Spolufinancováno Evropskou unií

Ministerstvo životního prostředí

UNIVERZITA J. E. PURKYNĚ V ÚSTÍ NAD LABEM

OSVĚTOVĚ ODBORNÝVZDĚLÁVACÍ PROGRAM V OBLASTI KYBERNETICKÉ BEZPEČNOSTI

vzdělávací akce realizovaná v rámci projektu

CZ.10.02.01/00/22_002/0000210, Aktivita KA1_B.3.10

RUR – Region univerzitě, univerzita regionu

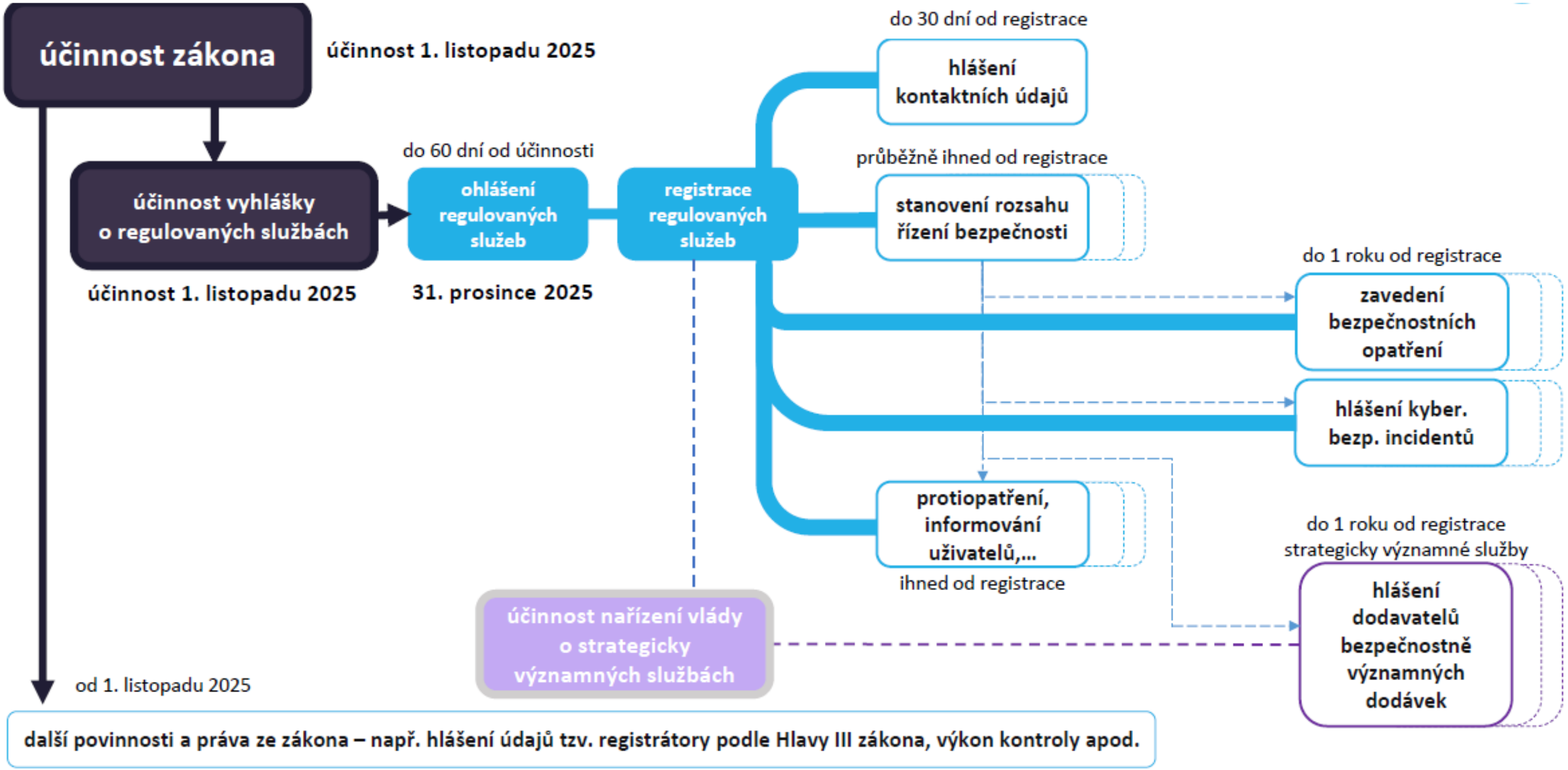
Centrum kybernetické bezpečnosti

RUR - Region univerzitě, univerzita regionu
reg. č. CZ.10.02.01/00/22_002/0000210

