SMĚRNICE NIS2

A

NOVÝ ČESKÝ ZÁKON O KYBERNETICKÉ BEZPEČNOSTI

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Ivan Senčák
Vedoucí oddělení regulace dodavatelů informačních technologií
Odbor regulace

1. Nový zákon o kybernetické bezpečnosti
2. Základní povinnosti
3. Digitální služby
4. Statistiky

Zákon č. 264/2025 Sb., o kybernetické bezpečnosti

Účinnost od **1. listopadu 2025**

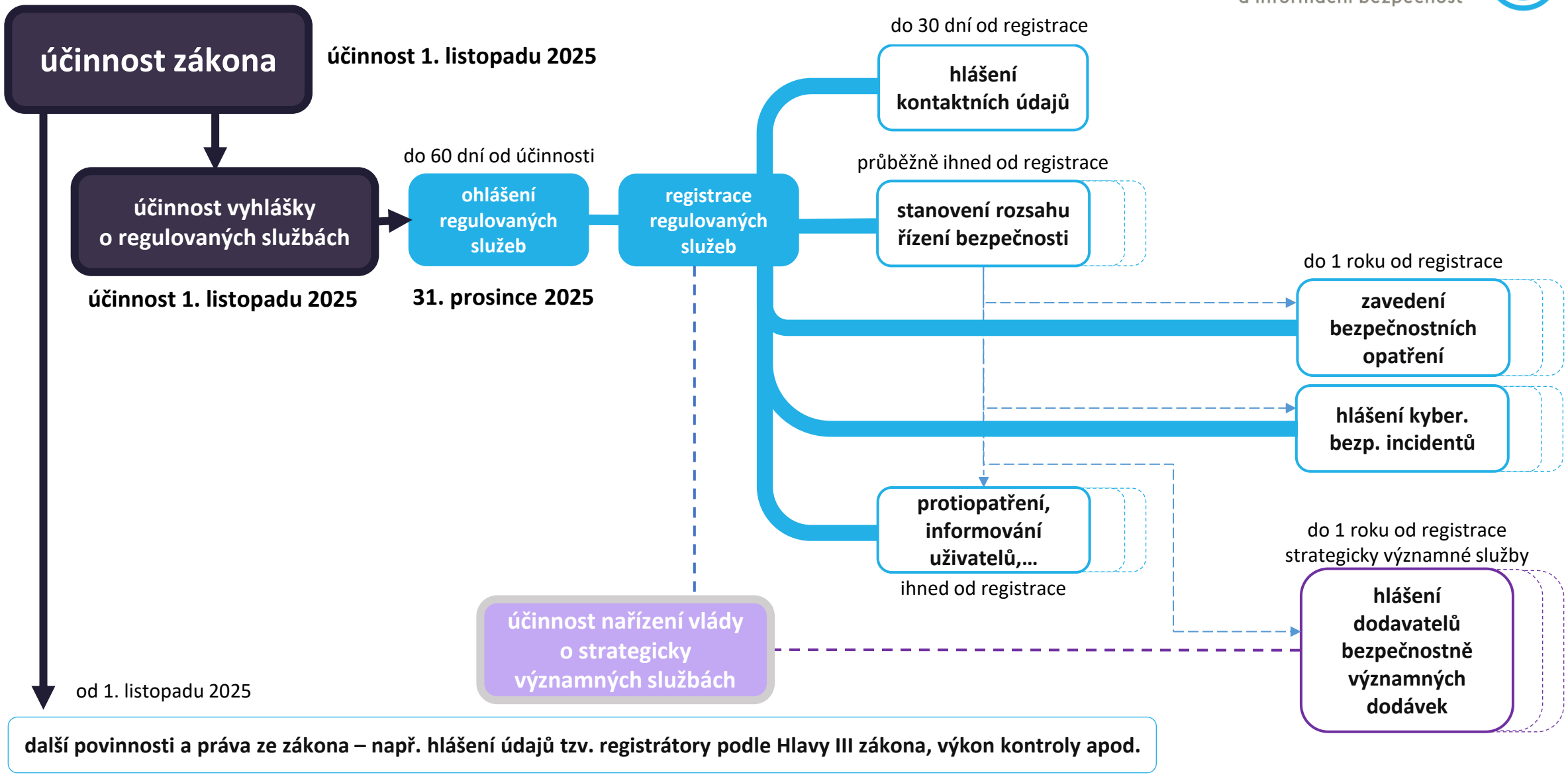
9 prováděcích právních předpisů

stovky jednání

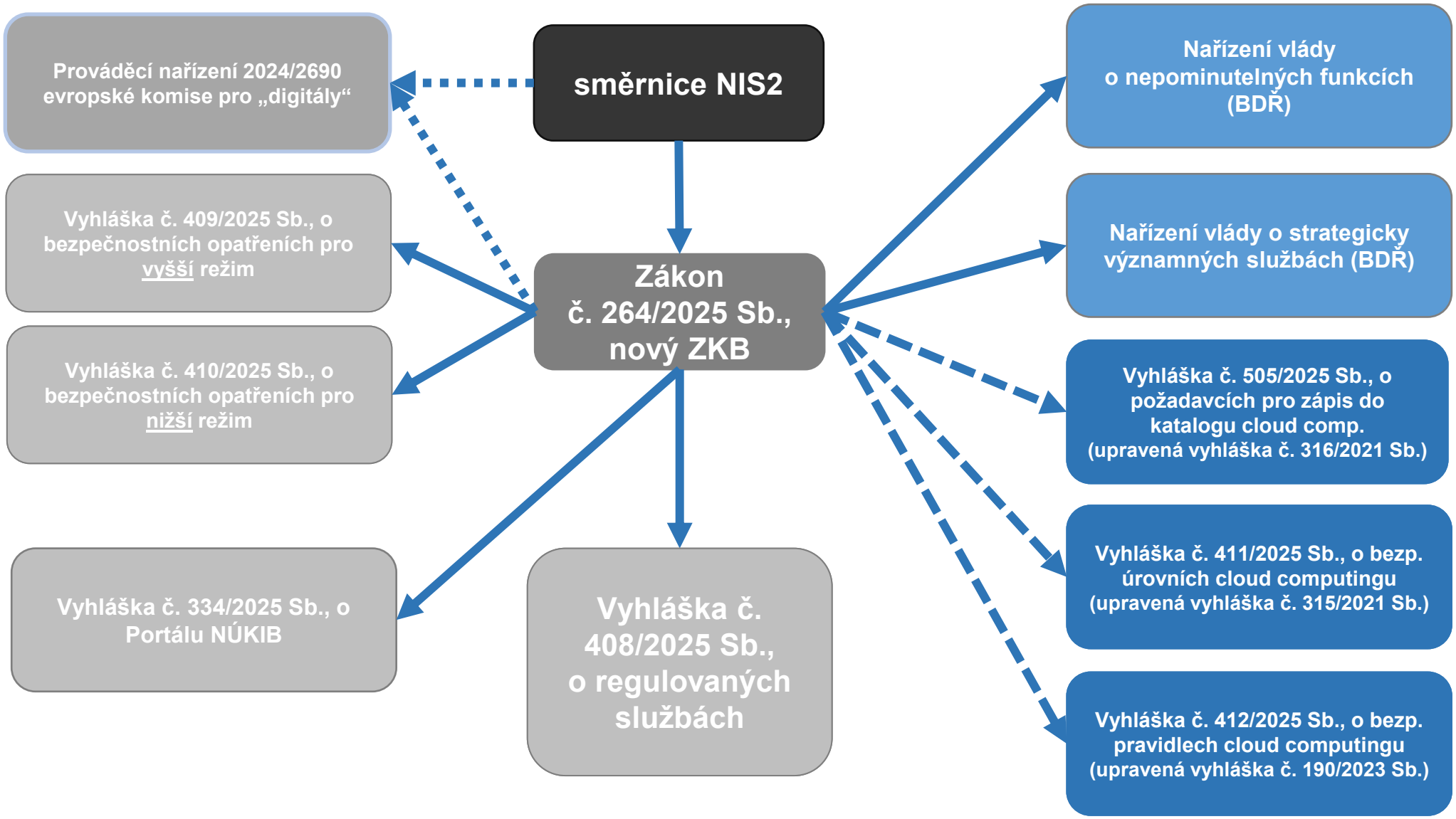
3 roky, 8 měsíců a 9 dní

(od přípravy po účinnost)

