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

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Jan Hénik
Oddělení regulace veřejného sektoru
Odbor regulace

19. listopadu 2025
TLP: CLEAR

Národní úřad
pro kybernetickou
a informační bezpečnost

Zákon č. 246/2025 Sb., o kybernetické bezpečnosti

Účinnost od **1. listopadu 2025**

9 prováděcích právních předpisů

stovky jednání

3 roky, 8 měsíců a 9 dní

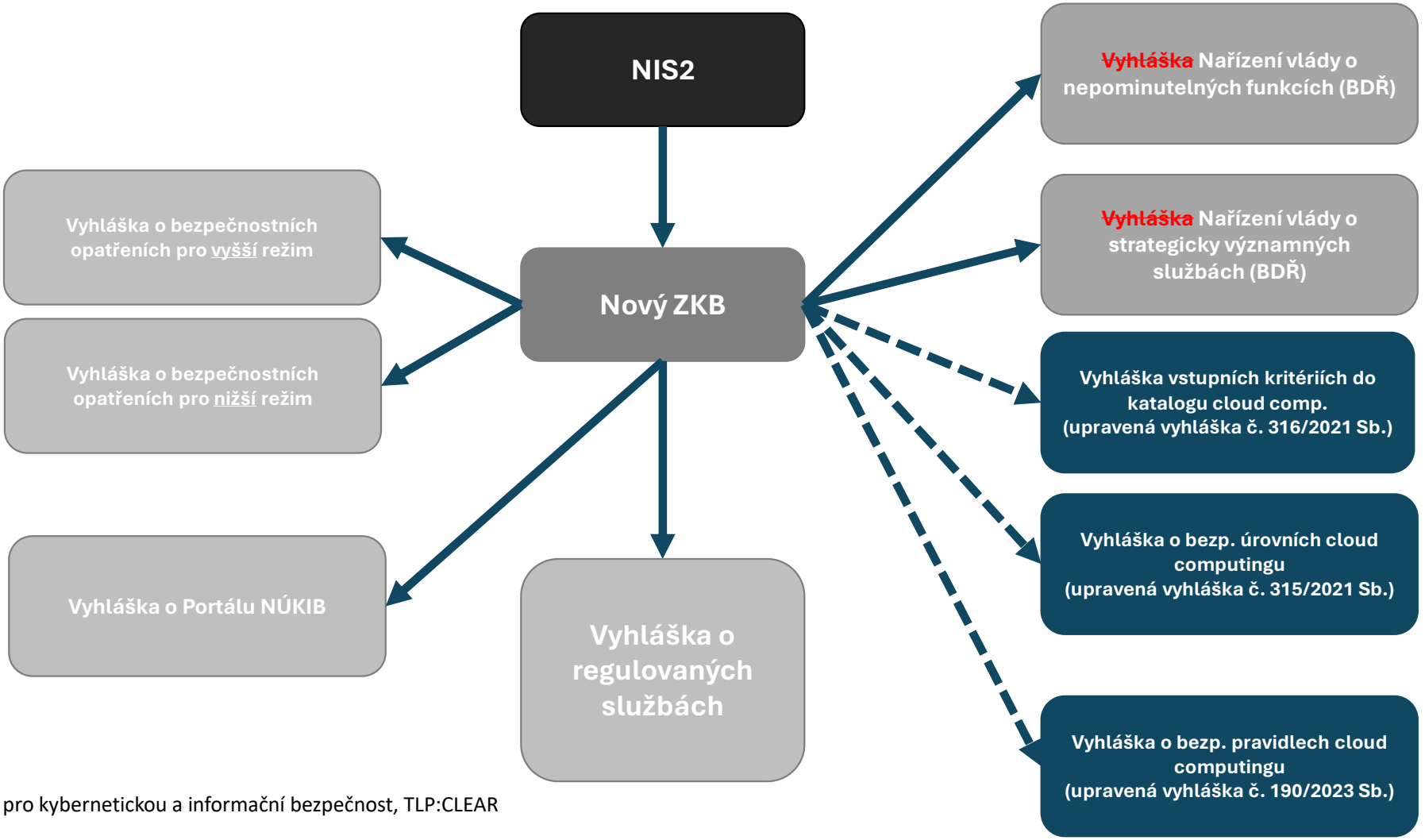
(od přípravy po účinnost)

Ohlédnutí za zajímavými momenty roku 2025

- Zákon byl schválen ve sněmovně, účinnost od 1.11.2025
  - Přítomno: 166 (2014) x 165 (2025) – z toho pro návrh: 161 (2014) x 159 (2025), proti návrhu: 0 (2014) x 0 (2025)
  - Nepřihlášen, omluven, zdržel se: 39 (2014) x 41 (2025)
- Zákon v Poslanecké sněmovně strávil celkem 9 měsíců (od 25. července 2024 do 13. května 2025).
- Senát schválil zákon 66 hlasy pro, 1 proti
- Zákon prošel 5 legislativními informačními systémy (eKlep Úřadu vlády, Informační systém PSP, systém na Senátní tisky, proces ve Sbírce zákonů, E-sbírka)
- Reálně byl na stole návrh, aby všechny vyhlášky vydávala vláda jako nařízení
- Reálně byl na stole návrh, aby vyhlášky byly vydávány ve spolugesci s 11 dalšími ministerstvy

