Směrnice NIS2 a povinnosti subjektů kritické informační infrastruktury

Petr Kopřiva
Vedoucí Oddělení regulace dodavatelů informačních technologií
Klára Humpolíková
Oddělení regulace soukromého sektoru
Odbor regulace

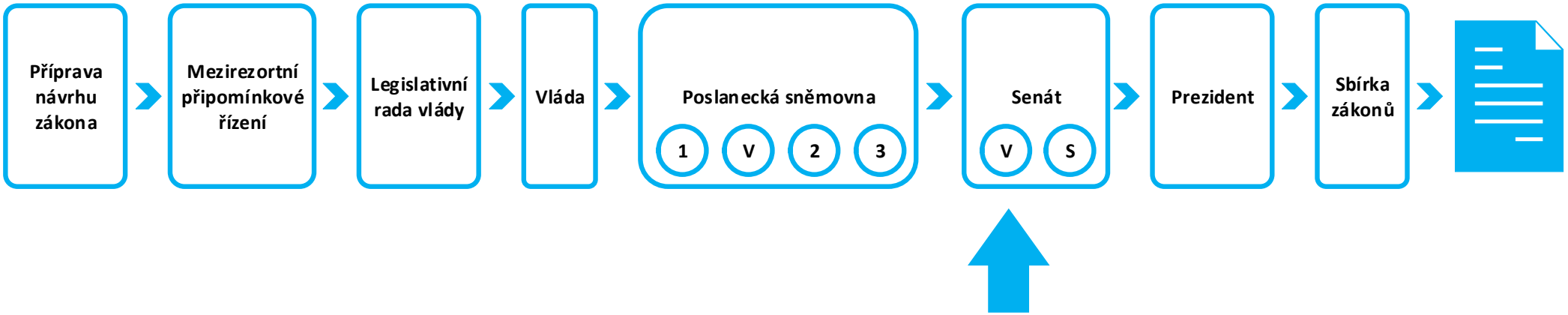
TLP: CLEAR

Směrnice NIS2

- **Směrnice NIS2** [*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)*] byla dne 27. prosince 2022 zveřejněna v Úředním věstníku Evropské unie.
- Publikovaná podoba směrnice NIS2 je oficiální a **nebude se již dále měnit.**

Návrh nZKB v legislativním procesu

Národní úřad pro kybernetickou a informační bezpečnost



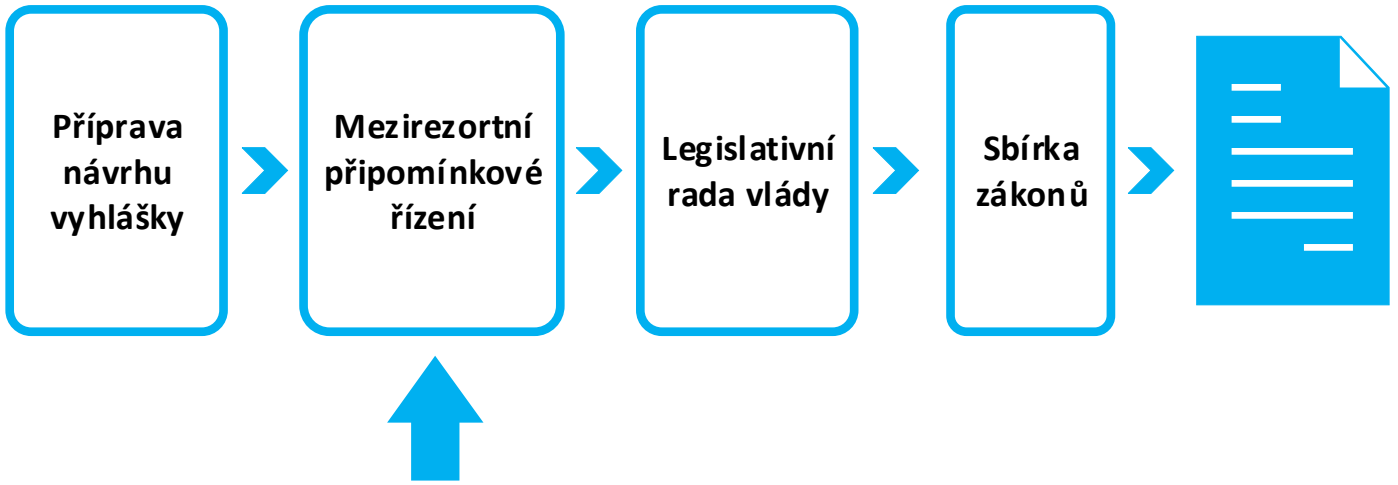
Vláda předložila Poslanecké sněmovně návrh zákona 25. července 2024.
Poslanecká sněmovna schválila zákon ve třetím čtením dne 25. dubna 2025.
Zákon předán Senátu dne 13. května 2025.

