Návrh nového zákona o kybernetické bezpečnosti – aktuální stav

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Jan Hénik
oddělení regulace veřejného sektoru

24. září 2024

TLP: CLEAR

Východiska obsahu návrhu nZKB

Směrnice NIS 2.0

Transpozice směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148

Mechanismus BDŘ

Úkol z usnesení Bezpečnostní rady státu č. 41 ze dne 21. června 2022 k Bezpečnosti dodavatelských řetězců strategické infrastruktury státu, č. j. 28261/2022-UVCR

Zlepšení a zkušenosti

Reflexe poznatků a dosavadních zkušeností, odstranění současných nedostatků, zohlednění podnětů a připomínek a další doplňující úpravy

Nový zákon o kybernetické bezpečnosti v LRV

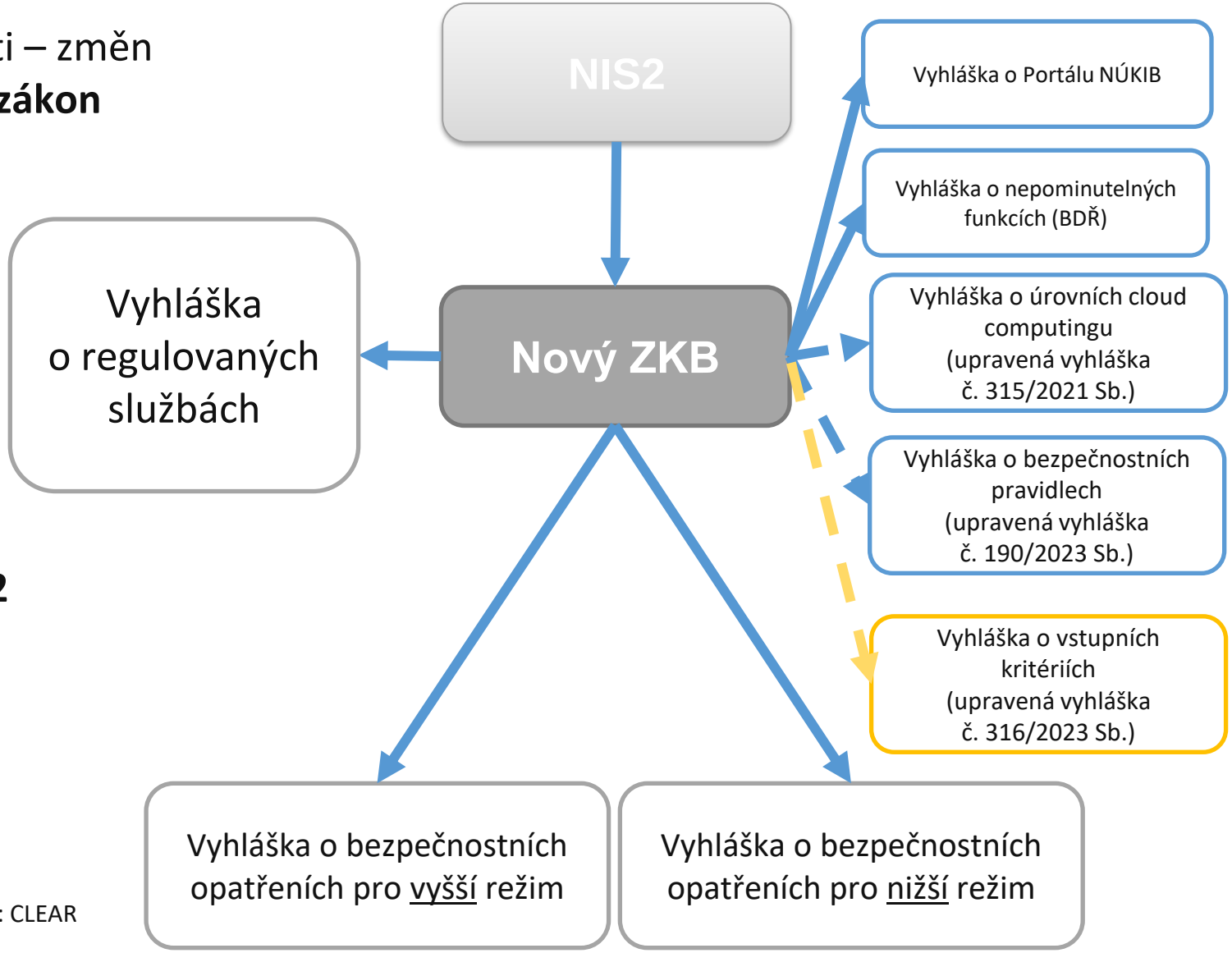
Nový zákon o kybernetické bezpečnosti – změn je tolik, že bylo **potřeba vytvořit nový zákon**