- Připomínky k zákonu i vyhláškám byly v některých případech stejné od některých úřadů a soukromého sektoru (vč. překlepů☺)
- U vyhlášek uděleny výjimky z RIA, následně pak nebyly uznány
- NÚKIB navrhoval do vyhlášky o regulovaných službách např. výjimku pro charity poskytující zdravotnické služby
- Neprošla novela správního řádu – není umožněno automatizované podepisování rozhodnutí – pečetit (se pak těžko digitalizuje) – solidní komplikace přípravy nových systémů

Ekosystém NZKB – prováděcí předpisy



Koho se to týká?

Koho se regulace týká?

Regulovanou službou je

- služba naplňující podmínky pro registraci (podle § 4) = alespoň jedno „**kritérium pro identifikaci“ regulované služby podle vyhlášky o regulovaných službách**

  = **samoidentifikace**

nebo

- služba naplňující podmínky pro registraci (podle § 5) = **služba stanovená rozhodnutím** NÚKIB na základě kritéria pro určení regulované služby.

  = **určení regulátorem**

Kritétirum služby (regulovaná odvětví)

- **Veřejná správa**
- Energetika – Elektřina
- Energetika – Ropa a ropné produkty
- Energetika – Zemní plyn
- Energetika – Teplárenství
- Energetika – Vodík
- Výrobní průmysl
- Potravinářský průmysl
- Chemický průmysl
- Vodní hospodářství
- Odpadové hospodářství
- Letecká doprava
- Drážní doprava
- Vodní doprava
- Silniční doprava
- Digitální infrastruktura a služby
- Finanční trh
- Zdravotnictví
- Věda, výzkum a vzdělávání
- Poštovní a kurýrní služby
- Obranný průmysl
- Vesmírný průmysl

Vyhláška o regulovaných službách – kde jste vy?