Národní úřad pro kybernetickou a informační bezpečnost



Ekosystém nZKB – prováděcí předpisy



Vybrané vyhlášky a jejich obsah

vyhláška č. 408/2025 Sb., o regulovaných službách

- Seznam služeb + podmínky významnosti = regulovaná služba
- Režim poskytovatele regulované služby
- 22 sektorů: energetika, doprava, bankovnictví, zdravotnictví, digitální infrastruktura a služby

vyhláška č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností

- Organizační a technická opatření
- Přílohy: hodnocení aktiv (důvěrnost, dostupnost, integrita), likvidace informací a dat, zranitelnosti a hrozby, hodnocení rizik, řízení dodavatelů, rozvoj povědomí

vyhláška č. 410/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností

- Povinná základní bezpečnostní opatření a přiměřeně zaváděná bezpečnostní opatření
- Přílohy: přehled BO, požadavky na smluvní ujednání, témata na rozvoj povědomí

Základní povinnosti

Základní povinnosti podle ZKB

Ohlášení

Ohlášení regulované služby a nahlášení kontaktních údajů

Portál NÚKIB

Do 60 dní od naplnění podmínek pro registraci

Bezpečnostní opatření

Vyhláška o bezpečnostních opatřeních – **nižší/vyšší režim**

11/25 opatření nižší/vyšší režim

1 rok od doručení rozhodnutí o registraci

Hlášení incidentů

Vychází ze zákona a vyhlášky o bezpečnostních opatřeních

Významné incidenty – nižší a větší okruh vyšší

1 rok od doručení rozhodnutí o registraci

Provedení protiopatření

Vydá a doručí NÚKIB

Reaktivní protiopatření/varování

Lhůty dané protiopatřením

Samoidentifikace

Střední nebo velký podnik

- 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 – počet zaměstnanců nebo rozvaha nebo obrat
  - **Střední podnik** (nad 50 zaměstnanců/10 mil. EUR rozvaha/10 mil. EUR obrat)
  - **Velký podnik** (nad 250 zaměstnanců/43 mil. EUR rozvaha/50 mil. EUR obrat)
- Partnerské podniky (25-50 % účasti) do výše podílu / Propojené podniky (nad 50 % účasti) **se z pohledu velikosti sčítají**

Poskytuje regulovanou službu

- Viz vyhláška o regulovaných službách – vychází z příloh směrnice NIS2

Typicky velké podniky ve vybraných odvětvích vyšší režim, střední podniky nižší režim, ale pozor na **výjimky**

- **DNS, registr internetových domén nejvyšší úrovně, veřejná správa, případně dle národní implementace**
- **ISP spadají do regulace všichni** – jejich velikost má vliv na režim

Samoidentifikace – vyhláška o regulovaných službách

16. **Digitální infrastruktura a služby**

Regulovaná služba	
Služba	**Podmínky významnosti poskytovatele regulované služby a jeho režim**
16.1 Poskytování veřejně dostupné služby elektronických komunikací podle zákona o elektronických komunikacích[30])	Osoba poskytující veřejně dostupnou službu elektronických komunikací podle zákona o elektronických komunikacích je I. poskytovatelem regulované služby v režimu vyšších povinností v případě, že je a) velkým nebo středním podnikem, b) poskytovatelem veřejně dostupné služby elektronických komunikací prostřednictvím nejméně 350 000 aktivních mobilních SIM karet na území České republiky, nebo c) poskytovatelem nejméně 100 000 aktivních pevných internetových přípojek na území České republiky, nebo II. poskytovatelem regulované služby v režimu nižších povinností v případě, že je malým podnikem, nebo mikropodnikem podle doporučení Komise 2003/361/ES o definici mikropodniků a malých a středních podniků.
16.2 Zajišťování veřejné komunikační sítě podle zákona o elektronických komunikacích	Osoba zajišťující veřejnou komunikační síť podle zákona o elektronických komunikacích je I. poskytovatelem regulované služby v režimu vyšších povinností v případě, že je a) velkým nebo středním podnikem, b) poskytovatelem veřejně dostupné služby elektronických komunikací prostřednictvím nejméně 350 000 aktivních mobilních SIM karet na území České republiky, nebo c) poskytovatelem nejméně 100 000 aktivních pevných internetových přípojek na území České republiky, nebo II. poskytovatelem regulované služby v režimu nižších povinností v případě, že je malým podnikem, nebo mikropodnikem.
16.3 Poskytování služby výměnného uzlu internetu (IXP)	Poskytovatel služby výměnného uzlu internetu (IXP) je I. poskytovatelem regulované služby v režimu vyšších povinností v případě, že a) je velkým podnikem, nebo b) umožňuje propojení nejméně 100 nezávislých sítí s datovým tokem alespoň 1 Tbps, nebo II. poskytovatelem regulované služby v režimu nižších povinností v případě, že je středním podnikem.
16.4 Poskytování služby systému překladu doménových jmen s výjimkou služby poskytované jako součást regulované služby podle bodu 16.1	Poskytovatel služeb systému překladu doménových jmen s výjimkou poskytovatele, který tuto službu poskytuje jako součást regulované služby podle bodu 16.1, je poskytovatelem regulované služby v režimu vyšších povinností v případě, že a) aktivně poskytuje veřejně dostupné služby pro rekurzivní překlad doménových jmen koncovým uživatelům internetu, nebo b) poskytuje služby pro autoritativní překlad doménových jmen pro použití třetí stranou pro více než 10 000 domén druhého řádu.