Návrh zákona rozeslán poslancům jako sněmovní tisk 759/0.
Schválený návrh zákona jako senátní tisk 109 a 110

Očekávaná účinnost podzim 2025

Samostatný proces přijímání vyhlášek

Národní úřad pro kybernetickou a informační bezpečnost



S návrhem zákona se připravují také teze jeho vyhlášek.

Přichází čas zahájit 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 bezpečnostních úrovních (cloud)**
6. **Vyhláška o bezpečnostních pravidlech (cloud)**
7. **Vyhláška o požadavcích pro zápis do katalogu CC (cloud)**

+ nařízení vlády o nepominutelných funkcí

+ nařízení vlády o strategicky významných službách

Východiska obsahu návrhu zákona

Národní úřad pro kybernetickou a informační bezpečnost

Směrnice NIS 2.0

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

Regulované služby

Směrnice NIS1:

7 odvětví

Kritérium dopadu incidentu

- **cca 400 povinných osob**

Směrnice NIS2:

22 odvětví

Kritérium velikosti subjektu

- **minimálně 6 000 povinných osob**

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, řídící 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

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.

Vyhláška o regulovaných službách

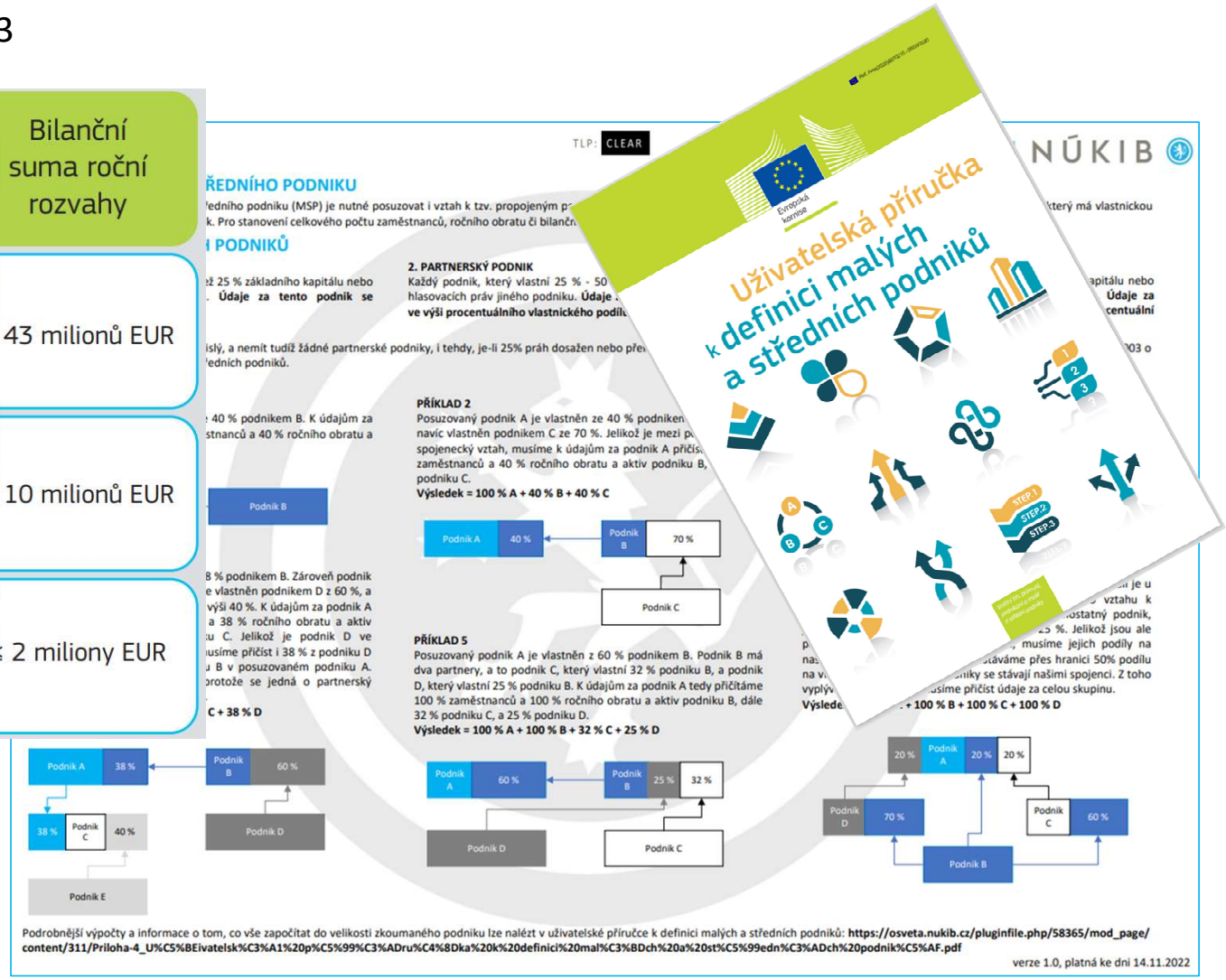
5.1. Výroba tepelné energie	Držitel licence na výrobu tepelné energie podle energetického zákona je I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že a) je velkým podnikem, nebo b) disponuje zdrojem tepelné energie s celkovým instalovaným tepelným výkonem nejméně 200 MW, II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je středním podnikem.
5.2. Provoz soustavy zásobování tepelnou energií	Držitel licence na rozvod tepelné energie podle energetického zákona je I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že a) je velkým podnikem, nebo b) disponuje soustavou zásobování tepelnou energií s celkovou přenosovou kapacitou nejméně 160 MW, II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je středním podnikem.