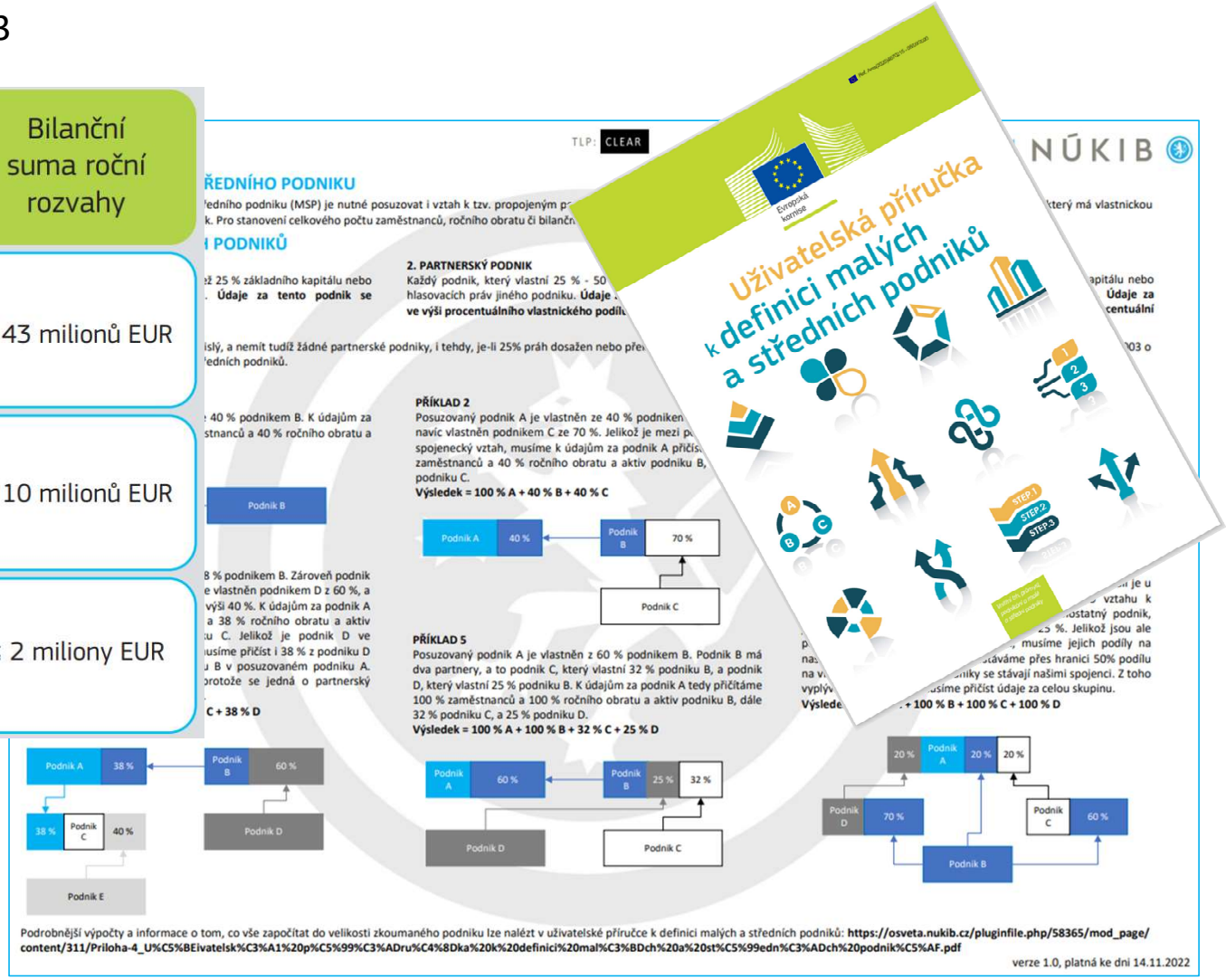
1. Veřejná správa

Regulovaná služba	
Služba	**Podmínky významnosti poskytovatele regulované služby a jeho režim**
1.1 Výkon svěřených pravomocí	I. Poskytovatelem regulované služby v režimu vyšších povinností je a) ústřední orgán státní správy, b) jiný správní úřad s celostátní působností neuvedený v písmeni a), c) ústředí, generální nebo ústřední inspektorát, generální nebo ústřední ředitelství nebo obdobná součást správního úřadu, kterým jsou podřízeny součásti správního úřadu s krajskou, okresní nebo jinou územní působností, d) Kancelář prezidenta republiky, e) Kancelář Senátu, f) Kancelář Poslanecké sněmovny, g) Česká národní banka, h) Policejní prezidium České republiky[4], i) krajské ředitelství Policie České republiky[5], j) útvar Policie České republiky s celostátní působností[6], který zajišťuje speciální policejní činnosti v oblasti odhalování nelegální migrace, letecké služby, pyrotechnické služby, kriminalistických expertíz, ochrany ústavních činitelů České republiky, dalších určených osob a chráněných objektů nebo boje proti organizovanému zločinu, terorismu a kybernetické kriminalitě, k) Generální inspekce bezpečnostních sborů, l) součást Hasičského záchranného sboru České republiky podle § 5 písm. a) až c) zákona o hasičském záchranném sboru[7], m) Kancelář veřejného ochránce práv a ochránce práv dětí, n) Nejvyšší kontrolní úřad, o) Úřad pro zastupování státu ve věcech majetkových, p) Správa úložišť radioaktivních odpadů, q) Ústavní soud, r) zdravotní pojišťovna, s) kraj, nebo t) hlavní město Praha. II. Poskytovatelem regulované služby v režimu nižších povinností je a) správní úřad nebo jeho součást s krajskou, okresní nebo jinou územní působností, b) profesní komora[8], c) vysoká škola, d) Akademie věd České republiky, e) obec s rozšířenou působností, nebo f) městská část Praha 1 až Praha 22.

Podmínky významnosti - velikost podniku

Doporučení Komise 2003/361/ES z 6. května 2003

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



Národní úřad pro kybernetickou a informační bezpečnost, TLP:CLEAR

Zvláštní ustanovení o určování velikosti podniku

nZKB § 7 Zvláštní ustanovení o určování velikosti podniku

Odchylně od pravidel doporučení Komise 2003/361/ES pro účely tohoto zákona platí, že

a) čl. 3 odst. 4 doporučení Komise 2003/361/ES se neuplatní, */nesčítají se veřejné subjekty – obce, kraje/*

b) za podnik se nepovažují organizační složky státu, územní samosprávné celky a Česká národní banka,

c) za partnerský nebo propojený podnik se nepovažují osoby, jejichž technická aktiva jsou zcela oddělena od technických aktiv, která používá posuzovaná osoba při poskytování regulované služby, a

d) pro určování velikosti poskytovatele regulované služby v odvětví věda, výzkum a vzdělávání, který není podnikem, se pravidla pro určování velikosti podniku podle doporučení Komise 2003/361/ES, včetně speciálních pravidel upravených tímto zákonem, použijí obdobně.

