

AKTUÁLNÍ STAV NOVÉHO NÁVRHU ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI

NÚKIB



Národní úřad
pro kybernetickou
a informační
bezpečnost



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 17. 7. 2024 schválen vládou a předložen do Poslanecké sněmovny jako [Sněmovní tisk 759 \(psp.cz\)](#); 13. 8. 2024 mu byl přidělen zpravodaj a garanční výbor – Bezpečnostní výbor PSP**
- **Transpoziční termín** směrnice je stanoven na 17. října 2024

Nový zákon o kybernetické bezpečnosti v LRV

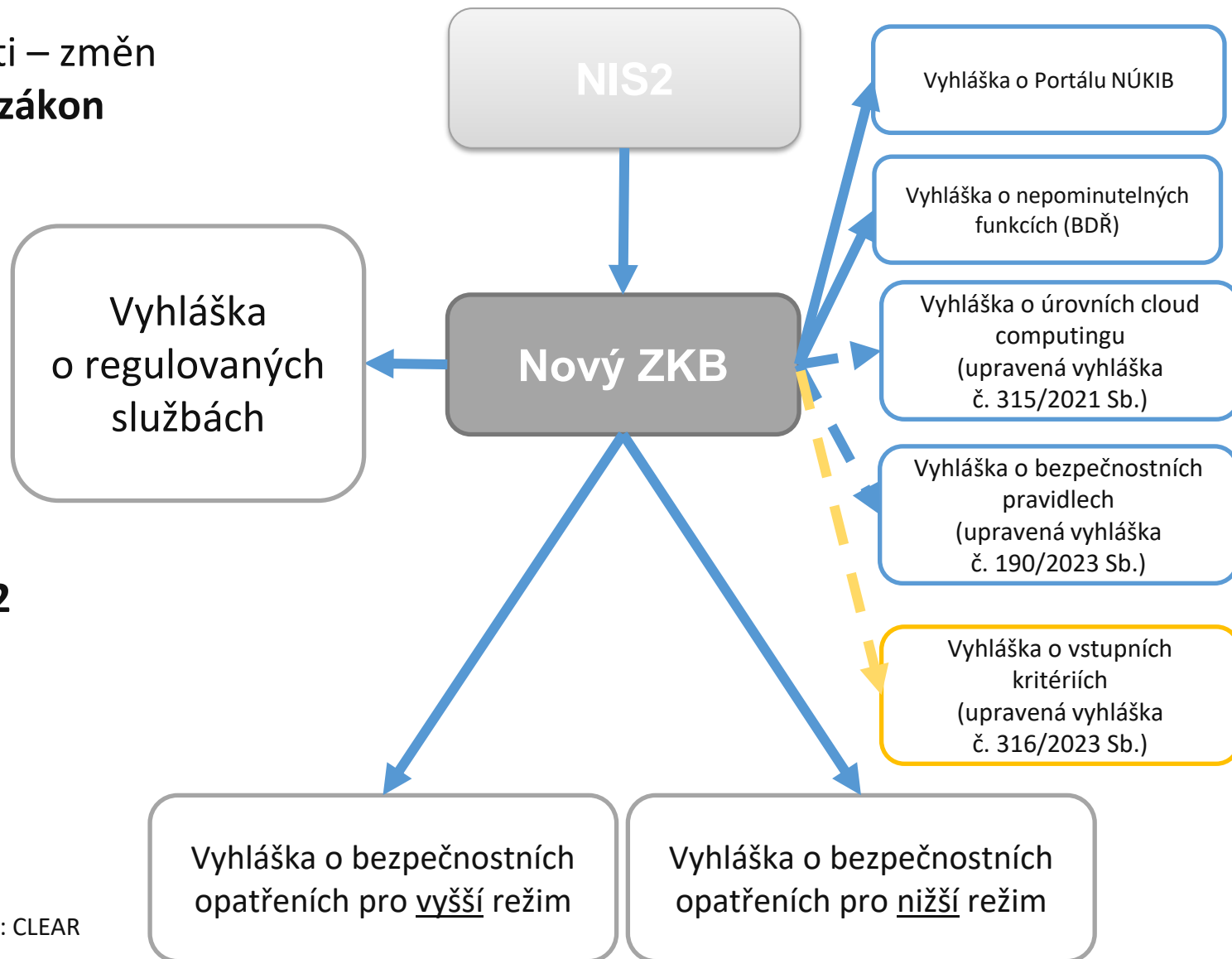


Nový zákon o kybernetické bezpečnosti – změna je tolik, že bylo **potřeba vytvořit nový zákon**
= zcela nová úprava – 73 paragrafů