Pro zjištění, zda se vás regulace týká, lze využít kalkulačka NÚKIB na Kalkulačka | Portál NÚKIB

Ohlášení služby a hlášení kontaktních údajů

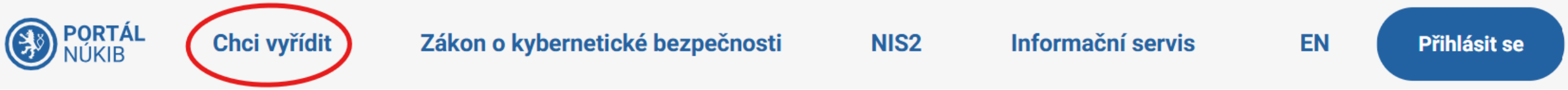
Ohlášení regulované služby

- **31. prosince 2025**
- Povinnost poskytovatele (samoidentifikace)
- Výhradně prostřednictvím **Portálu NÚKIB**
- Následně bude vydáno rozhodnutí o registraci (počítání lhůt)

Hlášení kontaktních údajů

- Cílem je:
  - zpřehlednění vztahu mezi Úřadem a povinnou osobou (regulované služby, režim,…)
  - nastavení přímé komunikační linky mezi Úřadem a povinnou osobou
- Hlášení má probíhat skrze **Portál NÚKIB**
  - Předmět hlášení je uveden v Portálové vyhlášce
    - identifikační údaje, funkce, pracovní zařazení, telefonní číslo, e-mail oprávněné osoby

Ohlášení regulované služby



Chci vyřídit

Regulované služby

Ohlášení regulované služby

Ohlášení splnění podmínek pro registraci podle § 6 zákona o kybernetické bezpečnosti.

Hlášení údajů k regulovaným službám

Hlášení kontaktních a doplňujících údajů podle § 11 zákona o kybernetické bezpečnosti.

Správa regulovaných služeb

Tento formulář slouží subjektům k ohlášení dalších, ke změně dříve nahlášených nebo k žádosti o zrušení registrace regulovaných služeb.

[Jak ohlásit regulovanou službu | Portál NÚKIB]

Bezpečnostní opatření a stanovení rozsahu řízení KB

Bezpečnostní opatření

- Dvojrychlostní kybernetická bezpečnost
- Nižší a vyšší režim povinností (vyhláška o regulovaných službách)
  - výsledný vždy jen jeden režim povinností

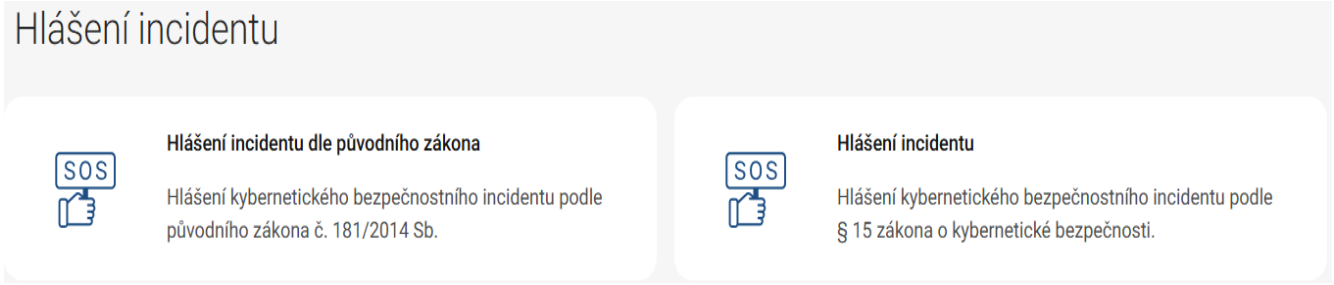
Stanovení rozsahu řízení kybernetické bezpečnosti