Určení ze strany NÚKIB

§ 5 nZKB

Podmínky pro registraci regulované služby jsou dále splněny v případě, že

a) jde o službu podle § 4 odst. 1 písm. a) a
   1. její poskytovatel je jediným poskytovatelem této služby v České republice a tato služba je zásadní pro zabezpečení důležitých společenských nebo ekonomických činností nebo pro bezpečnost v České republice,
   2. narušení této služby by mohlo mít významný dopad na bezpečnost České republiky, vnitřní pořádek nebo život a zdraví,
   3. narušení této služby by mohlo vyvolat významná systémová rizika, zejména v odvětvích, kde by takové narušení mohlo mít přeshraniční dopad, nebo
   4. její poskytovatel je kvůli svému specifickému významu na regionální nebo celostátní úrovni zásadní pro konkrétní odvětví, ve kterém působí, nebo typ služby, kterou poskytuje anebo pro jiná vzájemně propojená odvětví v České republice,
b) jde o službu, jejíž narušení může způsobit závažný zásah do života více než 125 000 osob, a to prostřednictvím ohrožení bezpečnosti České republiky, vnitřního pořádku, života a zdraví, majetkové hodnoty nebo životního prostředí,
c) jde o službu, jejíž narušení může způsobit závažný zásah do schopnosti poskytovat jinou regulovanou službu poskytovatele v režimu vyšších povinností, nebo
d) jde o službu, jejíž poskytovatel je subjektem kritické infrastruktury podle právního předpisu upravujícího krizové řízení a kritickou infrastrukturu; v takovém případě je regulovanou službou služba odpovídající prvku kritické infrastruktury určenému u tohoto subjektu.

Regulovaná služba a její režim

Strategicky významná služba – specialita vyššího režimu

Vyhláška o regulovaných službách

§ 5

Regulované služby splňující podmínky strategicky významné služby

(1) Strategicky významnou službou v odvětví veřejná správa je
   a) výkon svěřených pravomocí vykonávaný orgánem nebo osobou uvedenou v příloze k této vyhlášce v odvětví 1. Veřejná správa, služby 1.1. Výkon svěřených pravomocí, bod I. písm. a) až k).

(2) Strategicky významnou službou v odvětví energetika je
   a) výroba elektřiny v rámci výrobny s celkovým instalovaným elektrickým výkonem nejméně 100 MW vykonávaná držitelem licence na výrobu elektřiny podle energetického zákona,
   b) provoz přenosové soustavy elektřiny vykonávaný držitelem licence na přenos elektřiny podle energetického zákon,
   c) provoz distribuční soustavy elektřiny v rámci celé distribuční soustavy elektřiny s přenosovou kapacitou nejméně 220 MW vykonávaný držitelem licence na distribuci elektřiny podle energetického zákona,

- ….

Pro tyto služby platí ještě **mechanismus bezpečnosti dodavatelského řetězce** a **zajištění dostupnosti**

Nebudou definovány ve vyhlášce ale v nařízení vlády

Co subjekty zřizované kraji?

- **Subjekty zřizované kraji nejsou automaticky v regulaci** jen proto, že je zřizuje kraj.
- Pokud ale vykonávají sami některou ze služeb ve vyhlášce, pak sama tato organizace **musí posoudit, zda nenaplní kritéria.**
- **Zaměstnanci a obrat kraje se nebude připočítávat** v rámci sčítání velikostí.
- Odhadovaná zájmová odvětví: **Zdravotnictví, doprava, digitální infrastruktura**

SLUŽBY UVEDENÉ V PŘÍLOZE I

Subjekty poskytující služby uvedené v příloze I níže a splňující podmínku „velký podnik" dle doporučení Komise (EU) 2003/361/EC budou regulovány vždy v režimu „essential".

ENERGETIKA

Provozovatelé distribuční a přenosové soustavy, výrobci a prodejci elektrické energie, nominovaní organizátoři trhu s elektřinou, provozovatelé dobíjecích stanic spolu s poskytovateli elektromobility.

Subjekty poskytující službu dálkového vytápění nebo chlazení.

Provozovatelé ropovodů, zařízení na těžbu, rafinaci a zpracování ropy, skladovacích a přenosových zařízení, ústřední správci zásob.

Obchodníci s plynem, distributoři plynu, přepravci plynu, výrobci plynu a poskytovatelé uskladňování plynu.

Provozovatelé výroby, skladování a přepravy vodíku. Doposud však není implementováno do českého právního řádu.

DOPRAVA

Komerční letečtí dopravci, řídicí orgány letišť a subjekty provozující pomocná zařízení v rámci letišť, provozovatelé kontroly řízení provozu.

Provozovatel dráhy celostátní nebo regionální anebo veřejné přístupné vlečky a dopravce provozující na těchto drahách drážní dopravu.

Předmětné předpisy se vztahují na námořní přístavy a pro Českou republiku tedy nejsou relevantní.

Silniční orgány odpovědné za plánování, kontrolu a správu silnic spadajících do jejich územní působnosti, poskytovatelé služeb ITS.

BANKOVNICTVÍ

Sektor bankovnictví je regulován nařízením DORA.

INFRASTRUKTURA FIN. TRHŮ

Sektor infrastruktura finančních trhů je regulován nařízením DORA.

ZDRAVOTNICTVÍ

Poskytovatelé zdravotní péče (nemocnice a další), subjekty provádějící výzkum a vývoj léčivých výrobků a přípravků, výrobci základních farmaceutických přípravků.