= 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/



Hlavní body nZKB

Samoidentifikace	Režimy	4 pilíře povinností	Národní bezpečnost
22 odvětví	Vyšší režim	Kontaktní údaje	BDŘ
100+ služeb	Nižší režim	Bezpečnostní opatření	Zajištění dostupnosti z ČR
Samoposouzení		Hlášení incidentů	SKN
Registrace na Portálu		Plnění protiopatření	

Povinné osoby – odvětví, služby

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 oddělen<u>y na úrovni podpůrných aktiv nesčítají se</u>
    - Územní samosprávy, OSS a ČNB nejsou podnikem
    - Veřejnosprávní zřizovatelé se nepřipočítávají ke zřizovaným organizacím (obec vs. vodárna)

Regulované služby

Regulovaná služba	
Služba	**Podmínky významnosti poskytovatele regulované služby a jeho režim**
1.1. Výkon svěřených pravomocí	Orgán nebo osoba je I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že je a) ústředním orgánem státní správy, b) jiným správním úřadem s celostátní působností neuvedeným v písm. a), a to včetně ústředí a generálního ředitelství územně dekoncentrovaných (specializovaných) orgánů státní správy, c) Kanceláří prezidenta republiky, d) Kanceláří Senátu, e) Kanceláří Poslanecké sněmovny, f) Českou národní bankou, g) Policejním prezidiem, h) útvarem policie s celostátní působností, i) Generální inspekcí bezpečnostních sborů

II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je

a) územně dekoncentrovaným (specializovaným) orgánem státní správy,

b) profesní komorou[1][1],

c) vysokou školou,

d) Akademií věd České republiky, nebo

e) obcí s rozšířenou působností, nebo

f) městskou části hlavního města Prahy, na kterou byl přenesen výkon působnosti dle zákona o hlavním městě Praze[2][2].

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

Bezpečnostní opatření – rozdíly vyšší a nižší režim

- **Redukovaná bezpečnostní opatření pro nižší režim**

organizační opatření – **vyšší** režim

1. systém řízení bezpečnosti informací,
2. povinnosti pro vrcholové vedení,
3. bezpečnostní role,
4. řízení bezpečnostní politiky a bezpečnostní dokumentace,
5. řízení aktiv,
6. řízení rizik,
7. řízení dodavatelů,
8. bezpečnost lidských zdrojů,
9. řízení změn,
10. akvizice, vývoj a údržba,
11. řízení přístupu,
12. zvládání kybernetických bezpečnostních událostí a incidentů,
13. řízení kontinuity činností a
14. audit kybernetické bezpečnosti

technická opatření – **vyšší** režim

1. fyzická bezpečnost,
2. bezpečnost komunikačních sítí,
3. správa a ověřování identit,
4. řízení přístupových oprávnění,
5. detekce kybernetických bezpečnostních událostí,
6. zaznamenávání událostí,
7. vyhodnocování kybernetických bezpečnostních událostí,
8. aplikační bezpečnost,
9. kryptografické algoritmy,
10. zajišťování dostupnosti regulované služby,
11. zabezpečení průmyslových, řídících a obdobných specifických aktiv

bezpečnostní opatření – **nižší** režim

1. zajišťování kybernetické bezpečnosti,
2. povinnosti vrcholového vedení,
3. bezpečnost lidských zdrojů,
4. řízení kontinuity činností,
5. řízení přístupu,
6. řízení identit a jejich oprávnění,
7. detekce a zaznamenávání kybernetických bezpečnostních událostí,
8. řešení kybernetických bezpečnostních incidentů,
9. bezpečnost komunikačních sítí,
10. aplikační bezpečnost,
11. kryptografické algoritmy

Bezpečnostní opatření pro nižší a vyšší režim - rozdíl

NIŽŠÍ REŽIM

§ 7
Řízení kontinuity činností

Povinná osoba v rámci řízení kontinuity činností

1. v rámci primárních aktiv stanoví jejich prioritu a pořadí a postupy jejich obnovy,
2. stanoví odpovědnosti a povinnosti při obnově podle písm. a),
3. vytváří pravidelné zálohy nastavení technických aktiv, informací a dat nezbytných zejména pro účely obnovy regulované služby pro případ kybernetického bezpečnostního incidentu.

