých členských státech, zástupci EK a ENISA
  - 13 aktivních Work Streamů: bezpečnostní opatření, hlášení incidentů, dozor a spolupráce při výkonu dozoru, volby do EP, energetika, regulace poskytovatelů digitálních služeb, 5G, zdravotnictví, bezpečnost dodavatelského řetězce (NÚKIB inicioval a po dobu CZ PRES vedl), letectví, posuzování rizik, WHOIS, finanční sektor
  - NÚKIB vede pracovní podskupinu zaměřenou na vydefinování regulovaných subjektů
  - Standardní výstupy:
    - non-papery (právně nezávazné), jednotnost postupu všech členských států v určitých otázkách (např. tlak na vyšší bezpečnost dodavatelského řetězce),
    - tlak na EK k vyřešení problematických otázek (výstupem např. 3 Q&A dokumenty k NIS2 nebo úspěšný společný tlak na změnu textu Network Code k přeshraničnímu poskytování elektřiny)
  - Specifické výstupy:
    - Podkladové dokumenty pro EK pro účely vytvoření prováděcích předpisů podle NIS2 – k bezpečnostním opatřením a hlášení incidentů

Meziresortní připomínkové řízení

Oficiální meziresortní připomínkové řízení bylo zahájeno 19. června 2023 a ukončeno 26. července 2023 (téměř 6 týdnů)

- Návrh byl zaslán 85 připomínkovým místům
- Dalších 11 připomínkových míst zaslalo připomínky z vlastní iniciativy

Celkem NÚKIB obdržel 886 připomínek od 51 připomínkových míst

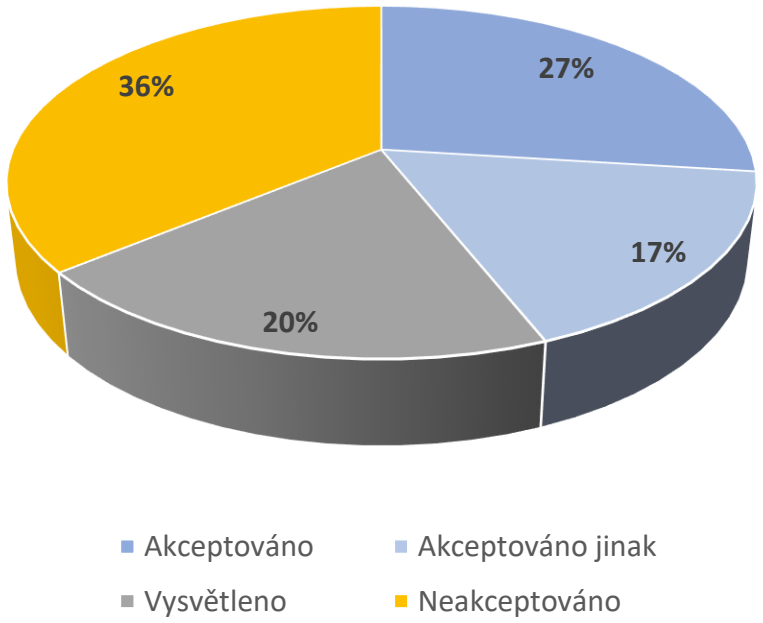
- 518 připomínek bylo zásadních, 368 připomínek bylo doporučujících

Za účelem vypořádání připomínek proběhlo 28 vypořádacích jednání

- Souhlasně bylo vypořádání 589 připomínek (**2/3 z celkového počtu**)

Rozpor přetrvává u 4 připomínkových míst

- Český telekomunikační úřad
- Svaz měst a obcí
- Asociace krajů
- Svaz průmyslu a dopravy



Nesouhlas s vypořádáním připomínek, který není předmětem rozporu přetrvává u některých dalších připomínkových míst – např. u Hospodářské komory

Shrnutí rozporů

Svaz měst a obcí

- Rozpory uplatněny u všech připomínek, tedy i u těch, kde bylo připomínkám vyhověno a byly akceptovány
- Hlavní rozpory:
  - Regulaci obcí s rozšířenou působností – vypuštění obcí nebo vynětí z přestupkové odpovědnosti
  - Určovací kritéria ve vyhlášce a nikoliv v zákoně
  - Zpracování dopadové analýzy RIA