PITNÁ VODA

Dodavatelé a distributoři vody určené k lidské spotřebě, avšak kromě těch, pro které je to vedlejší činnost k jejich hlavní činnosti zabývající se distribucí jiných komodit a zboží.

ODPADNÍ VODA

Subjekty shromažďující, vypouštějící nebo upravující městské nebo průmyslové odpadní vody nebo splašky, avšak kromě těch, pro které se jedná pouze o vedlejší činnost k jejich hlavní činnosti.

DIGITÁLNÍ INFRASTRUKTURA

Poskytovatelé: výměnných uzlů internetu (IXP), cloud computingu, datového centra, služeb vytvářejících důvěru, elektronických komunikací, CDN služeb, registrů TLD, služeb systému doménových jmen (DNS), s výjimkou poskytovatelů root name serverů .

POSKYTOVATELÉ ŘÍZENÝCH ICT SLUŽEB

Poskytovatelé řízených ICT služeb a poskytovatelé řízených ICT bezpečnostních služeb. Subjekty, pro zákazníky provozující či spravující ICT služby a nástroje, typicky na základě smlouvy o úrovni služeb (SLA).

VEŘEJNÁ SPRÁVA

Ústřední orgány státní správy, veřejná správa na regionální úrovni, soudy a státní zastupitelství a další instituce významné pro chod státu.

VESMÍR

V České republice nejsou umístěny žádné subjekty pozemní infrastruktury, pro Českou republiku tedy nerelevantní.

SLUŽBY UVEDENÉ V PŘÍLOZE II

Subjekty poskytující služby uvedené v příloze I a splňující podmínku „střední podnik" a subjekty poskytující služby uvedené v příloze II a splňující podmínku „velký podnik" a „střední podnik" dle doporučení Komise (EU) 2003/361/EC budou regulovány v režimu „important" (nižší nároky z hlediska bezpečnostních opatření), pokud nebude stanoveno speciálními kritérii jinak.

POŠTOVNÍ SLUŽBY

Subjekty, poskytující poštovní služby, tzn. výběr, třídění, přepravu a dodání poštovních zásilek, včetně provozovatelů kurýrních služeb.

ODPADNÍ HOSPODÁŘSTVÍ

Subjekty, poskytující službu nakládání s odpady, tzn. zařízení určená pro nakládání s odpady, obchodníci, zprostředkovatelé, dopravci podle zákona č. 541/2020 Sb., kromě těch, pro které nakládání s odpady není jejich hlavní ekonomickou činností.

CHEMICKÝ PRŮMYSL

Subjekty, poskytující služby v chemickém průmyslu, tzn. výrobci, distributoři, včetně maloobchodníka, který skladuje a uvádí na trh chemickou látku nebo předmět.

POTRAVINÁŘSTVÍ

Potravinářské subjekty, které se zabývají velkoobchodní distribucí a průmyslovou výrobou nebo zpracováním.

VÝROBA

Výroba: zdravotnických a diagnostických zdravotnických prostředků, počítačů, elektronických a optických přístrojů, elektrických zařízení, strojů a zařízení, motorových vozidel (kromě motocyklů), přívěsů a návěsů, ostatních dopravních prostředků a zařízení.

POSKYTOVATELÉ DIGI SLUŽEB

Poskytovatelé on-line tržišť, internetových vyhledávačů, platforem služeb sociálních sítí.

VÝZKUM

Výzkumné organizace, s výjimkou vzdělávacích institucí, jejichž hlavním cílem je provádět aplikovaný výzkum nebo experimentální vývoj s ohledem na využití výsledků tohoto výzkumu pro komerční účely.

Co regulace přináší?

Hlavní povinnosti vyplývající ze zákona

V případě **všech poskytovatelů regulované služby**

0. Ohlásit regulovanou službu
I. Hlásit kontaktní údaje
II. Stanovit rozsah řízení kybernetické bezpečnosti
III. Zavádět bezpečnostní opatření
IV. Hlásit kybernetické bezpečnostní incidenty
V. Informovat uživatele o incidentech a hrozbách
VI. Zavádět protiopatření vydaná NÚKIB

V případě těch, kteří jsou zároveň tzv. poskytovateli **strategicky významné služby navíc**

VII. Mechanismus prověřování bezpečnosti dodavatelského řetězce
VIII. Zajištění dostupnosti strategicky významné služby

0. Ohlášení služby

- **Ohlášení** regulované služby je povinnost poskytovatele (samoidentifikace)
  - Výhradně prostřednictvím Portálu NÚKIB
  - Následně bude vydáno rozhodnutí o registraci (počítání lhůt)

Portál NÚKIB

I. 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** (Portál NÚKIB (gov.cz))
- Co se hlásí upraveno vyhláškou o portálu NÚKIB
  - Upravuje jak se přes systém bude řešit
    - Registrace poskytovatele regulované služby a související změny
    - Pověřování osob aby mohly jednat s NÚKIB
    - Hlášení kontaktních a dalších údajů
    - Hlášení incidentů
    - Hlášení provedení protiopatření
    - Hlášení provedení nápravných opatření
    - Výmaz regulované osoby z registru
    - Hlášení informací o dodavatelích (BDŘ)

II. Stanovení rozsahu řízení kybernetické bezpečnosti

Obecně vždy platí – pokud chcete něco skutečně řídit, musíte vědět, že to máte!