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

Reálně se ale bude upravovat ještě jedna vyhláška navíc, ale ne kvůli NIS2 (č.316/2023)

Celý návrh zveřejněn zde:
<https://portal.nukib.gov.cz/>





Nový zákon dopadne na minimálně 6 000 organizací

- jde téměř výhradně o požadavek směrnice
- reguluje přes **107 služeb ve 22 odvětvích** (energetika, zdravotnictví, bankovníctví, 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**:

Režimu 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,...



Koho se nový ZKB bude týkat:

- Všech podle NIS2
- Nad rámec požadavků NIS2:
 - Vybrané subjekty v odvětví letectví – po konzultaci s ÚCL
 - Vybrané subjekty v oblasti výzkumu a vývoje (nekomerční užití, citlivá činnost, vysoké školy)
 - Obranný průmysl – vojenský materiál
 - Vybrané instituce veřejné správy

Velikostní kritérium

- **Sčítání velikosti podniků vychází z NIS2**
 - Přidána navíc speciální úprava:
 - Pokud jsou podniky odděleny na úrovni podpůrných aktiv nesčítají se
 - Územní samosprávy, OSS a ČNB nejsou podnikem
 - Veřejnosprávní zřizovatelé se nepřipočítávají ke zřizovaným organizacím (obec vs. vodárna)



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/nížší)
- **hlásit kybernetické bezpečnostní incidenty** – podle režimu v kterém je služba určena (vyšší/nížší)
- **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



Významné informační systémy (181/2014 Sb.)

Orientace na systém

Správce VIS/KII

Dopadová kritéria a povinné systémy

Výjimka z regulace pro obce

Jedna sada bezpečnostních opatření pro všechny organizace

Poskytovatel regulované služby (nZKB)

Orientace na službu

Poskytovatel regulované služby

Vyjmenované organizace

Zahrnutí ORP – nižší režim

Dvě sady bezpečnostních opatření pro různé organizace



Samoidentifikace

- Podobné významným informačním systémům
- Do 60 dní od zjištění, že jsem poskytovatelem regulované služby se registruji do portálu ([Portál NÚKIB \(gov.cz\)](https://portal.nukib.gov.cz) v pilotním provozu)
- NÚKIB vrátí rozhodnutí o registraci – potvrzení o naplnění kritérií – doručí poskytovateli regulované služby
- Do 30 dní od doručení rozhodnutí o registraci od NÚKIB hlásím kontaktní údaje - konkrétní osobu

Incidenty

- **Nižší režim** – posuzuje významnost dle vyhlášky, hlásí jen významné;
- **Vyšší režim** – KBI z kyberprostoru u kterých nelze vyloučit úmyslné zavinění (významnost a nutnost dalších hlášení posuzuje NÚKIB)
- Nově nejen prvotní hlášení - i průběžné a závěrečná zpráva o incidentu
- Lhůty – délka daná NIS2 (do 24 hodin po zjištění KBI)

Bezpečnostní opatření

- Do 1 roku od doručení rozhodnutí o registraci (pro nové)
- Původní povinné osoby – dodržují původní úpravu v době přechodného roku – přechází na nový ZKB

Provozovatel informačního systému

- Zrušen – nově jen významný dodavatel
- Dodavatelské společnosti regulovány jako MSP a MSSP



- Mechanismus prověřování bezpečnosti dodavatelského řetězce je nástroj, kterým ČR realizuje **strategickou kontrolu dodavatelského řetězce** nad nejkritičtějšími službami.
- Dopadne na poskytovatele strategicky významných služeb – jedná se o **cca 150 nejvíce klíčových subjektů** ze sektorů: veřejná správa, energetika, letecká doprava, drážní doprava, digitální infrastruktura a služby.
- Umožňuje ve velmi výjimečných případech opatřením obecné povahy **omezit nebo zakázat rizikového dodavatele** do nejkritičtější infrastruktury.
- Má za cíl **odhalit hrozby dříve**, než budou moci způsobit narušení bezpečnosti informací, a tím také **přispívá k bezpečnosti a odolnosti** strategicky významné služby.