VYŠŠÍ REŽIM

§ 16
Řízení kontinuity činností

1. Povinná osoba v rámci řízení kontinuity činností
a) stanoví metodiku pro provedení analýzy dopadů,
b) pomocí analýzy dopadů vyhodnotí a dokumentuje možné dopady kybernetických bezpečnostních incidentů a zohlední hodnocení rizik podle § 9, v rámci kterého posoudí možná rizika související s ohrožením kontinuity činností,
c) na základě výstupů analýzy dopadů a hodnocení rizik podle písmene b) stanoví cíle řízení kontinuity činností formou určení
    i) minimální úrovně poskytovaných služeb, která je přijatelná pro užívání, provoz a správu regulované služby,
    ii) doby obnovení chodu, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb regulované služby a
    iii) bodu obnovení dat jako časové období, za které musí být zpětně obnovena data po kybernetickém bezpečnostním incidentu nebo po selhání,
d) stanoví politiku řízení kontinuity činností, která obsahuje naplnění cílů podle písmene c) a stanoví práva a povinnosti administrátorů a osob zastávajících bezpečnostní role,
e) vypracuje, aktualizuje a pravidelně testuje plány kontinuity činností a plány obnovy související s poskytováním regulované služby a
f) realizuje bezpečnostní opatření pro zvýšení odolnosti podle § 27.
2. Cíle řízení kontinuity podle odst. 1 písm. c) tohoto ustanovení jsou stanoveným časem a kvalitou regulované služby podle § X [Zajištění dostupnosti strategicky významné služby] zákona. Stanoveným časem je doba obnovení chodu podle odst. 1 písm. c) bod ii) tohoto ustanovení a stanovenou kvalitou regulované služby je minimální úroveň poskytovaných služeb podle odst. 1 písm. c) bodu i) tohoto ustanovení.

Nejvýznamnější rozdíly v regulaci veřejného sektoru

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

Hlavní změny ve fungování pro veřejnou správu

Samoidentifikace

- Podobné významným informačním systémům
- Do 60 dní od zjištění, že jsem poskytovatelem regulované služby se registruji do portálu (Portál NÚKIB (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

Bezpečnost dodavatelského řetězce

- 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.

- Umožnuje 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.

Mýty o bezpečnosti dodavatelského řetězce

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.**

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

- 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

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

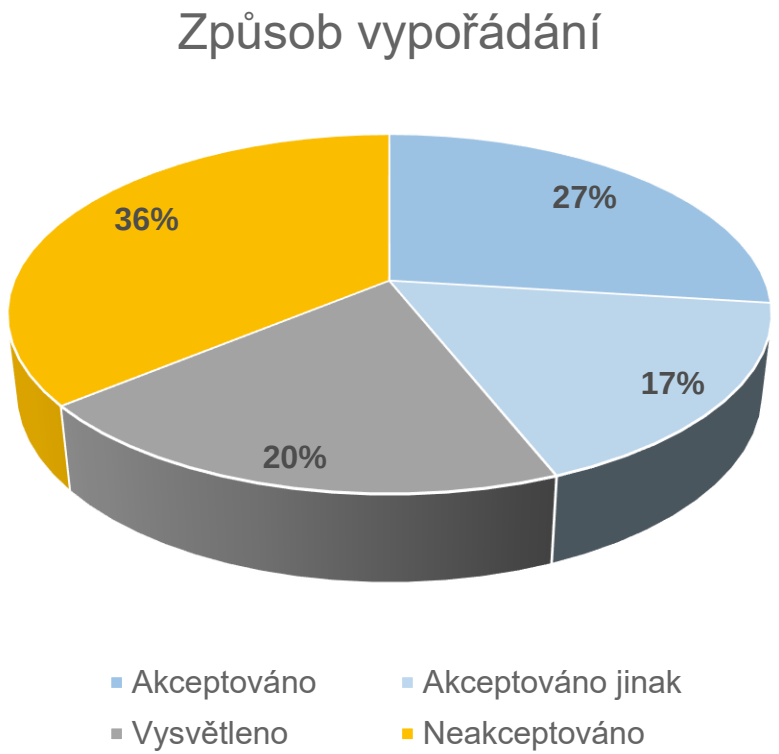
- 518 připomínek bylo zásadních, 368 připomínek bylo doporučujících