Součástí rozsahu řízení kybernetické bezpečnosti jsou **aktiva související s poskytováním regulované služby.**

= stanovený rozsah

Postup:

Za účelem vymezení stanoveného rozsahu poskytovatel regulované služby

a) **určí všechna svá primární aktiva,**

b) **posoudí, zda** primární aktiva **souvisí s poskytováním regulované služby**, **a**

c) u primárních aktiv podle písmene b) **určí podpůrná aktiva.**

V rámci stanoveného rozsahu jsou pak plněny povinnosti ze zákona.

Fikce stanovení rozsahu = pokud/dokud rozsah není stanoven má se za to, že je rozsahem celá organizace.

Aktivum = fyzický nebo digitální prostředek, osoba nebo činnost související se zpracováváním informací a dat v elektronické podobě
Primární aktivum = aktivum v podobě zpracovávané informace nebo poskytované služby

Vymezení rozsahu řízení bezpečnosti informací: výkon svěřených pravomocí

Přenesená působnost kraje

- Evidence obyvatel
- Matrika
- Vidimace a legalizace
- Poskytování informace
- Krizové řízení
- Přestupky
- Státní občanství

Samostatná působnost kraje

- Správa vlastního majetku
- Vyřizování petic a stížností
- Vyhlašování krajského referenda
- Poskytování dotací
- Poskytování informací
- Zřizování příspěvkových organizací
- Vydávání obecně závazných vyhlášek
- Navrhování zákonů Poslanecké sněmovně

Vymezení rozsahu řízení bezpečnosti informací: Kraj

- Kraj může vykonávat agendy v přenesené působnosti prostřednictvím přístupu do systémů řízených centrálně -> za jejich zajištění by měl být zodpovědný ÚOSS
- **Kraje zabezpečují ty systémy, kterými disponují -> užší rozsah aktiv, na která budou zaváděna opatření**

Spisová služba

Elektronická pošta

Úřední deska

Ekonomický systém

III. Bezpečnostní opatření - základní východiska

Základní princip – přiměřenost

- Nižší režim - ***zavede a provádí přiměřená bezpečnostní opatření***
- *Vyšší režim - na základě cílů, bezpečnostních potřeb a řízení rizik* ***zavede přiměřená bezpečnostní opatření***

Bezpečnostní opatření pro **nižší režim**

- Minimum – 8 stran, 15 paragrafů.
- Povinná osoba neprovádí hodnocení rizik ve smyslu současného znění vyhlášky o kybernetické bezpečnosti.
- Pokud některé nemůže zavést – řádně zdůvodní a přijme jiné vhodné bezpečnostní opatření.

Bezpečnostní opatření pro **vyšší režim**

- Povinnosti vycházejí ze stávající vyhlášky o kybernetické bezpečnosti.
- Zavedení systému řízení bezpečnosti informací.
- Postaveno na standardu ISO 27001.

III. Bezpečnostní opatření

Pro PRS v režimu vyšších povinností

Organizační opatření

a) systém řízení bezpečnosti informací,
b) povinnosti vrcholného vedení,
c) bezpečnostní role,
d) řízení bezpečnostní politiky a bezpečnostní dokumentace,
e) řízení aktiv,
f) řízení rizik,
g) řízení dodavatelů,
h) bezpečnost lidských zdrojů,
i) řízení změn,
j) akvizice, vývoj a údržba,
k) řízení přístupu,
l) zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,
m) řízení kontinuity činností a
n) audit kybernetické bezpečnosti

Technickými opatření

a) fyzická bezpečnost,
b) bezpečnost komunikačních sítí,
c) správa a ověřování identit,
d) řízení přístupových oprávnění,
e) detekce kybernetických bezpečnostních událostí,
f) zaznamenávání bezpečnostních a relevantních provozních událostí,
g) vyhodnocování kybernetických bezpečnostních událostí,
h) aplikační bezpečnost,
i) kryptografické algoritmy,
j) zajišťování dostupnosti regulované služby a
k) zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv.