Služba	Podmínky významnosti poskytovatele regulované služby a jeho režim
7.1. Výroba počítačů, elektronických a optických přístrojů a zařízení	Výrobce počítačů, elektronických a optických přístrojů a zařízení ve smyslu oddílu 26 klasifikace CZ-NACE, který je velkým nebo středním podnikem, je poskytovatel regulované služby v režimu nižších povinností.
7.2. Výroba elektrických zařízení	Výrobce elektrických zařízení ve smyslu oddílu 27 klasifikace CZ-NACE, který je velkým nebo středním podnikem, je poskytovatel regulované služby v režimu nižších povinností.

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

Regulovaná služba a její režim

Základní povinnosti podle nZKB

Ohlášení

- Ohlášení regulované služby a nahlášení kontaktní osoby
- 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

Bezpečnostní opatření – rozdíly vyšší a nižší režim

Organizační opatření – **vyšší** režim:

1. systém řízení bezpečnosti informací,
2. požadavky na vrcholové vedení,
3. stanovení bezpečnostních rolí,
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 práv a 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. požadavky na vrcholové 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.

Lhůty pro plnění povinností

Provazby nZKB a nZKI

Legislativní rámec

Současný stav

- Zákon č. 240/2000 Sb., o krizovém řízení.
  - definice, pravomoci orgánů, předmět CI, plánu krizové připravenosti subjektu KI atd.
- Nařízení vlády č. 432/2010 Sb. o kritériích pro určení prvku kritické infrastruktury
  - Stanovení kritérií
- Kritická informační infrastruktura
  - Zákon o kybernetické bezpečnosti - zákon č. 181/2014 Sb.
  - Vyhláška o kybernetické bezpečnosti - č. 82/2018 Sb.

