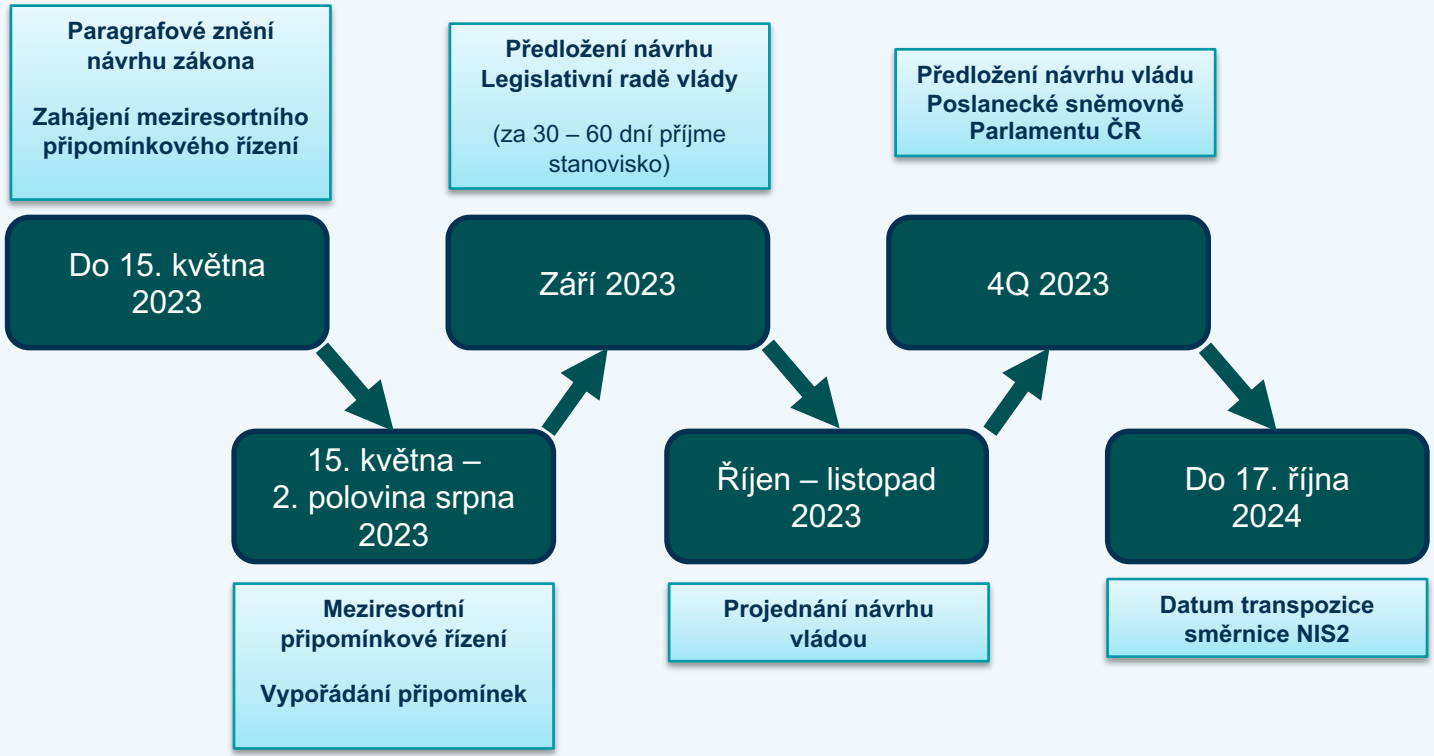
CHRENEK | TOMAN | KOTRBA

Nový zákon o kybernetické bezpečnosti

Mgr. Šimon Toman

Časová osa legislativního procesu

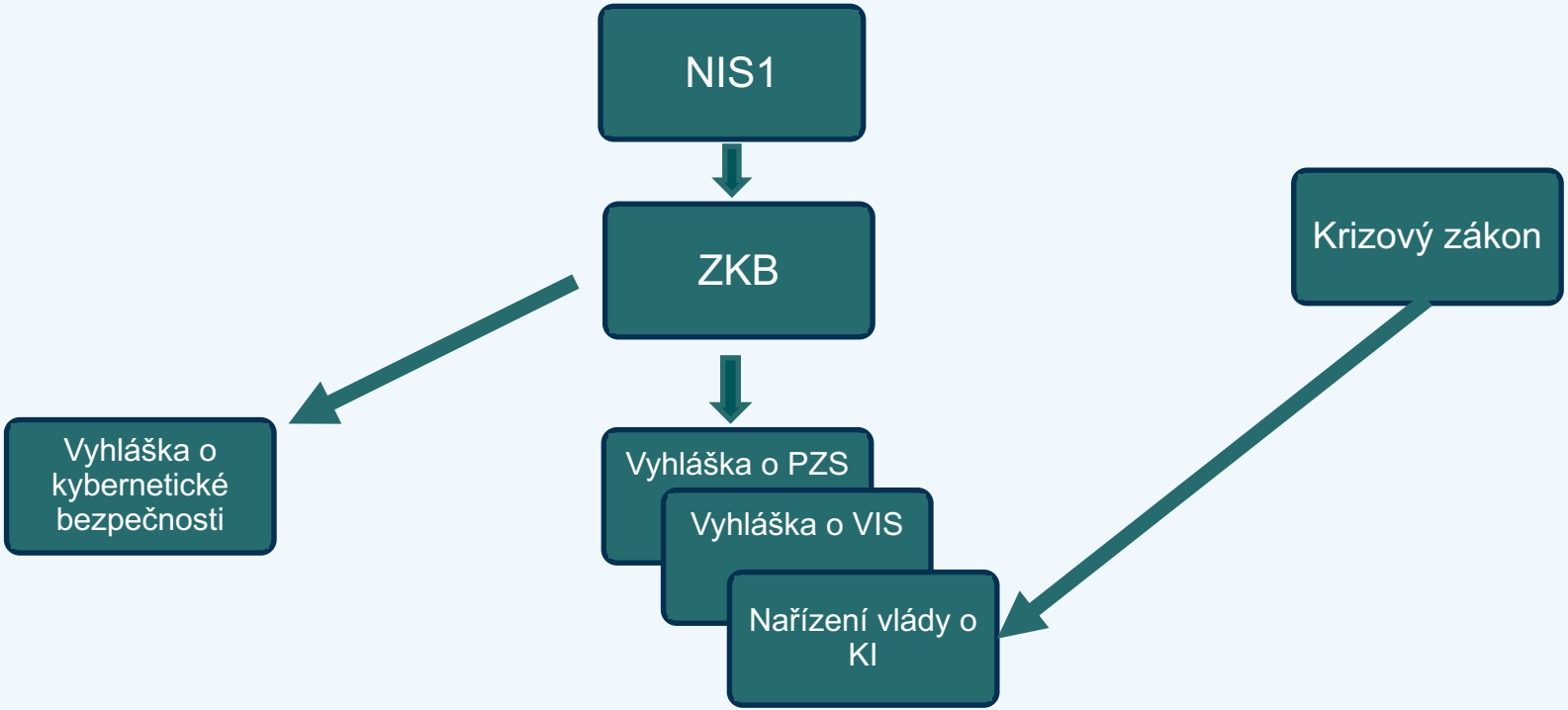