- X ČR má jako jediná mechanismus BDŘ, který je navíc příliš přísný a neadekvátní**
 - Spíše naopak - obdobné mechanismy fungují i v jiných státech v EU i mimo EU. Oproti daným státům se však náš mechanismus vyznačuje **transparentním procesem vyřazování a množstvím zákonných brzd.**
- X Rozsah mechanismu je nepřiměřeně široký/neomezený**
 - Mechanismus je **omezený na úrovni zákona**, přičemž **dopadá pouze na nekritičtější služby**, a to pouze na ty jejich části, které jsou nezbytné z pohledu poskytování strategicky významné služby. Povinné subjekty mají navíc možnost požádat o výjimku ze zákazu.
- X Všechny pravomoci jsou koncentrovány pouze do rukou NÚKIB**
 - NÚKIB bude o omezení či zákazu dodavatele rozhodovat ve spolupráci s mnoha orgány. Do procesu prověřování BDŘ či do samotného vydávání OOP je zapojena například **Bezpečnostní rada státu, klíčová ministerstva a také samotná vláda.**



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

- Od počátku roku 2024 přes centrální e-mail regulace@nukib.cz - 280 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 40 národních i mezinárodních konferencí, řada bilaterálních zahraničních jednání
- Aktivní komunikace s 28 svazy a oborovými sdruženími

Informační podpora

- Web nis2.nukib.gov.cz - 485 302 přístupů k 19. 8 2024 (AJ verze přes 13 000)
- 1. 8. 2024 byl spuštěn Portál NÚKIB, na který byl k 2. 9. 2024 přesunut obsah webu NIS2 <https://portal.nukib.gov.cz/>

Vyjednávání na EU úrovni

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

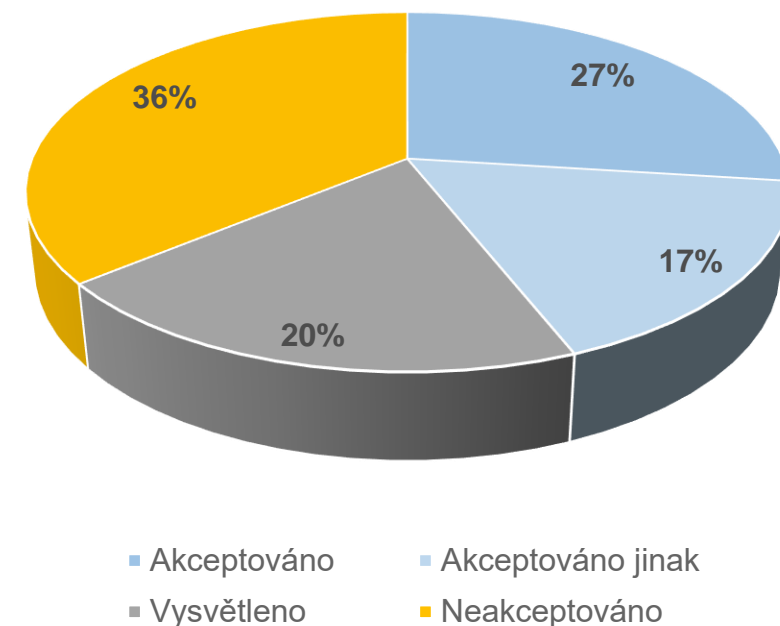
- Souhlasně bylo vypořádání 589 připomínek (**2/3 z celkového počtu**)

Rozpor přetrval na jednání vlády 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

Způsob vypořádání



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**
- **LRV neopakuje MPŘ – ŘEŠÍ SE TAM JINÉ OTÁZKY (nikoli věcné)**

Statistické okénko ohledně přerušování zákonů na LRV – za rok 2023

- Celkem se v roce 2023 projednalo 35 návrhů zákonů
- Z toho bylo 2 x věcný návrh zákona, 13 x návrh nového zákona, 18 x novelizace zákona, 1 x novelizace vyhlášky, 1 x mezinárodní smlouva
- Relevantní je projednávání návrhu nového zákona (tedy jako ZKB) – 13 x
- **Z těch 13 návrhů zákona bylo 11 x přerušeno, 2 x doporučeno ke schválení**
- z těch 18 novelizací je to 7x přerušeno, 10x doporučeno ke schválení ve znění připomínek a 1x není uveden závěr
- **= přerušování není nic nezvyklého**

Co je LRV?