- Stanovený rozsah = aktiva související s poskytováním regulované služby
- V rámci stanoveného rozsahu jsou pak plněny povinnosti ze zákona
- Platí fikce stanovení rozsahu
- Postup:
  1. určení všech svých primárních aktiv,
  2. posouzení, zda primární aktiva souvisí s poskytovanou regulovanou službou,
  3. pro primární aktiva se určí jejich podpůrná aktiva.

Hlášení kybernetických bezpečnostních incidentů

Poskytovatel regulované služby **v režimu vyšších povinností** je povinen:

- Hlásit NÚKIB (Portál NÚKIB)
- Hlásí **všechny** kybernetické bezpečnostní incidenty
- Významný dopad: do 24 hodin vyhodnotí NÚKIB



Hlásím incidenty, které:

- projevily ve stanoveném rozsahu
- původ v kybernetickém prostoru
- nelze vyloučit úmyslné zavinění

Poskytovatel regulované služby **v režimu nižších povinností** je povinen:

- Hlásit Národnímu CERT (Portál NÚKIB)
- Hlásí ty incidenty, které mají **navíc významný dopad** na poskytování regulované služby
- Významný dopad: vyhodnotí sám podle vyhlášky o bezpečnostních opatřeních

Provedení protiopatření

Výstraha

- Informování **veřejnosti** o kybernetickém bezpečnostním **incidentu či o porušování povinností** daných tímto zákonem

Varování

- NÚKIB vydá varování, dozví-li se o **závažné hrozbě nebo zranitelnosti** v oblasti KB
- Vstupuje do analýzy rizik (vyšší režim povinností), možné dobrovolné zohlednění + povinnost ve smlouvách s dodavateli (nižší režim povinností)

Reaktivní protiopatření

- Uložení povinnosti poskytovateli regulované služby provést reaktivní protiopatření
  - k řešení **incidentu**, k zabezpečení aktiv před incidentem, ke zvýšení bezpečnosti na základě incidentu
- Forma: správní rozhodnutí nebo opatření obecné povahy

Informační povinnost

Informační povinnost – kybernetický bezpečnostní incident

- Pokud to poskytovatel regulované služby považuje **za vhodné, oznámí bez zbytečného odkladu uživatelům regulované služby kybernetický bezpečnostní incident s významným dopadem,** který by **mohl negativně ovlivnit** poskytování této služby
- NÚKIB může poskytovateli regulované služby uložit povinnost nebo zákaz informovat uživatele regulované služby o tomto incidentu

Informační povinnost – významná hrozba

- Poskytovatel regulované služby je **povinen informovat uživatele** regulované služby, který může být ovlivněn **významnou hrozbou** o **krocích k minimalizaci dopadu** hrozby
  - je-li to vhodné a možné, informuje také o této významné hrozbě
- **Významná hrozba** má potenciál závažně ovlivnit aktiva poskytovatele regulované služby nebo uživatele regulované služby natolik, že způsobí značnou újmu

Digitální služby

Regulované služby

16.1. Poskytování veřejně dostupné služby elektronických komunikací

16.2. Zajišťování veřejné komunikační sítě

16.3. Poskytování služby výměnného uzlu internetu

16.4. Poskytování služby systému překladu doménových jmen

16.5. Poskytování služby registrace a správy doménových jmen

16.6. Správa a provoz registru domény nejvyšší úrovně

16.7. Správa a provoz domény gov.cz

16.8. Poskytování služby cloud computing

16.9. Poskytování služby datového centra

16.10. Poskytování služby sítě pro doručování obsahu (CDN)

16.11. Správa kvalifikovaného systému elektronické identifikace

16.12. Poskytování služby vytvářející důvěru

16.13. Poskytování řízené služby

16.14. Poskytování řízené bezpečnostní služby

16.15. Poskytování služby on-line tržiště

16.16. Poskytování služby internetového vyhledávače

16.17. Poskytování platformy sociální sítě

16.18. Provozování Národního CERT

Řízené služby

Řízené služby

„řízenou službou služba související s instalací, správou, provozem nebo údržbou technických aktiv, a to prostřednictvím asistence nebo aktivní správy, které jsou prováděny v prostorách zákazníků nebo na dálku “