Legislativní rámec

Budoucí stav

- Zákon č. 240/2000 Sb., o krizovém řízení.
- Směrnice (EU) 2022/2557 o odolnosti kritických subjektů (CER – Critical Entities Resilience)

- Zákon o odolnosti subjektů kritické infrastruktury a o změně souvisejících zákonů (zákon o kritické infrastruktuře) – sněmovní tisk 947
  - Nařízení vlády o základních službách a kritériích významnosti
  - Vyhláška o náležitostech a zpracování plánu odolnosti, posouzení rizik a obsahu a rozsahu opatření k zajištění odolnosti
  - Vyhláška k podrobnostem hlášení incidentů

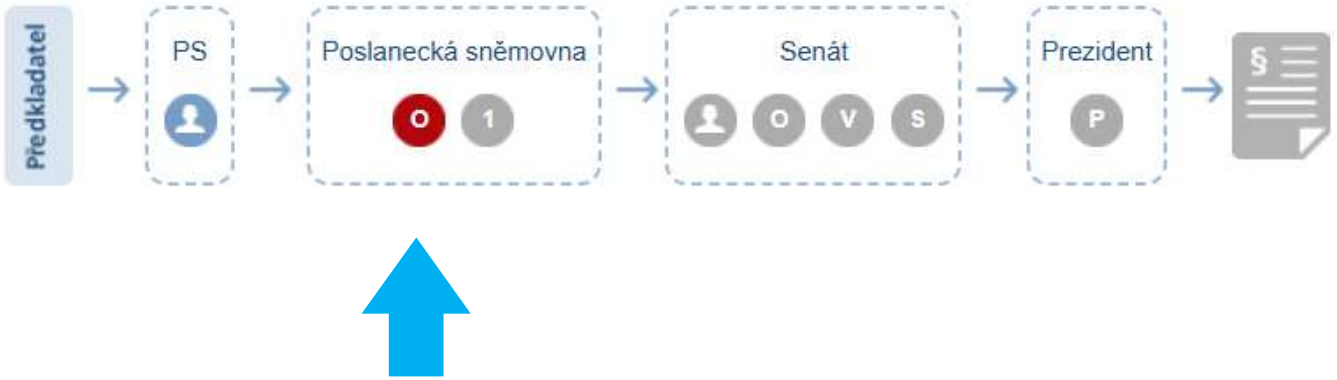
Legislativní rámec

Budoucí stav

- Zákon o kybernetické bezpečnosti - sněmovní tisk 759
  - Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností
  - Prováděcí nařízení Komise (EU) 2024/2690
    - technické a metodické požadavky bezpečnostních opatření uvedených v čl. 21 odst. 2 NIS2 a
    - případy, kdy se incident považuje za významný ve smyslu čl. 23 odst. 3 NIS2,

n.z. o odolnosti subjektů kritické infrastruktury

Národní úřad pro kybernetickou a informační bezpečnost



Vláda předložila Poslanecké sněmovně návrh zákona 4. dubna 2025.
Organizační výbor projednání návrhu zákona doporučil dne 16. dubna 2025.

Navrhovatel navrhl sněmovně projednávání návrhu zákona tak, aby sněmovna s ním mohla vyslovit souhlas již v prvém čtení.