- *poradní orgán vlády*
- *Posuzuje zda jsou legislativní návrhy:*
 - *v souladu s ústavním pořádkem a s ostatními součástmi právního řádu České republiky,*
 - *v souladu s mezinárodními smlouvami,*
 - *v souladu s právem Evropské unie,*
 - *přehledně členěny, srozumitelně a jednoznačně formulovány,*
 - *soulad s ostatními závaznými pravidly legislativního procesu.*



Obecně došlo k drobným formulačním úpravám některých definic, nejzásadnější změny jsou popsány níže. **Úpravou definic se ale nijak nemění přístup zákona k vymezení aktiv.**

- Nová definice **aktiva**: *fyzický nebo digitální prostředek, osoba nebo činnost související se zpracováváním informací a dat v elektronické podobě.*
- **Určování povinných osob** - věcně funguje zákon pořád stejně, tj. dochází buď k sebeidentifikaci na základě vyhlášky o regulovaných službách, nebo k určení Úřadem.
 - V obou případech hovoříme o naplnění podmínek pro registraci regulované služby (sebeidentifikace podle § 4 / určení Úřadem podle § 5).
 - Úřad vždy rozhoduje o registraci regulované služby. **Od doručení rozhodnutí o registraci regulované služby pak poskytovatelům běží lhůty pro plnění dalších povinností.**
- **Kritéria pro registraci se mění na podmínky pro registraci**
- **Hlášení údajů** bylo pouze zestručněno a byla odstraněna explicitní povinnost zajištění zastupitelnosti osob oprávněných jednat za poskytovatele regulovaných služeb
- **Stanovení rozsahu řízení kybernetické bezpečnosti** bylo zestručněno a popsáno srozumitelněji.



- Do ustanovení o **bezpečnostních opatřeních** byla přesunuta povinnost **vybírat svého dodavatele v souladu s požadavky vyplývajícími z bezpečnostního opatření a zahrnovat požadavky vyplývající z bezpečnostního opatření do smluv s dodavatelem.**
- **Hlášení incidentů** doznalo pouze kosmetických úprav s ohledem na změny terminologie při ohlašování/registraci.
- **Varování** nově platí i pro režim nižších povinností
- **Mechanismus BDŘ se věcně nějak nemění.** Došlo pouze k drobným formulačním změnám či doplněním a k odstranění odstavců, které byly nadbytečné.
- **Nepominutelnou funkcí** je činnost nebo vlastnost aktiva zajišťující provoz strategicky významné služby, jejichž narušení by mohlo mít závažný dopad na poskytování strategicky významné služby.
- **Přestupky byly rozděleny** z jednoho do tří paragrafů pro větší přehlednost
- O **pozastavení výkonu řídicí funkce** členovi statutárního orgánu nově **může rozhodnout přímo NÚKIB.**
- **Stav kybernetické nebezpečí (SKN)** funguje pořád stejně – došlo především k legislativně-technickým změnám. O uložení opatření v rámci řešení SKN rozhoduje samotný Úřad, nikoliv ředitel