Hlavní regulační změny

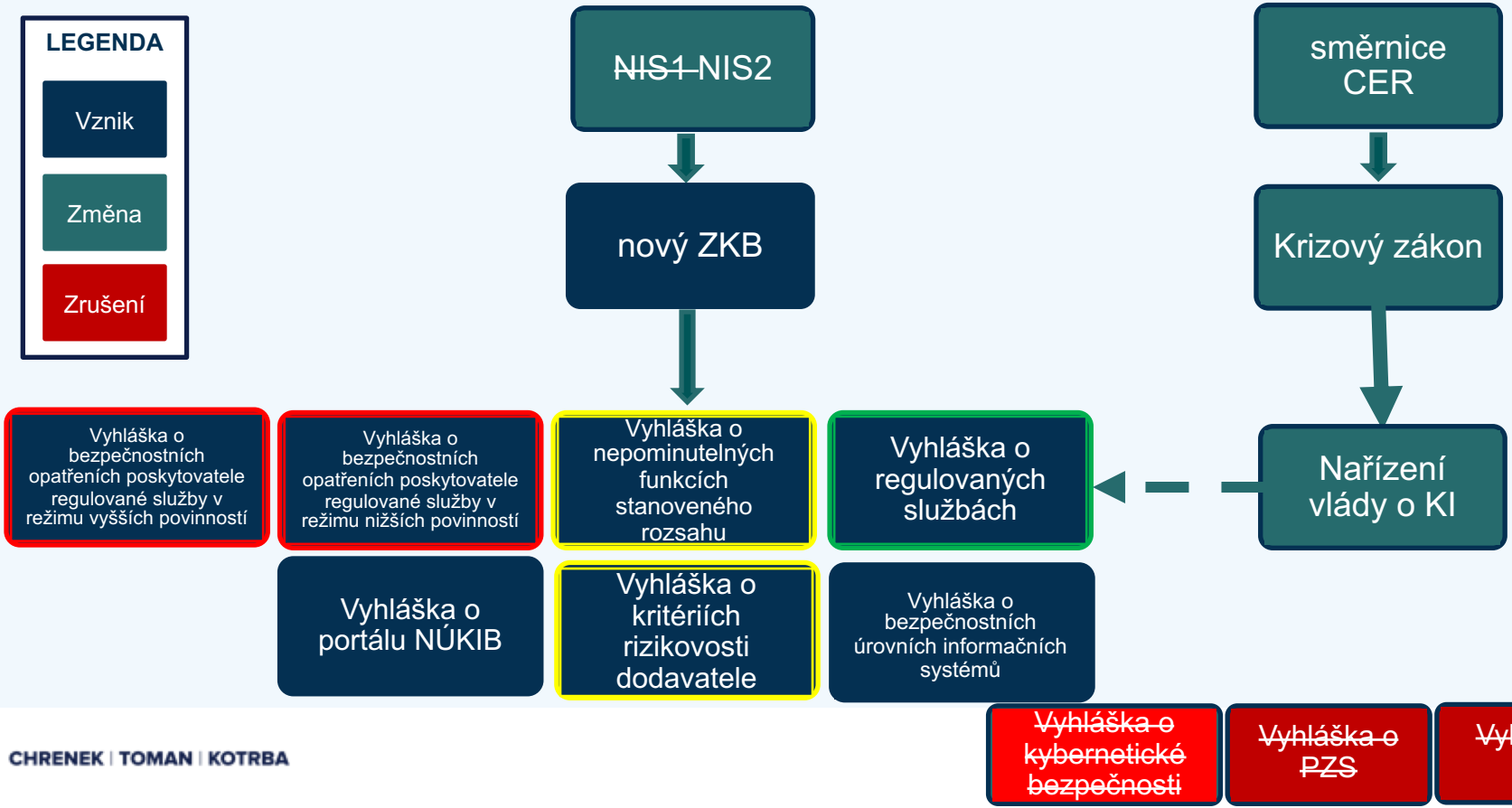
- Rozšíření počtu povinných osob
- Povinné vzdělávání vrcholového vedení organizace
- Zpřísnění sankcí
- Změny v procesu hlášení incidentů