Režim vyšších povinností
- velký podnik

Režim nižších povinností
- střední podnik

Řízené bezpečnostní služby

„řízenou bezpečnostní službou služba, která spočívá v činnostech souvisejících s řízením kybernetických bezpečnostních rizik nebo poskytováním asistence pro tyto činnosti“

Režim vyšších povinností
- velký podnik

Režim nižších povinností
- střední podnik

Regulace poskytovatelů digitálních 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

Mapování bezpečnostních opatření dle prováděcího nařízení pro poskytovatele digitálních služeb a vyhlášky č. 410/2025 Sb. | Portál NÚKIB
Mapování bezpečnostních opatření dle prováděcího nařízení pro poskytovatele digitálních služeb a vyhlášky č. 409/2025 Sb. | Portál NÚKIB

Regulace poskytovatelů digitálních služeb

Article 3

Significant incidents

1. An incident shall be considered to be significant for the purposes of Article 23(3) of Directive 2022/2555 with regard to the relevant entities where one or more of the following criteria are fulfilled:

(a) the incident has caused or is capable of causing direct financial loss for the relevant entity that exceeds EUR 500 000 or 5 % of the relevant entity's total annual turnover in the preceding financial year, whichever is lower;

(b) the incident has caused or is capable of causing the exfiltration of trade secrets as set out in Article 2 point (1), of Directive (EU) 2016/943 of the relevant entity;

(c) the incident has caused or is capable of causing the death of a natural person;

(d) the incident has caused or is capable of causing considerable damage to a natural person's health;

(e) a successful, suspectedly malicious and unauthorised access to network and information systems occurred, which is capable of causing severe operational disruption;

(f) the incident meets the criteria set out in Article 4;

(g) the incident meets one or more of the criteria set out in Articles 5 to 14.

Významné incidenty identifikované podle pravidel prováděcího předpisu Evropské komise

Article 4

Recurring incidents

Incidents that individually are not considered a significant incident within the meaning of Article 3, shall be considered collectively as one significant incident where they meet all of the following criteria:

(a) they have occurred at least twice within 6 months;

(b) they have the same apparent root cause;

(c) they collectively meet the criteria set out in Article 3(1)(a).

Výhled do budoucna

- Cyber Resilience Act – CRA
- NIS2+
- Cyber Security Act – CSA2

Jak se na zákon připravit?

Přehled v organizaci

- Mé agendy/služby, co poskytuji
- Co pro to 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 kapacity?
- Co je má prioritní služba?
- Provedu analýzy, stanovím plán se zohledněním kapacit a priorit.

Zavádění opatření

- Určím odpovědné osoby.
- Priorita je vzdělávání zaměstnanců včetně vedení.
- Pokračuji dle plánu.

Zásada přiměřenosti:

- Náklady na zaváděné opatření by neměly převyšovat náklady na případnou realizaci kybernetického incidentu.

- Nechci všechno najednou, postupně se zlepšuji.

Statistiky

Statistiky

- **Počet návštěv Portálu**
  - Od 1. 1. 2026 – 64 655 návštěv
  - Za posledních 12 měsíců – 323 882 návštěv
- **Dostupnost Portálu**
  - V posledních 30 dnech – 99,827 %
  - Za poslední rok – 99,833 %
  - Počítáme i odstávky
- **Počty ohlášení**
  - Celkem 5437 poskytovatelů regulovaných služeb
  - Celkem 7967 regulovaných služeb
  - Nejvíce ohlášení 18. prosince 2025 – 409
  - Na Štědrý den – 9, na Silvestra – 175, na Nový rok – 7
- **Počet dotazů**
  - Prosinec 2025 – cca 300
  - Od 1. ledna 2026 – cca 150 měsíčně
- **Podpůrné materiály**
  - Celkový počet – 36
  - Počet zobrazení – 134 859
  - Nejzobrazovanější je materiál Jak ohlásit regulovanou službu | Portál NÚKIB

Děkuji za pozornost

regulace@nukib.gov.cz

nukib.gov.cz

PORTÁL NÚKIB

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