Pro PRS v režimu nižších povinností

Organizační a technická opatření

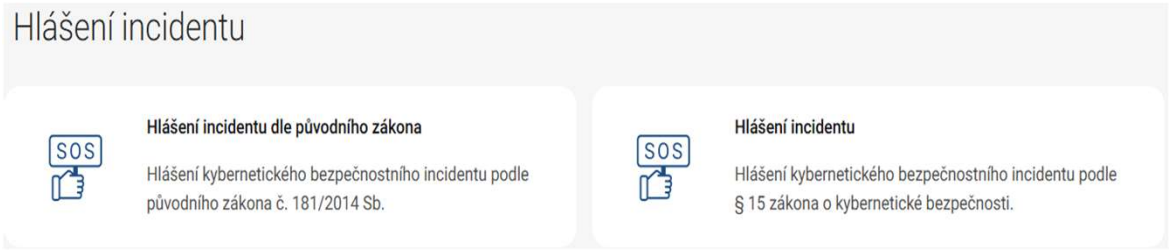
a) systém zajišťování minimální kybernetické bezpečnosti,
b) požadavky na vrcholné vedení,
c) řízení aktiv,
d) řízení rizik,
e) bezpečnost lidských zdrojů,
f) řízení kontinuity činností,
g) řízení přístupu,
h) řízení identit a jejich oprávnění,
i) detekce a zaznamenávání kybernetických bezpečnostních událostí,
j) řešení kybernetických bezpečnostních incidentů,
k) bezpečnost komunikačních sítí,
l) aplikační bezpečnost a
m) kryptografické algoritmy

*„na základě cílů systému řízení bezpečnosti informací, bezpečnostních potřeb a řízení rizik **zavede přiměřená bezpečnostní opatření ...**“*

IV. 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

V. Informační povinnost – incident a hrozba

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

VI. 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 (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

VII. Bezpečnost dodavatelského řetězce

- nová oblast, nevyplývá ze směrnice NIS2 ale z národního rozhodnutí
- platí pouze pro strategicky významné služby
- organizace v rámci této povinnosti musí nahlásit dodavatele
- budou prověřování dodavatelé do kritické části systému = aktiva s hodnotou 4 (kritická), kteří dodávají bezpečnostně významnou dodávku = má výpočetní kapacitu
- stát prověří
  - NÚKIB k tomu vyžaduje informace a součinnost řady orgánů (PČR, SLUŽBY, FAU, NSZ, MPO, MV, NBÚ, ÚOHS…)
- vláda může vydat zákaz dodavatele použít nebo upozornění na riziko (je řešitelné bezp. opatřením)
- lze udělit výjimku (např. pokud to nikdo jiný nevyrábí, ohrozilo by to službu apod.)
  - k vyřazení již dodaných technologií nemusí dojít hned – počítá se s přechodnými lhůtami
- hlášení dodavatelů do 1 roku od určení poskytovatele regulované služby

- detail koho přesně se to týká - nařízení vlády o strategicky významných službách
- jakých aktiv se to týká - nařízení vlády o nepominutelných částech a těch s hodnocením kritická

VIII. Zajištění dostupnosti SVS

- Východiska:
  - zajištění dostupnosti **směruje na službu**, nikoli nutně na její dílčí aktiva (a už vůbec ne na všechna),
  - zajištění dostupnosti služby je **možné i mimo kyberprostor,**
  - kvalita služby může být snížena – míru snížení si definuje sám poskytovatel v BCM,
  - úroveň služby může být snížena – míru snížení si definuje sám poskytovatel v BCM,
  - rozsah služby může je dle připomínek subjektů nutno omezit/definovat, aby byla právní jistota.

- Cíl:
  - kritické služby musíme být schopni zajistit alespoň omezeně z České republiky, abychom byli připraveni na mimořádné situace v zahraničí.

- Prakticky to tedy znamená, že:
  - je potřeba být schopen službu poskytovat z území ČR, tedy bez zajištění služeb ze zahraničí,
  - zajištění služby může být i mimo ICT, např. náhradním postupem fyzicky - pokud to splní stanovený rozsah a kvalitu.

Sankce a nápravná opatření

- **Pokuty**
  - poskytovatel regulované služby v režimu nižších povinností může dostat maximální pokutu ve výši 175 000 000 Kč nebo 1,4 % z obratu (podle toho, co je vyšší).
  - poskytovatel v režimu vyšších povinností pak do výše 250 000 000 Kč nebo 2 % z obratu (podle toho, co je vyšší).
- **Jiné správní tresty**
  - dočasný zákaz výkonu funkce pro člena statutárního orgánu (vyšší režim)
  - pozastavení platnosti certifikace (vyšší režim)
- **Nápravná opatření**

Cílem zákona není sankcionovat subjekty, ale přispět k vyšší kybernetické bezpečnosti v České republice.

- růst incidentů, obchodní a finanční dopady, společenská odpovědnost

Co teď?

