Směrnice NIS2 a nový zákon o kybernetické bezpečnosti

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Zelinářské dny 2025

28. 1. 2025

TLP:CLEAR

Josef Alexa
referent
Odbor regulace

Disclaimer

- Tato prezentace má obecný informační a osvětový charakter a vychází ze znění návrhů dotčených právních předpisů ke dni 28. 1. 2025.

- Vzhledem ke stále probíhajícímu legislativnímu procesu, v němž se návrh nového zákona o kybernetické bezpečnosti a jeho prováděcí právní předpisy nacházejí, je tedy nutné k informacím obsaženým v této prezentaci přistupovat s tím vědomím, že v průběhu času může dojít k jejich změně.

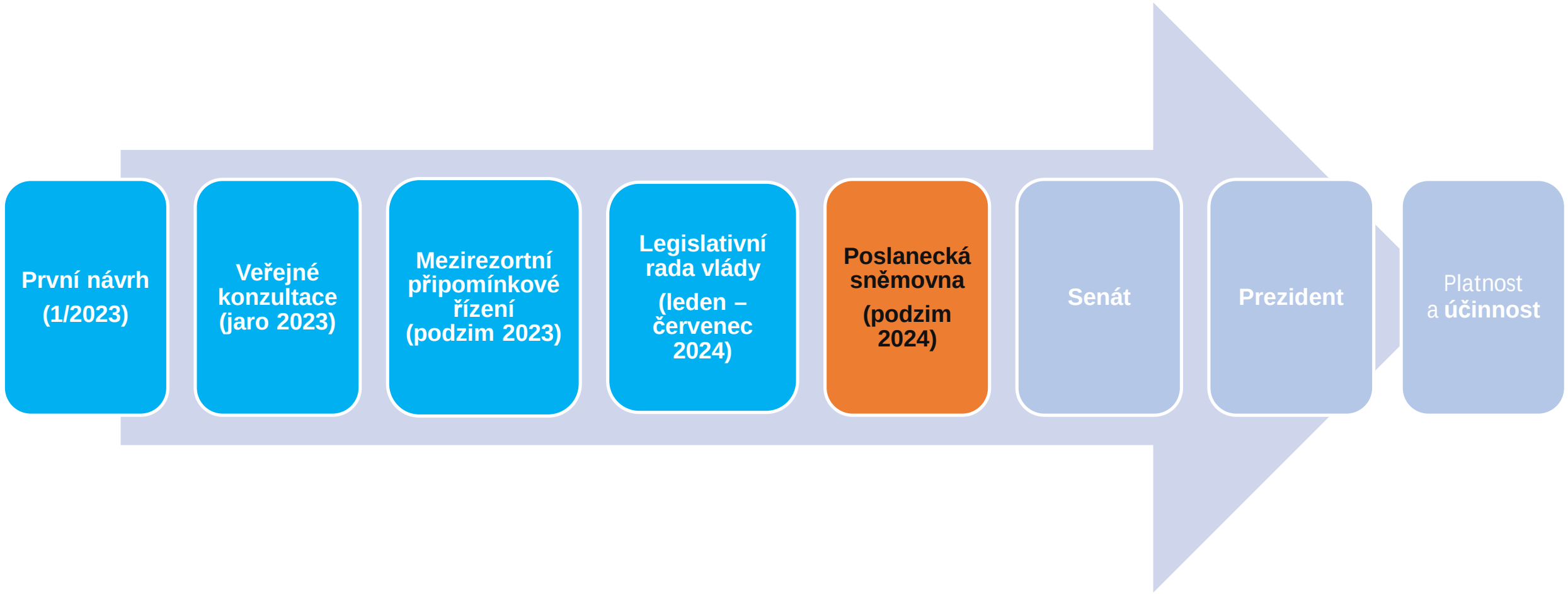
- Tato prezentace může obsahovat informace zahrnující názory a plány NÚKIB jakožto gestora dotčené problematiky.

Směrnice NIS2 a návrh nového zákona

- směrnice NIS2 přijata 14. 12. 2022
- nejedná se o přímo použitelný akt EU ➡ její obsah je nutné transponovat
- připraven návrh nového zákona o kybernetické bezpečnosti
- návrh 17. 7. 2024 schválen vládou ČR a předložen do Poslanecké sněmovny (zařazen na pořad 112. schůze – tj. od 10. září 2024)

- transpoziční lhůta směrnice NIS2: do 17. 10. 2024
- předpokládaná účinnost nZKB: od druhé poloviny roku 2025