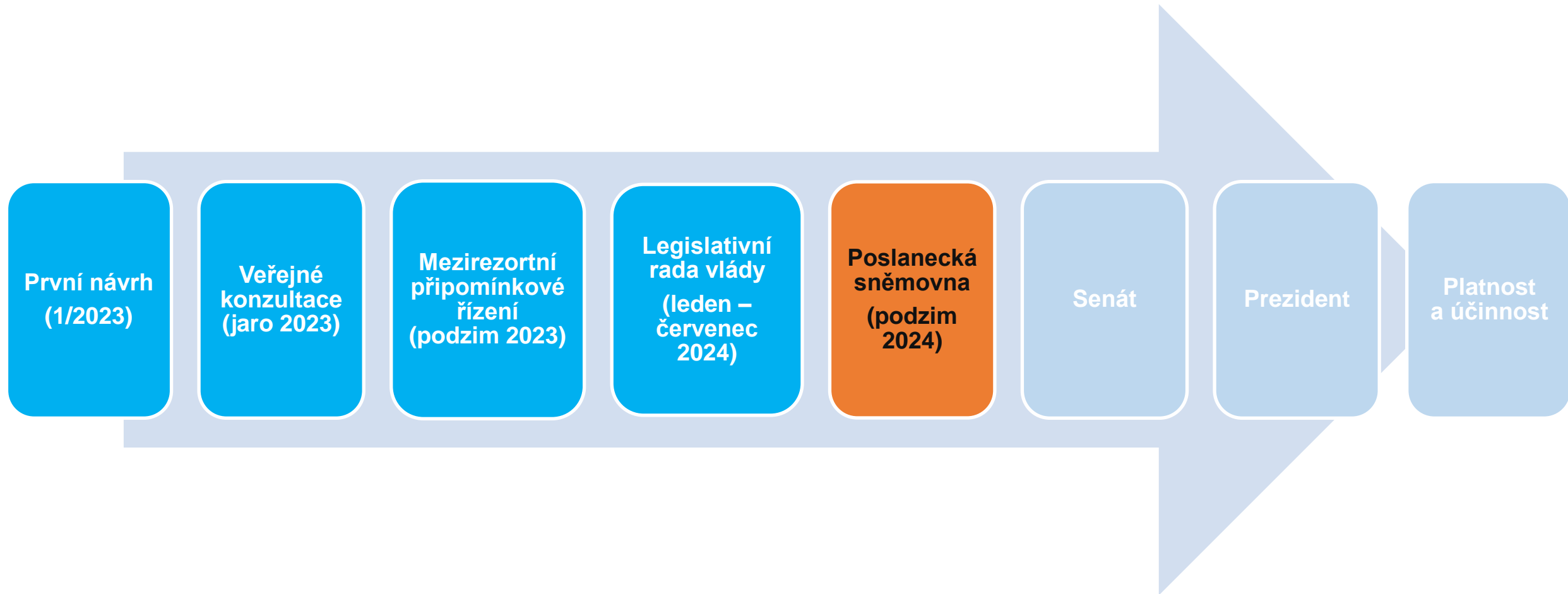


- Návrh zákona byl vládou schválen 17. 7. 2024
- Na základě rozhodnutí vlády došlo k úpravě v procesu vydávání opatření obecné povahy (OOP) sloužícího k realizaci mechanismu prověřování bezpečnosti dodavatelského řetězce.
- Navrhovaná verze:
 - Ministerstvo vnitra, Ministerstvo zahraničních věcí a Ministerstvo průmyslu a obchodu vydávali závazné stanovisko v případě, že je lhůta stanovena OOP kratší než odpisová lhůta nebo 5 let.

Nová verze:

Vláda ČR rozhoduje o postupu v případě, že je lhůta k vyloučení či omezení dodavatele navržená v OOP kratší než odpisová lhůta nebo 5 let.

- V určitých případech tedy dochází tedy k přímému zapojení vlády do procesu plynoucího z Mechanismu prověřování dodavatelského řetězce.
- Do procesu je nadále ve **všech případech** zapojena **Bezpečnostní rada státu**, která má možnost konkrétní případy eskalovat na vládní úroveň.



Vyhlášky k nZKB





Přehled v organizaci

- Jaké vykonávám agendy a poskytují služby?
- Co pro výkon těchto agend potřebuji?
- Z toho vyplývá rozsah, ve kterém KB řeším.

Aktuální stav KB

- Mám již zavedena některá opatření?
- Zdokumentuji aktuální stav zavedených a nezavedených opatření.

Určení priorit

- Jaké mám finanční a personální kapacity?
- Co je má prioritní služba?
- Provedu analýzy, stanovím plán se zohledněním kapacit a priorit.