RUR

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

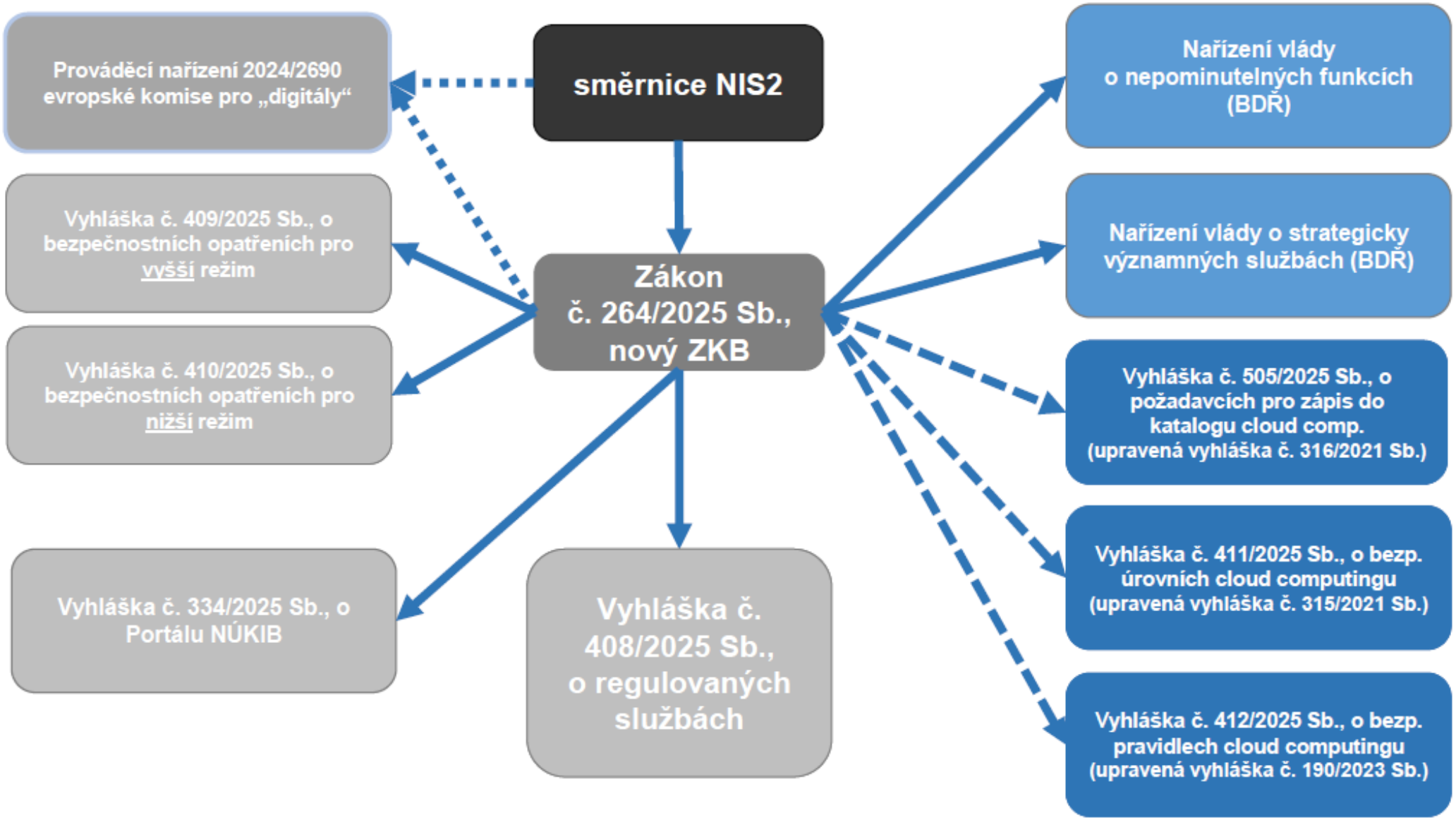
Směrnice NIS2


účinnost zákona
účinnost 1. listopadu 2025
účinnost vyhlášky o regulovaných službách
účinnost 1. listopadu 2025
do 60 dní od účinnosti
ohlášení regulovaných služeb
31. prosince 2025
registrace regulovaných služeb
do 30 dní od registrace
hlášení kontaktních údajů
průběžně ihned od registrace
stanovení rozsahu řízení bezpečnosti
do 1 roku od registrace
zavedení bezpečnostních opatření
hlášení kyber. bezp. incidentů
protiopatření, informování uživatelů,...
ihned od registrace
účinnost nařízení vlády o strategicky významných službách
do 1 roku od registrace strategicky významné služby
hlášení dodavatelů bezpečnostně významných dodávek
od 1. listopadu 2025
další povinnosti a práva ze zákona – např. hlášení údajů tzv. registrátory podle Hlavy III zákona, výkon kontroly apod.

Hlavní změny v novém zákoně o kybernetické bezpečnosti

- rozšíření počtu povinných osob, a to jak rozšířením regulovaných odvětví, tak rozšířením stávajících regulovaných odvětví o nové regulované služby,
- změna způsobu identifikace povinných osob,
- doplnění nových požadavků na zavádění bezpečnostních opatření,
- doplnění nových požadavků na proces hlášení kybernetických bezpečnostních incidentů,
- větší odpovědnost vrcholného vedení za zajišťování kybernetické bezpečnosti,
- větší důraz na sdílení informací,
- prohloubení spolupráce nejen mezi Úřadem a regulovanými osobami, ale i mezi Úřadem a dalšími orgány veřejné moci,
- zvýšení pokut a nové formy správního trestání,
- nové požadavky na řešení problematiky bezpečnosti dodavatelského řetězce.

Ekosystém nZKB – prováděcí předpisy



Vybrané vyhlášky

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

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

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 Národního úřadu pro kybernetickou a informační bezpečnost** na základě kritéria pro určení regulované služby.

  = určení regulátorem

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 zákona,

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,

o ….

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

Nebudou definovány ve vyhlášce ale v nařízení vlády

Hlavní povinnosti vyplývající z návrhu 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 Národním úřadem pro kybernetickou a informační bezpečnost

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

VII. Mechanismus prověřování bezpečnosti dodavatelského řetězce

VIII. Zajištění dostupnosti strategicky významné služby

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

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

Bezpečnostní opatření – 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.

Organizační a technická bezpečnostní opatření

Pro poskytovatele regulované služby v režimu vyšších povinností jsou

- Pro poskytovatele regulované služby v režimu nižších povinností jsou bezpečnostními opatřeními

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

Technickái 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.

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 …“

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

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

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

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 dojí 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

Zajištění dostupnosti strategicky významných regulovaných služeb

- **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,
  - zjištění služby může být i mimo ICT, např. náhradním postupem fyzicky - pokud to splní stanovený rozsah a kvalitu.