Asociace krajů

- Rozpory uplatněny u všech připomínek, tedy i u těch kde bylo připomínkám vyhověno a byly akceptovány
- Zejména jde o:
  - mechanismus prověřování bezpečnosti dodavatelského řetězce (např. vyloučení RAN),
  - zpracování dopadové analýzy RIA, určovací kritéria ve vyhlášce a nikoliv v zákoně

Shrnutí rozporů

Svaz průmyslu a dopravy

- Určovací kritéria by měla být dána nařízení vlády a nikoli vyhláškou
- Zrušení vyhlášky o nepominutelných funkcích a omezení BDŘ jen na kritická aktiva
- Zapojení regulátora a vlády do BDŘ

Český telekomunikační úřad

- Rozpory přetrvávají u dvou připomínek
  - Omezení rozsahu BDŘ pouze na kritická aktiva
  - BDŘ by se nemělo vztahovat na přístupovou část sítí (RAN)

Podrobněji jsou všechny připomínky a návrhy jejich vypořádání uvedeny ve vypořádací tabulce dostupné zde:

ODok Portál - VeKLEP - Návrh zákona o kybernetické bezpečnosti

Vyhodnocení hlavních připomínek v MPŘ

Definice

- připomínkovány některé definice (např. aktiva, významný dopad/hrozba/incident), požadováno doplnění dalších definic -> upraveno, tam kde to dávalo smysl doplněno

Kritéria regulované služby

- nastavení vztahu zákon – zákon dostatečně nevymezuje některé instituty a nechává to na vyhláškách -> upraveno
- požadavky na neregulování některých služeb – např. obcí III. typu nebo vědeckých institucí -> neakceptováno, ale upraven režim

Rozsah a evidence aktiv

- nesouhlas s požadavkem evidovat všechna primární aktiva -> neakceptováno – jde o nezbytný požadavek a základ bezpečnosti

Kontaktní údaje a incidenty

- požadavek na to, aby vyšší režim nehlásil všechny incidenty, požadavek na prodloužení lhůty pro hlášení z 24 na 72 hodin

-> neakceptováno jde o požadavek směrnice

(Proti)opatření

- dílčí připomínky k reaktivnímu protiopatření nebo např. požadavek, aby institut varování nebyl -> neakceptováno, jde o důležitý institut

Vyhodnocení hlavních připomínek v MPŘ

Mechanismus prověřování bezpečnosti dodavatelského řetězce

- požadavky na zrušení institutu -> neakceptováno
- nedostatečně projednáno -> neakceptováno, více než 60 jednání k tomuto
- kompenzace – stát by měl platit náhrady -> doplněno zohlednění životního cyklu
- přechodné lhůty – mají být delší -> doplněno zohlednění životního cyklu
- zapojení sektorových regulátorů -> doplněno
- zúžení rozsahu dotčených aktiv – jen core, transportní a přístupové vrstvy ne
  - -> neakceptováno, ran je také důležitý
- pevné stanovení hloubky dodavatelského řetězce, který se bude prověřovat
  - -> neakceptováno – nedávalo by to smysl

V mechanismu provedeny tyto dodatečné úpravy:

- Dodržení životního cyklu zařízení (odpisy nebo 5 let)
- Projednání s MF
- Projednání se sektorovými regulátory – ČTÚ, ERÚ
- Předložení pro informaci BRS
- Doplněno ustanovení o tom co musí případné rozhodnutí zohledňovat (dopady, životnost zařízení, odpisy)

Vyhodnocení hlavních připomínek v MPŘ

Přestupky a další sankce

- vyvratitelná domněnka společenské škodlivosti -> akceptováno - upraveno
- vynětí územních samosprávných celků ze sankcí -> neakceptováno, nedává smysl
- snížení pokut státní správě -> neakceptováno, nedává smysl

Zabezpečení ISVS podle vyhlášky o nižším režimu -> neakceptováno, ISVS by měly být zabezpečeny – nižší režim

Financování -> akceptováno, doplnění důvodové zprávy

Legislativní připomínky

- doplnění důvodových zpráv -> akceptováno
- formální úpravy -> akceptováno
- zmocnění k vyhláškám -> akceptováno, upraveno

Stav kybernetického nebezpečí

- zejména otázky stran návaznosti na krizové stavy -> akceptováno, upraveno – vydefinováno s MV/GŘHZS