Za účelem vypořádání připomínek proběhlo 28 vypořádacích jednání

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

Rozpor 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

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**
- **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
- **= přerušení 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.*

Legislativní rada vlády – nejvýznamnější změny

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.

Legislativní rada vlády – nejvýznamnější změny

- 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 řídící 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

Jednání vlády – provedena změna

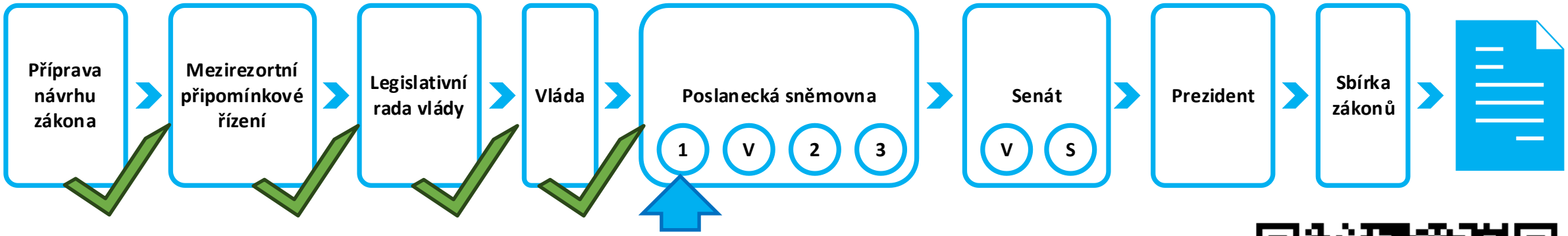
- Návrh zákona byl vládou schválen 17. 7. 2024
- Na základě rozhodnutí vlády došlo k úpravě v procesu vydávání opatření obecné povahy (OOP) sloužícího k realizaci mechanismu prověřování bezpečnosti dodavatelského řetězce.
- Navrhovaná verze:
  - Ministerstvo vnitra, Ministerstvo zahraničních věcí a Ministerstvo 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.

Návrh nZKB v legislativním procesu



Vláda předložila Poslanecké sněmovně návrh zákona 25. července 2024.

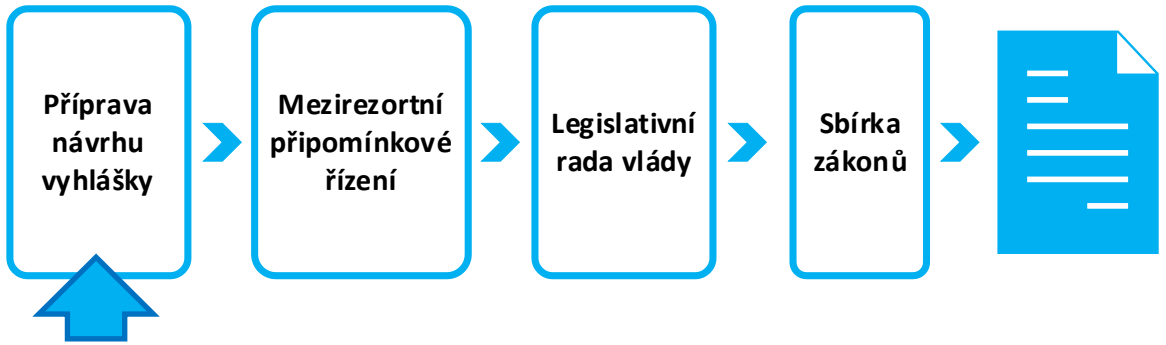
Návrh zákona rozeslán poslancům jako **sněmovní tisk 759/0.**

Předsedkyně sněmovny **projednání zákona doporučila,** určila **zpravodaje** a navrhla přikázat návrh zákona k projednání **Výboru pro bezpečnost** (později doplněn také Hospodářský výbor).

