NOVÝ ZÁKON O KYBERNETICKÉ BEZPEČNOSTI

AKTUALITY A DOPORUČENÍ

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Petr Kopřiva
Vedoucí oddělení regulace dodavatelů informačních technologií

21. ledna 2025

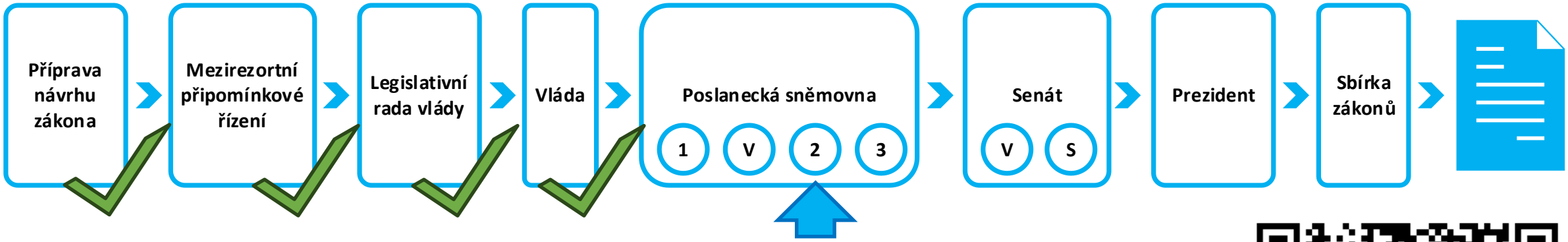
TLP: CLEAR

Shrnutí situace

- V České republice existuje zákon o kybernetické bezpečnosti **již od roku 2015**.
- Do současného zákona byly až následně promítnuty požadavky **směrnice NIS1**.
- Základem změn je nová **směrnice NIS2**, ale také potřeba zákon o kybernetické bezpečnosti aktualizovat.
- Směrnice NIS2 **změnila přístup k regulaci** – orientuje se již velmi plošně a zahrnuje do regulace (až) desítky tisíc nových organizací.
- Do návrhu zákona jsou promítnuty také **vnitrostátní instituty a požadavky**.
- Národní úřad pro kybernetickou a informační bezpečnost **připravil návrh** nového zákona o kybernetické bezpečnosti.
- **Termín pro transpozici** směrnice NIS2 uplynul 17. října 2024.
- Směrnice NIS2 nikomu nic nepřikazuje ani nikoho nezavazuje, **stěžejním legislativním dokumentem** je nový zákon o kybernetické bezpečnosti.

Návrh nZKB v legislativním procesu

Národní úřad pro kybernetickou a informační bezpečnost



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 a Výbor pro obranu).

Projednávání tisku v 1. čtení proběhlo 17. září 2024, **druhé čtení dnes 21. ledna 2025.**

Sněmovní tisk 759 (psp.cz)

Východiska obsahu návrhu nZKB

Národní úřad pro kybernetickou a informační bezpečnost

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 ZKB – hlavní body

Nový zákon dopadne na minimálně 6 000 organizací

- jde téměř výhradně o požadavek směrnice
- reguluje **více než služeb v 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**

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 úplně nové instituty

- zajištění dostupnosti strategicky významné služby nebo mechanismus prověřování bezpečnosti dodavatelského řetězce strategicky významných služeb