Nejzásadnější změny pro kraje

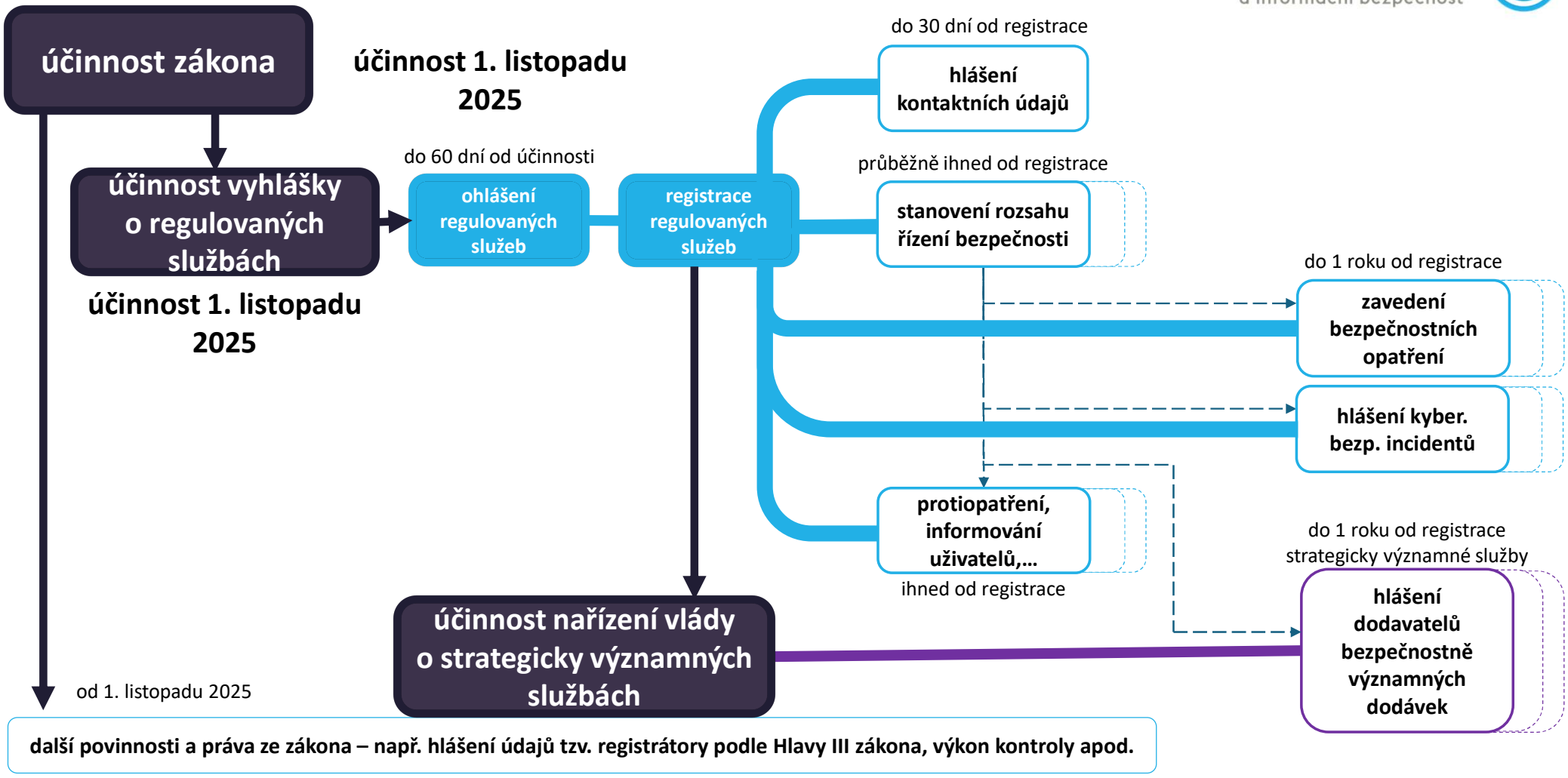
Rozsah aktiv

- Změna orientace ze systému na službu
- Rozsah nutno stanovit, jinak celá organizace
- Směrnice NIS2 preferovala celou organizaci – snaha NÚKIB o přiměřenost

Hlášení incidentů

- Prvotní hlášení všech incidentů s původem v kyberprostoru, vyjma těch u kterých lze vyloučit úmyslné zavinění
- Prvotní hlášení do 24 hodin
- Lhůty nepodkročitelné: požadavek NIS2

Národní úřad pro kybernetickou a informační bezpečnost



Jak se na zákon připravit?

Přehled v organizaci

- Jaké vykonávám agendy a poskytuji služby?
- Co pro výkon agend potřebuji?

= rozsah, ve kterém KB řeším

Aktuální stav KB

- Mám již některá opatření?

= aktuální stav zavedených a nezavedených opatření

Určení priorit

- Jaké mám finanční a personální kapacity?
- Co je má prioritní služba?

= provedu analýzy, stanovím plán

Zavádění opatření

- Osoba zodpovědná za KB.
- Vzdělávání zaměstnanců (i vedení)
- Bezpečnostní politika

= pokračuji dle plánu

Zásada přiměřenosti:

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

Praktická použitelnost:

- Šablonovitá dokumentace nikdy nebude používaná a nebude sedět mé organizaci
- Příliš složitý systém nebudu mít kapacitu udržovat

Kde najít další informace?

Portál NÚKIB

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

Hlavní komunikační platforma týkající se nového ZKB

- Podpůrné materiály
- Formuláře
- Kalkulačka
- Otázky & odpovědi

Děkuji za pozornost.

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

regulace@nukib.cz