Harmonogram legislativního procesu nZKB



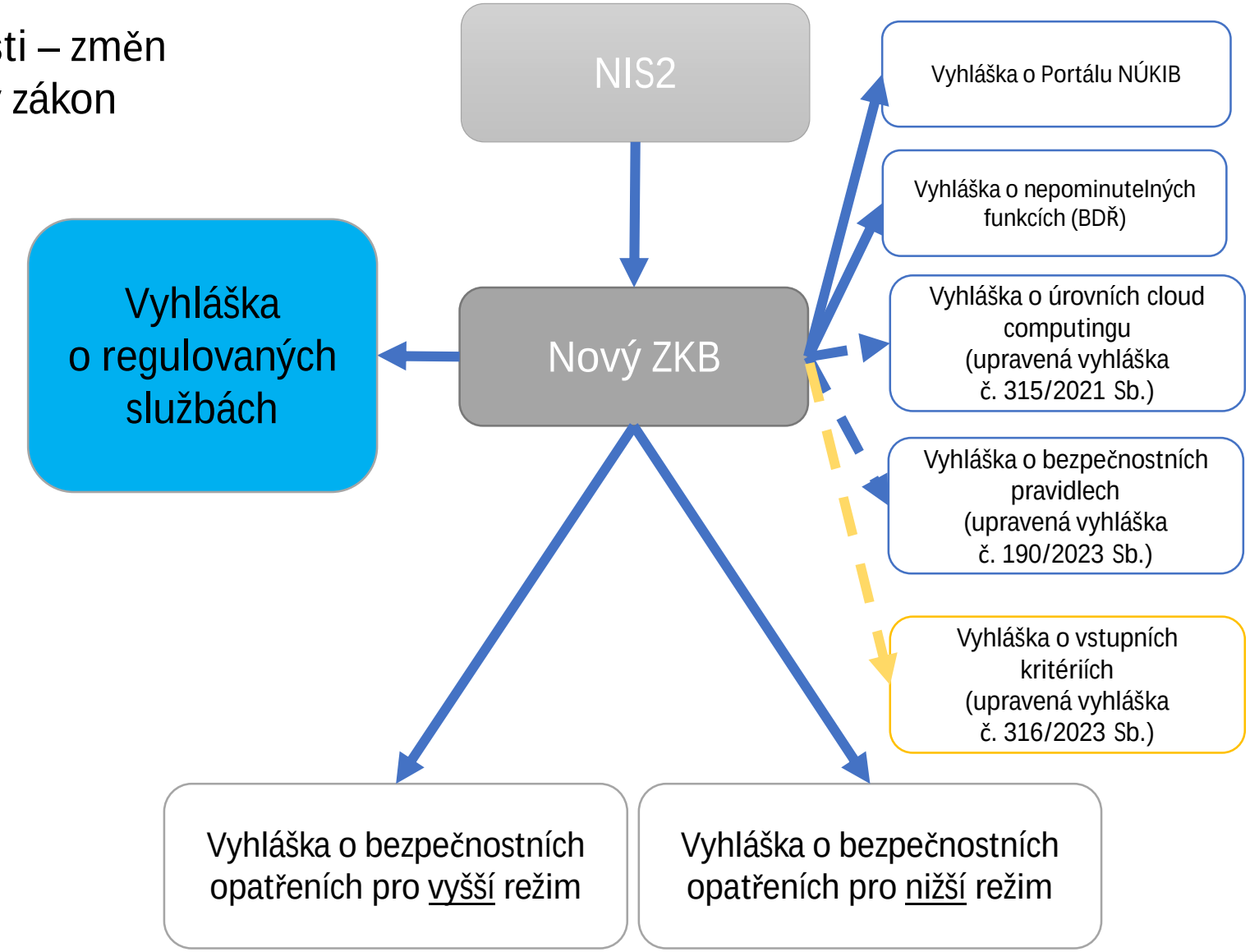
Prováděcí právní předpisy

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

= zcela nová úprava – 73 paragrafů

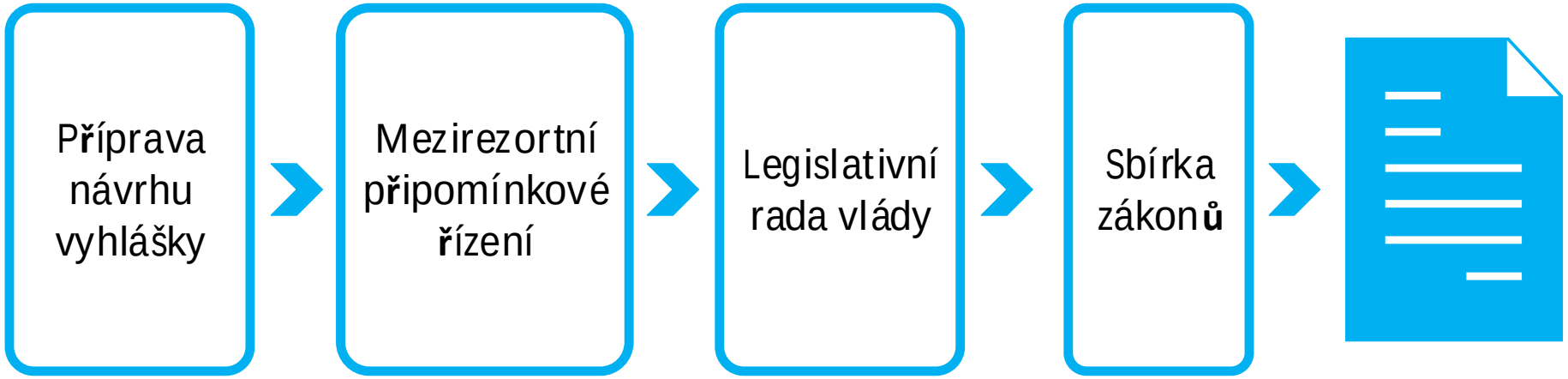
Verze po mez. připomínkovém řízení předpokládá navíc 7 vyhlášek.