Mění se některé stávající instituty

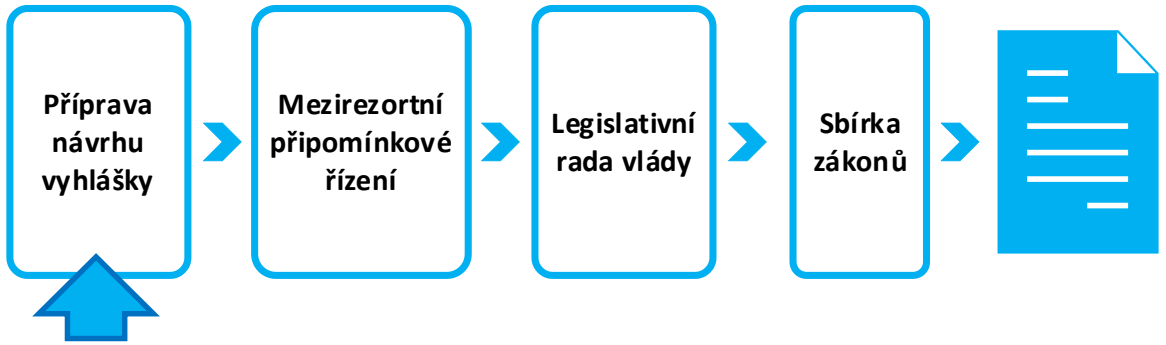
- stav kybernetického nebezpečí, (proti)opatření, konkrétní lhůty pro hlášení incidentů, sankce,…

Kritérium velikosti

Enterprise category	Headcount: Annual Work Unit (AWU)	Annual turnover	or	Annual balance sheet total
Medium-sized	< 250	≤ €50 million (in 1996 € 40 million)	or	≤ €43 million (in 1996 € 27 million)
Small	< 50	≤ €10 million (in 1996 € 7 million)	or	≤ €10 million (in 1996 €5 million)
Micro	< 10	≤ €2 million (previously not defined)	or	≤ €2 million (previously not defined)

Samostatný proces přijímání vyhlášek k nZKB

Národní úřad pro kybernetickou a informační bezpečnost



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.

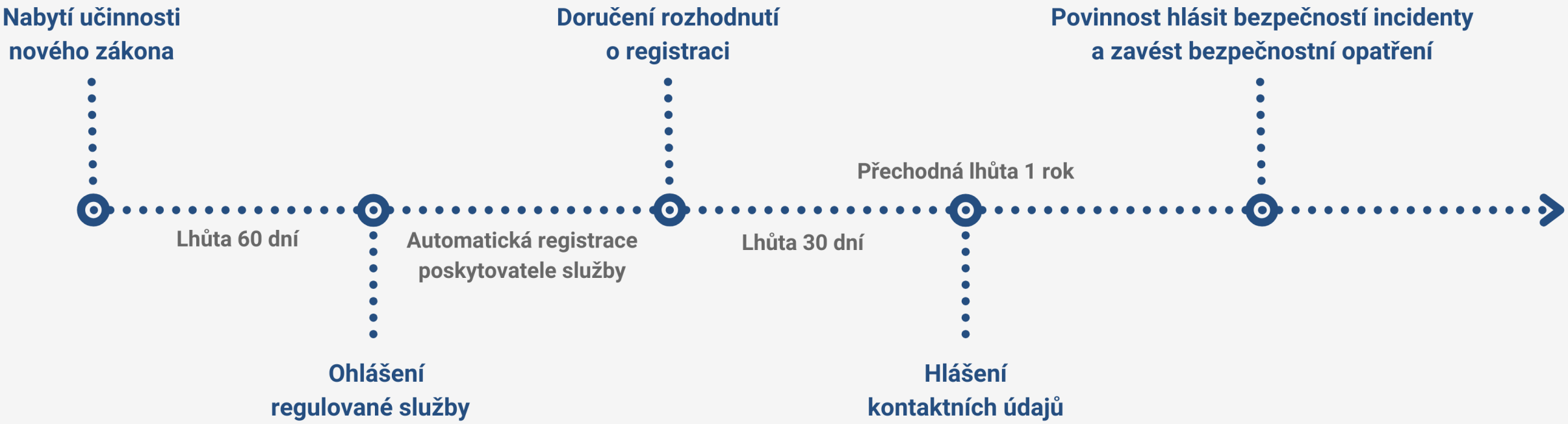
1. **Vyhláška o regulovaných službách**
2. **Vyhláška o bezpečnostních opatřeních pro vyšší režim**
3. **Vyhláška o bezpečnostních opatřeních pro nižší režim**
4. **Portálová vyhláška**
5. **Vyhláška o nepominutelných funkcích (BDŘ)**
6. **Vyhláška o bezpečnostních úrovních (cloud)**
7. **Vyhláška o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