Návrh zákona rozeslán poslancům jako **sněmovní tisk 947/0.**

Směrnice CER a NIS2

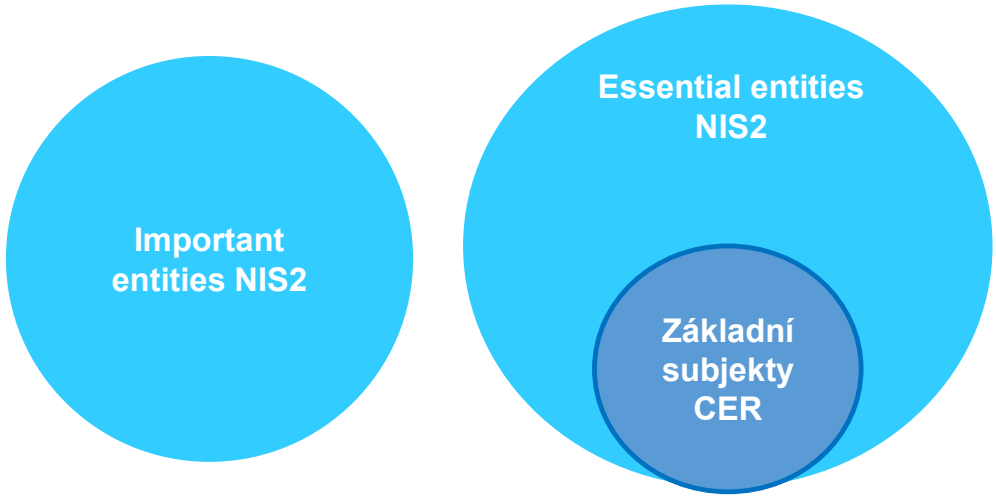
Obě směrnice počítají s úzkou koordinací a spoluprací subjektů na vnitrostátní úrovni tak, aby přístup k bezpečnosti byl koordinovaný, docházelo k výměně informací (recitál 24 směrnice CER a čl. 13 odst. 5 směrnice NIS2)

= bezpečnost je jen jedna

Obě směrnice mají nastavené mechanismy společného fungování tak, aby se doplňovaly a ideálně nepřekrývaly

= nemělo by docházet k přesunu administrativy primárně na subjekty

Nejzásadnější provazba (čl. 2 odst. 3 směrnice NIS2 a čl. 3 odst. 1 písm. f)



Provazba na institucionální úrovni

SOUČASNÝ STAV (OD 2015)

NÚKIB je gestorem oblasti kybernetická bezpečnost v odvětví komunikační a informační systémy dle nařízení vlády č. 432/2010 Sb. o kritériích pro určení prvku KB

G. Oblast kybernetické bezpečnosti:
a) informační systém, který významně nebo zcela ovlivňuje činnost určeného prvku kritické infrastruktury, a který je nahraditelný jen při vynaložení nepřiměřených nákladů nebo v časovém období přesahujícím 8 hodin,
b) komunikační systém, který významně nebo zcela ovlivňuje činnost určeného prvku kritické infrastruktury, a který je nahraditelný jen při vynaložení nepřiměřených nákladů nebo v časovém období přesahujícím 8 hodin,
c) informační systém spravovaný orgánem veřejné moci obsahující osobní údaje o více než 300000 osobách,
d) komunikační systém, zajišťující připojení nebo propojení prvku kritické infrastruktury, s kapacitou garantovaného datového přenosu nejméně 1 Gbit/s,
e) odvětvová kritéria pro určení prvku kritické infrastruktury uvedená v písmenech A. až F. se použijí přiměřeně pro oblast kybernetické bezpečnosti, pokud je ochrana prvku naplňujícího tato kritéria nezbytná pro zajištění kybernetické bezpečnosti.

STAV DLE nZKB a nZKI

NÚKIB je gestorem pododvětví ostatní digitální služby a infrastruktura v odvětví digitální služby a infrastruktura dle navrhovaného nařízení vlády

C. Ostatní digitální služby a infrastruktura

Kritéria významnosti pro základní službu

1.Poskytování a provozování služeb výměnných uzlů internetu
Poskytovatel služby výměnného uzlu internetu.

2. Poskytování služeb systému překladu jmen domén (DNS) s výjimkou služeb souvisejících s kořenovými jmennými servery
a) Poskytovatel aktivně poskytující veřejně dostupné rekurzivní služby pro překlad doménových jmen koncovým uživatelům internetu dosahující alespoň jednou za kalendářní rok průměrného počtu 20 tisíc DNS dotazů za vteřinu za období kalendářního měsíce, nebo
b) poskytovatel autoritativní služby překladu doménových jmen pro použití třetí stranou pro více než 50 000 domén druhého řádu.

3. Provoz a správa registrů domén nejvyšší úrovně (TLD)

Subjekt spravující a provozující registr národní domény nejvyšší úrovně.