Legislativní rada vlády

Zákon byl ve 4 pracovních komisích

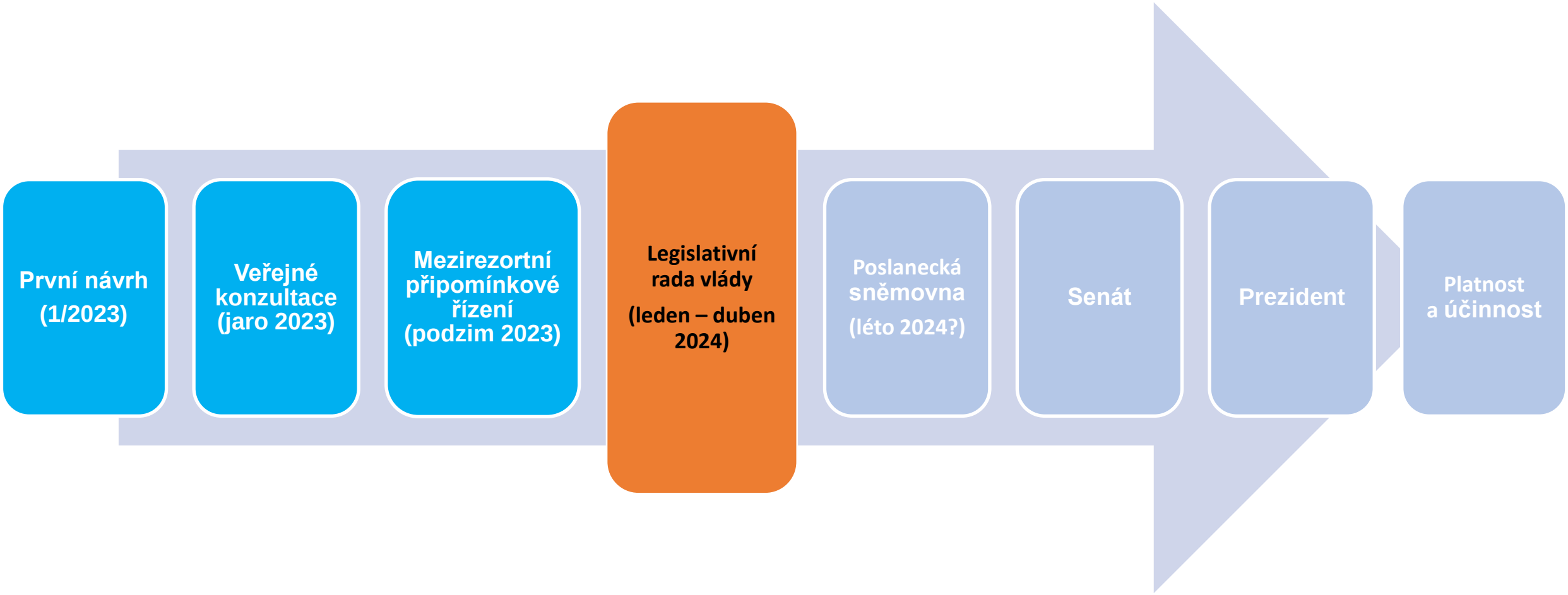
- Pracovní komise pro správní právo
- Pracovní komise pro soukromé právo
- Pracovní komise RIA
- Pracovní komise pro evropské právo

„Velká“ LRV proběhla 4. dubna

- Definice
- Široká zmocňovací ustanovení
- Procesní otázky – vyloučení rozkladu
- Legislativně technické připomínky, složitý jazyk
- Sankce – zejména zákaz činnosti statutárního zástupce
- Návrh není v rozporu s ústavou