Základní povinnosti dle nZKB

Národní úřad pro kybernetickou a informační bezpečnost

Ohlášení (§ 6) a hlášení kontaktních údajů (§ 11)	Stanovení rozsahu regulované služby (§ 12)	Bezpečnostní opatření (§ 13 a § 14)	Hlášení kybernetických bezpečnostních incidentů (§ 15 – § 17)	Informační povinnost poskytovatele regulované služby vůči zákazníkům (§ 19)	Provedení protiopatření (§ 20 – § 23)
Ohlášení regulované služby a nahlášení kontaktní osoby	Vymezení rozsahu aktiv, které v organizaci souvisejí s regulovanou službou	Zavádění bezpečnostních opatření podle zařazení organizace do režimu	Vychází ze zákona a vyhlášky o bezpečnostních opatřeních	Informování o kybernetickém bezpečnostním incidentu s významným dopadem	Vydá a doručí NÚKIB
Portál NÚKIB	Potřeba pro plnění ostatních povinností	Vyhláška o bezpečnostních opatřeních – nižší/vyšší režim	Zákonem dané podmínky hlášení	Informování o významných hrozbách pro uživatele	Výstraha Varování Reaktivní protiopatření
Ohlášení do 60 dní od naplnění podmínek pro registraci (kontaktní údaje do 30 dní od zaregistrování)	Není stanovena lhůta, ale je potřeba provést pro plnění ostatních povinností a jejich lhůt ->	1 rok od doručení rozhodnutí o registraci	1 rok od doručení rozhodnutí o registraci	Bez zbytečného odkladu	Lhůty dané protiopatřením

Lhůty pro plnění povinností



Regulace poskytovatelů regulovaných služeb

Poskytovatelé regulovaných služeb

Bezpečnostní opatření podle vyhlášek o bezpečnostních opatřeních

Incidenty identifikované podle pravidel zákona o kybernetické bezpečnosti

Regulace poskytovatelů digitálních služeb

Poskytovatelé

- služby systému překladu jmen domén
- služby vytvářející důvěru
- služby správy a provozu registru domén nejvyšší úrovně
- služby cloud computingu
- služby datového centra
- služby sítě pro doručování obsahu
- služby on-line tržiště
- služby internetového vyhledávače
- služby platformy sociální sítě
- řízené služby nebo řízené bezpečnostní služby

Bezpečnostní opatření podle prováděcího předpisu Evropské komise

Významné incidenty identifikované podle pravidel prováděcího předpisu Evropské komise

Kde najít další informace?

Portál NÚKIB

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

Hlavní komunikační platforma týkající se nového ZKB

- Podpůrné materiály
- Aktuality
- Otázky & odpovědi

Hlavní message nZKB

Zavedení minimálního bezpečnostního standardu je nezbytné.

Incidentů je mnoho – dopady jsou významné.

Nový ZKB (NIS2) nepřináší žádné drakonické požadavky.

Vychází se z používaných standardů, požadavky je zavádí přiměřeně.

Našim cílem je především zvýšení bezpečnostního povědomí a osvěta.

Nechceme GDPR 2.0 – koupím štos papírů a nestarám se.

Snažíme se být konstruktivní a transparentní.

Bez právní povinnosti a případné sankce je posun nulový.

Co teď?

- Identifikovat všechny poskytované služby
- Identifikovat velikost organizace
- Prostudovat návrh vyhlášky o regulovaných službách

Naplnění kritérií?

- NEPANIKAŘIT!
- Prostudovat nový zákon o kybernetické bezpečnosti
- Prostudovat návrhy zákona a vyhlášek o bezpečnostních opatřeních

Děkuji za pozornost.

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

regulace@nukib.cz