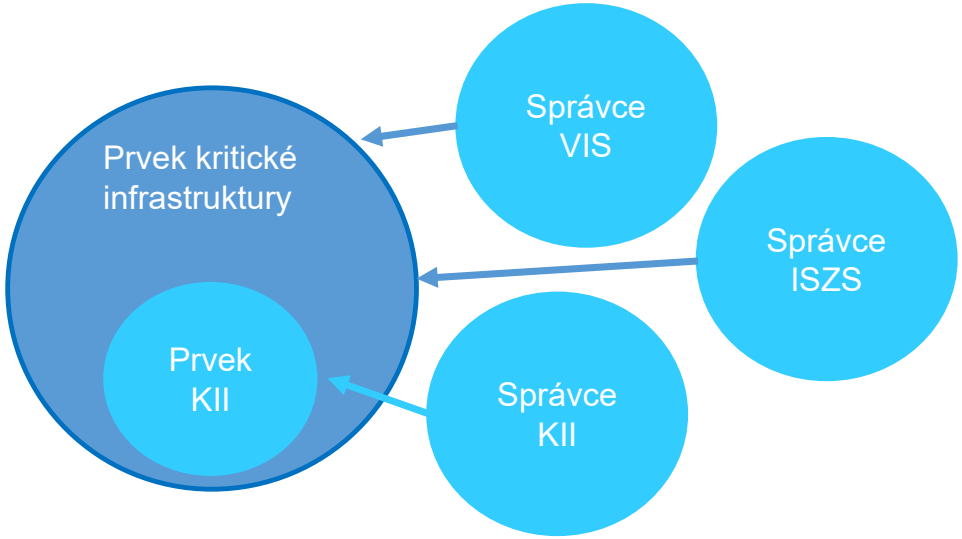
4. Správa a provoz domény gov.cz

Subjekt spravující a provozující doménu gov.cz.

Provazba na úrovni subjektů dle nZKB a dle nZKI

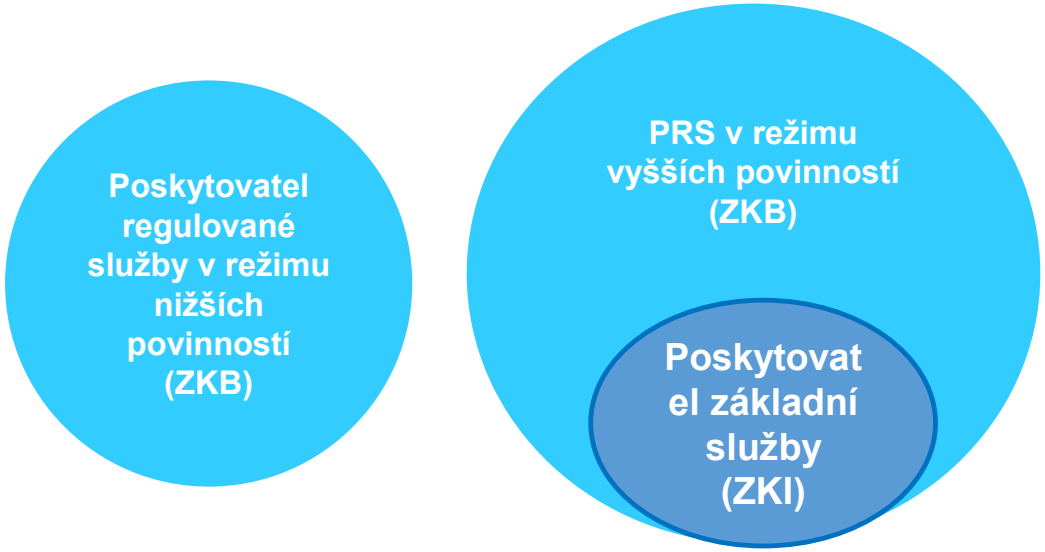
SOUČASNÝ STAV (OD 2015)

- Správce kritické informační infrastruktury jako speciální povinná osoba dle ZKB – metoda prvek v prvku
- Posuzování naplnění dopadů ICT složky organizace KI
- Zařazení mezi KII = zařazení mezi KI, ale ne naopak
- Procesně – usnesení vlády nebo OOP