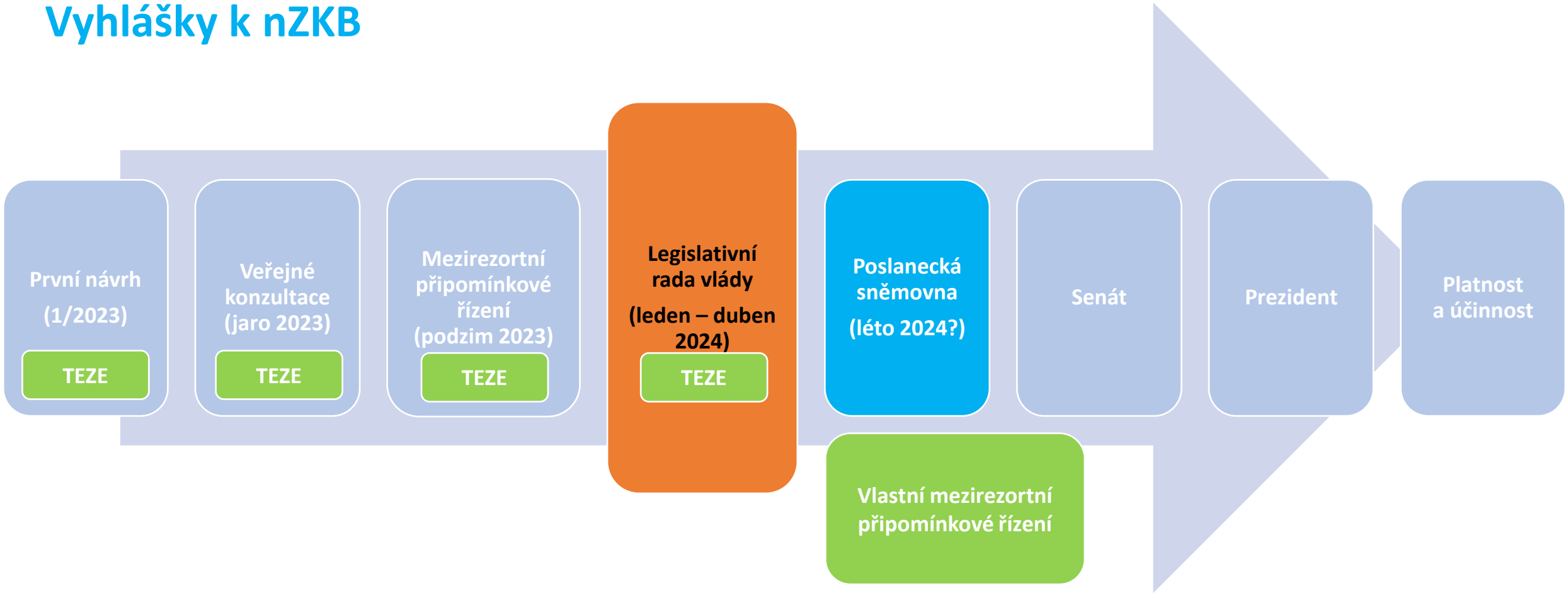
- **Projednávání bylo přerušeno**

Harmonogram



Harmonogram

Vyhlášky k nZKB



Nepřesnosti spojené s návrhem zákona

- **Pod zákon spadá vždy celý holding**
- **Pod zákon spadá jako regulovaná služba jen hlavní činnost naší firmy**
- **Vyšší režim je určen pro nadnárodní podniky a kritickou infrastrukturu**
- **Z hlášení incidentů vyplývá povinnost hlásit tisíce událostí denně**
- **Pokuty za porušení povinností jsou likvidační**
- **Rozsah mechanismu bezpečnosti dodavatelského řetězce je neomezený**
- **Návrh přináší neomezenou koncentraci pravomocí v rukou jednoho orgánu (NÚKIB)**

Ale regulace není jen o NIS2 a NZKB…

1. **The directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)**
2. **The Digital Operation Resilience Act (DORA)**
3. **The Critical Entities Resilience Directive (CER)**
4. **The Cybersecurity Act (CSA)**
5. **The European Cyber Resilience Act (CRA)**
6. EU Cyber Solidarity Act
7. **The General Data Protection Regulation (GDPR)**
8. The European ePrivacy Regulation
9. The European Data Governance Act (DGA)
10. The Digital Services Act (DSA)
11. The Digital Markets Act (DMA)
12. The European Chips Act

1. The European Data Act
2. The Artificial Intelligence Act
3. The Strategic Compass for Security and Defence
4. The European Cyber Defence Policy Framework
5. The EU Cyber Diplomacy Toolbox
6. 5G Toolbox
7. Regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union
8. The European Health Data Space (EHDS)
9. … and more in the near future

Děkuji za pozornost

nis2.nukib.gov.cz

regulace@nukib.cz

PRÁVNÍ PROSTOR

ODBORNÝ KONGRES

Děkujeme

kongrespravniprostor.cz