Projednávání tisku navrženo na pořad 112. schůze Poslanecké sněmovny (od 10. září 2024).

Sněmovní tisk 759 (psp.cz)

Samostatný proces přijímání vyhlášek k nZKB



S návrhem zákona se připravují také teze jeho vyhlášek.

Národní úřad pro kybernetickou a informační bezpečnost připravil teze již od počátku velmi podrobně (i s odůvodněním.)

Tím, jak návrh zákona prochází legislativním procesem přichází čas zahájit také oficiální legislativní proces vyhlášek.

1. **Vyhláška o regulovaných službách**
2. **Vyhláška o bezpečnostních opatřeních pro vyšší režim**
3. **Vyhláška o bezpečnostních opatřeních pro nižší režim**
4. **Portálová vyhláška**
5. **Vyhláška o nepominutelných funkcích (BDŘ)**
6. **Vyhláška o bezpečnostních úrovních (cloud)**
7. **Vyhláška o bezpečnostních pravidlech (cloud)**

Jak se na zákon připravit?

Přehled v organizaci

- Jaké vykonávám agendy a poskytuji 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

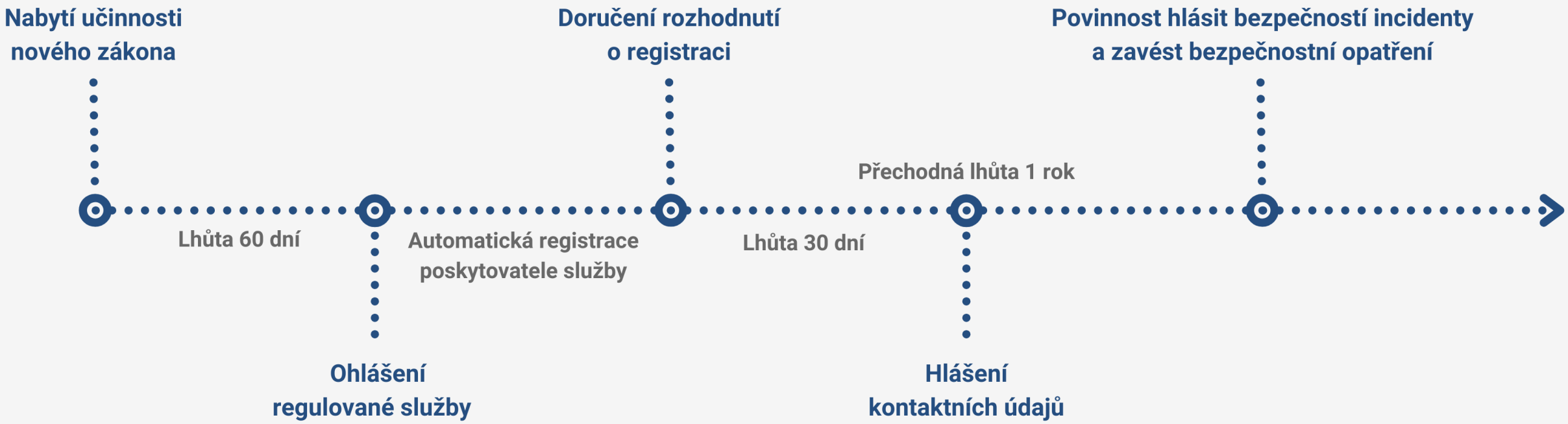
- Určím osobu odpovědnou za KB.
- Priorita je vzdělávání zaměstnanců včetně vedení.
- Vytvořím bezpečnostní politiku, kterou lze fakticky používat.
- Pokračuji dle plánu.

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?



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

Nepřesnosti spojené s návrhem zákona: 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:.	123 SMB Cybersecurity Statistics	Nová zpráva Izraelské INCD: analýza nákladů KBI na izraelskou ekonomiku:
• průměrné globální náklady na únik dat 4,45 milionu USD, tedy 103,5 milionu Kč • nárůst o 15 % za poslední tři roky	• 61 % malých a středně velkých podniků terčem kybernetického útoku • průměrné náklady na řešení KBI v roce 2023 od 826 do 653 587 USD	• 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

Děkuji za pozornost

regulace@nukib.gov.cz

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