STAV DLE nZKB a nZKI

- Není speciální subjekt – subjekty dle ZKI se stávají poskytovatelem regulované služby (vyšší režim)
- Pod ZKB se neposuzují žádné dopady
- Zařazení pod ZKI je důvodem pro zařazení pod ZKB
- Procesně – samoidentifikace + rozhodnutí NÚKIB



Provazba na úrovni povinností dle nZKB a nZKI

SOUČASNÝ STAV (OD 2015)

- Správce KII je i subjektem KI **= má práva a povinnosti dle ZKB i dle krizového zákona** – pro oba předpisy plnou sadu povinností a plnou sadu práv

STAV DLE nZKB a nZKI

- Všechny osoby povinné dle nZKI (poskytovatelé základních služeb) jsou povinné i podle ZKB (poskytovatelé regulované služby v režimu vyšších povinností)
- **ALE!**
- **Poskytovatelé základních služeb v odvětví digitální infrastruktury mají povinnosti primárně ze ZKB** stran kybernetické bezpečnosti **na úrovni ZKI mají primárně práva** spojená s tím být kritickou infrastrukturou

Povinnosti dle nZKB a nZKI – digitální infrastruktura

Pro subjekty kritické infrastruktury v odvětví digitální infrastruktura platí pouze povinnosti podle § 11 odst. 6, § 12 a § 14 odst. 1 písm. a), j), o) a q). (§ 28 odst. 2 nZKI)

§ 11 odst. 6 nZKI = obecně ustanovení, které stanoví, že subjekt je povinný ode dne doručení rozhodnutí o zařazení na seznam subjektů KI do dne doručení rozhodnutí o vyřazení ze seznamu subjektů KI

§ 12 nZKI = **hlášení změn** v rozsahu základní služby (nová, širší, užší) do 1 měsíce od změny

§ 14 odst. 1:

a) **Poskytování informací** o základní službě a o rozsahu kritické infrastruktury na území ČR – gestor (NÚKIB) a MV (GŘHZS) = nutný podklad např. pro dodávky v krizových stavech

j) Označit **kritické dodavatele** a nahlásit je – gestor (NÚKIB) a MV (GŘHZS) = podklad pro „BDŘ“ na úrovni ZKI a pro oprávnění ke vstupu do uzavřeného prostoru viz dále

o) Využívat pro plnění povinností **Portál KI**

q) Informovat o potřebě zabezpečení **nezbytnými věcnými prostředky** – gestor (NÚKIB) a MV (GŘHZS) = nouzové dodávky

Rozložení povinností pro odvětví digitální infrastruktury

Ohlášení a hlášení kontaktních údajů	Stanovení rozsahu regulované služby	Bezpečnostní opatření	Hlášení kybernetických bezpečnostních incidentů	Dozor	Jmenování manažera KI/ manažera KB
= samoidentifikace + nahlášení kontaktní osoby	= vymezení okruhu infrastruktury, na kterou je třeba aplikovat další povinnosti nebo vztahovat oprávnění	= samotná náplň preventivní přípravy I ZKB má požadavky na fyzickou bezpečnost – pouze se vztahuje k ICT	Hlásí pouze kybernetické bezpečnostní incidenty = NÚKIB předává data GŘHZS	Kontrola plnění bezpečnostních opatření	Osoba zodpovědná za zavádění povinností dle daného zákona
ZKB i ZKI	ZKB i ZKI	ZKB	ZKB	ZKB	ZKB

Oprávnění dle nZKI – digitální infrastruktura

Oprávnění subjektu kritické infrastruktury (§ 14 odst. 3 nZKI):

a) při přípravě na krizové situace požádat o **poskytnutí přednostního telco připojení pro kritické pracovníky** u gestora (NÚKIB) a MV (GŘHZS)

b) během mimořádné události nebo za krizového stavu požádat o **zprostředkování vstupu do vymezených míst nebo území, kam byl vstup zakázán, a to i pro kritického dodavatele** u gestora (NÚKIB) a MV (GŘHZS)

c) za krizového stavu požádat o **poskytnutí přednostního přístupu k základní službě poskytované jiným subjektem** kritické infrastruktury

+ věcné prostředky v rámci nouzového plánování

Děkuji za pozornost.

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

regulace@nukib.gov.cz