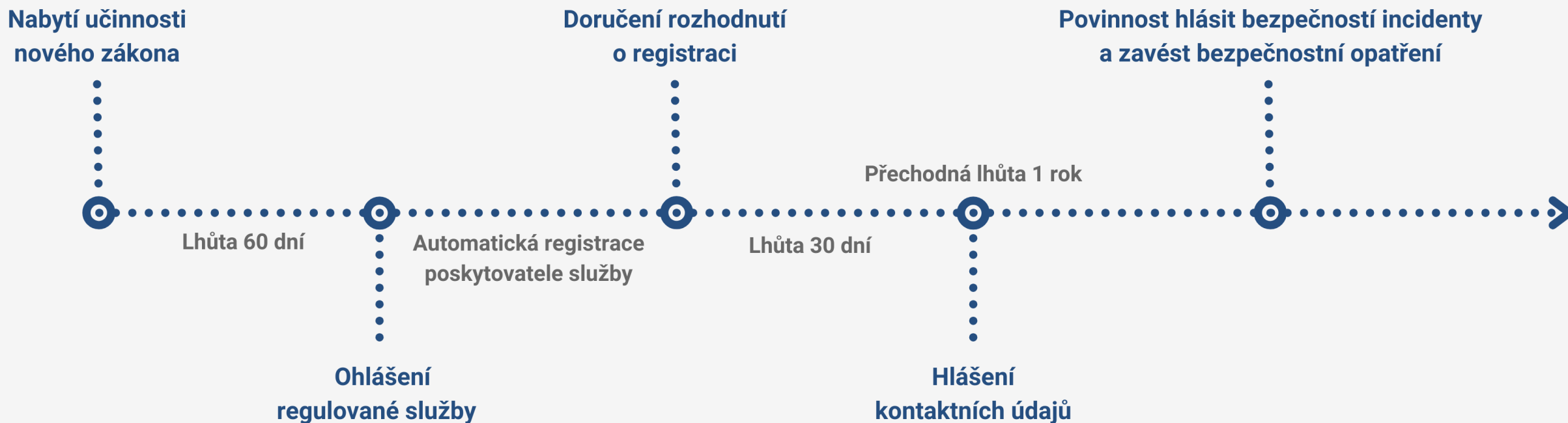
Zavádění opatření

- Určím osobu odpovědnou za KB.
- Priorita je vzdělávání zaměstnanců včetně vedení.
- Vytvořím bezpečnostní politiku, kterou lze fakticky používat.
- Pokračuji dle plánu.

Zásada přiměřenosti:

- Náklady na zaváděné opatření by neměly převyšovat náklady na případnou realizaci kybernetického incidentu.
- Nechci všechno najednou, postupně se zlepšuji.

Jak to bude s termíny?





- **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)**
- **Když nZKB nebude v transpozičním termínu schválen bude se postupovat podle NIS2**
- **Cena je nepřiměřená**



- **Přiměřenost nákladů** – bezpečnostní opatření nemá být dražší, než jaké jsou náklady realizovaného incidentu (Součást obou vyhlášek jako princip)

Cost of a Data Breach Report 2023 od IBM:.

- průměrné globální náklady na únik dat 4,45 milionu USD, tedy 103,5 milionu Kč
- nárůst o 15 % za poslední tři roky

123 SMB Cybersecurity Statistics

- 61 % malých a středně velkých podniků terčem kybernetického útoku
- průměrné náklady na řešení KBI u nich v roce 2023 od 826 do 653 587 USD

Nová zpráva Izraelské INCD: analýza nákladů KBI na izraelskou ekonomiku:

- nejméně 12 miliard NIS ročně = přes 76 miliard Kč
- základní opatření mohou snížit šance na útok o 30–50 %
- Kybernetická kriminalita se v roce 2025 stane 3. největší ekonomikou světa



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
13. The European Data Act
14. The Artificial Intelligence Act
15. The Strategic Compass for Security and Defence
16. The European Cyber Defence Policy Framework
17. The EU Cyber Diplomacy Toolbox
18. 5G Toolbox
19. Regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union
20. The European Health Data Space (EHDS)
21. ... and more in the near future



Děkuji za pozornost

regulace@nukib.gov.cz

! <https://portal.nukib.gov.cz/> !