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



Prováděcí předpisy k nZKB

- samostatný legislativní proces



- probíhá zpracování tezí ➡ jsme v závěrečné fázi jejich příprav
- postupné zahájení oficiálního legislativního procesu vyhlášek
- účinnost vyhlášek: společně s účinností nZKB

Vyhláška o regulovaných službách - obecně

- jeden z prováděcích předpisů nZKB

- <u>stanovuje:</u>

  a) seznam služeb a vymezení podmínek významnosti poskytovatele regulované služby

  b) rozdělení poskytovatelů regulovaných služeb do režimů

  c) kritéria pro určení služby jako strategicky významné

- 22 odvětví
- více než 100 regulovaných služeb
- 2 režimy povinností: režim vyšších povinností vs. režim nižších povinností
- hlavní (nikoli však jediné) kritérium pro zahrnutí do regulace: velikost subjektu

Jak bude regulace fungovat?

- aby mohlo dojít k aplikaci nZKB, musí existovat:

1) REGULOVANÁ SLUŽBA

2) POSKYTOVATEL REGULOVANÉ SLUŽBY

- Podmínky obou musí být splněny současně!
- seznam regulovaných služeb stanovuje Vyhláška o regulovaných službách
- poskytovatele regulované služby stanovuje též Vyhláška o regulovaných službách

Konkrétní příklad z vyhlášky

8. Potravinářský průmysl

Regulovaná služba	
Služba	**Podmínky významnosti poskytovatele regulované služby a jeho režim**
8.1. Výroba potravin	Potravinářský podnik podle přímo použitelného předpisu Evropské unie[10], který se zabývá průmyslovou výrobou potravin, je poskytovatel regulované služby v režimu nižších povinností, v případě, že je velkým podnikem nebo středním podnikem.
8.2. Zpracování potravin	Potravinářský podnik podle přímo použitelného předpisu Evropské unie[11], který se zabývá průmyslovým zpracováním potravin, je poskytovatel regulované služby v režimu nižších povinností, v případě, že je velkým podnikem nebo středním podnikem.
8.3. Distribuce potravin	Potravinářský podnik podle přímo použitelného předpisu Evropské unie[12], který se zabývá velkoobchodní

Počítání velikosti podniku

Při počítání velikosti subjektu se postupuje v souladu s doporučením komise 2003/361/ES o definici mikropodniků, malých a středních podniků.

Pro posouzení velikosti subjektu musí být naplněn zaměstnanecký nebo finanční ukazatel.

Kategorie podniku	Počet zaměst-nanců: roční pracovní jednotka (RPJ)	Roční obrat	nebo	Bilanční suma roční rozvahy
Střední podnik	< 250	≤ 50 milionů EUR	nebo	≤ 43 milionů EUR
Malý podnik	< 50	≤ 10 milionů EUR	nebo	≤ 10 milionů EUR
Mikropodnik	< 10	≤ 2 miliony EUR	nebo	≤ 2 miliony EUR

PODNIKEM NENÍ:

i) organizační složka státu
ii) územní samosprávný celek
iii) Česká národní banka

Povinnosti poskytovatele reg. služby

Hlavní povinnosti

- hlásit kontaktní a další údaje *(Portál NÚKIB)*
- zavádět bezpečnostní opatření – podle určeného režimu (*vyšší/nižší*)
- hlásit kybernetické bezpečnostní incidenty – podle určeného režimu (*vyšší/nižší*)
- provádět protiopatření *(výstraha, varování, reaktivní protiopatření)*

Další povinnosti

- plnit povinnosti z tzv. Mechanismu bezpečnosti dodavatelského řetězce u vybraných (strategicky významných) služeb
- stanovit rozsah řízení kybernetické bezpečnosti – definuje rozsah regulace v organizaci
- informovat zákazníky o incidentech a hrozbách
- zajistit dostupnost z České republiky u vybraných (strategicky významných) služeb

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

Hlášení kybernetických bezpečnostních incidentů

CO SE HLÁSÍ?

- Kybernetické bezpečnostní incidenty, které:
  - ❑ mají původ v kybernetickém prostoru,
  - ❑ mají významný dopad na poskytování regulované služby, a
  - ❑ u nichž do 24 hodin od jejich detekce nelze vyloučit úmyslné zavinění

KOMU SE HLÁSÍ?

- Národnímu CERT

Jak to bude s termíny?

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.

Děkuji za pozornost

regulace@nukib.gov.cz

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