- Aktuálně regulováno cca 400 povinných osob
- Nově regulováno minimálně 6 000 povinných osob (tzn. min 15x tolik)

Současný stav legislativy



Budoucí zamýšlený stav legislativy



Koho se nové povinnosti týkají dle směrnice NIS 2

- **Regulované služby** uvedeny v přílohách směrnice NIS 2
- Kybernetickou bezpečnost má být zajištěna např.
  - při výrobě elektřiny,
  - poskytování zdravotní péče,
  - poskytování služeb elektronických komunikací,
  - u dalších více než **60 služeb zařazených do 18 odvětví**
- Směrnice NIS2 nepředpokládá ukládání povinností každému subjektu, který danou službu poskytuje (viz čl. 2 směrnice NIS2 – zejm. s ohledem na kritérium velikosti podniku)

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 roov. skladovacích a přenosových zařízení.

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.

Pravidla regulace

Obecné pravidlo

Primární způsob stanovení, zda subjekt spadá pod regulaci směrnice, je **současné** naplnění následujících dvou pravidel:

1) organizace poskytuje **alespoň jednu službu** uvedenou v přílohách a zároveň
2) je **středním nebo velkým podnikem**

(tedy zaměstnává 50 a více zaměstnanců, nebo dosahuje ročního obratu nebo bilanční sumy roční rozvahy alespoň 10 milionů EUR (zhruba 250 milionů CZK)

Doplňující pravidla

Na vybrané subjekty se směrnice NIS2 vztahuje bez ohledu na jejich velikost

- dle čl. 2 odst. 2 směrnice NIS2 např.
  - poskytovatel služeb elektronických komunikací, poskytovatel služeb DNS…
  - poskytovatel služby, jejíž narušení mohlo mít významný dopad na veřejnou bezpečnost, veřejnou bezpečnost nebo ochranu zdraví osob
- povinné subjekty dle **směrnice CER**

Doporučení Komise 2003/361/ES
→ určení velikosti podniku

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

Návrh nového zákona o kybernetické bezpečnosti

Povinné osoby

- Jediný typ povinné osoby → „poskytovatel regulované služby“
- Poskytovatelem regulované služby je kdokoliv, kdo poskytuje alespoň **jednu regulovanou službu**
- Návrh nového zákona pracuje s tzv. režimy poskytovatele regulované služby:
  - Režim vyšších povinností (CCA 1000 subjektů)
  - Režim nižších povinností (CCA 5000 subjektů)

Stanovení regulované služby:

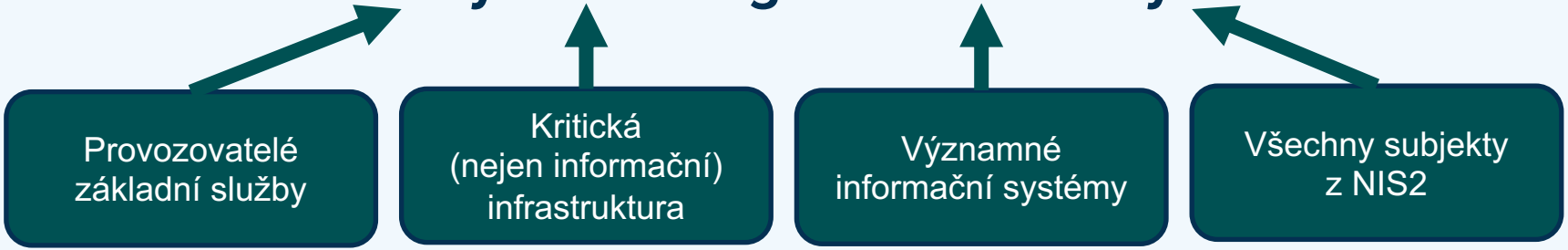
Vyhláška o regulovaných službách

- **kritéria pro identifikaci regulované služby** (samo-identifikace ze strany organizace)
- **kritéria pro určení regulované služby** (proces, kdy NÚKIB v rámci správního řízení s organizací zhodnotí, zda k naplnění kritérii došlo)

Návrh nového zákona o kybernetické bezpečnosti

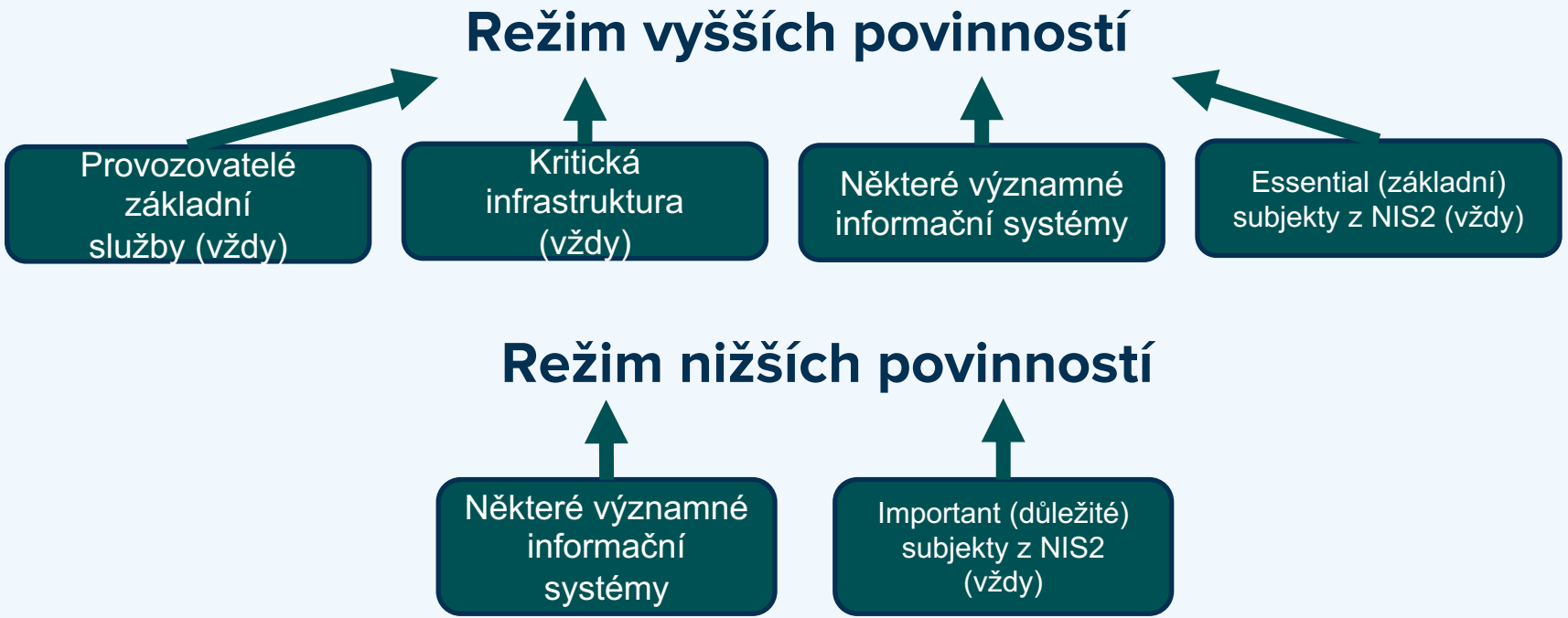
Jediný typ povinné osoby:

Poskytovatel regulované služby*

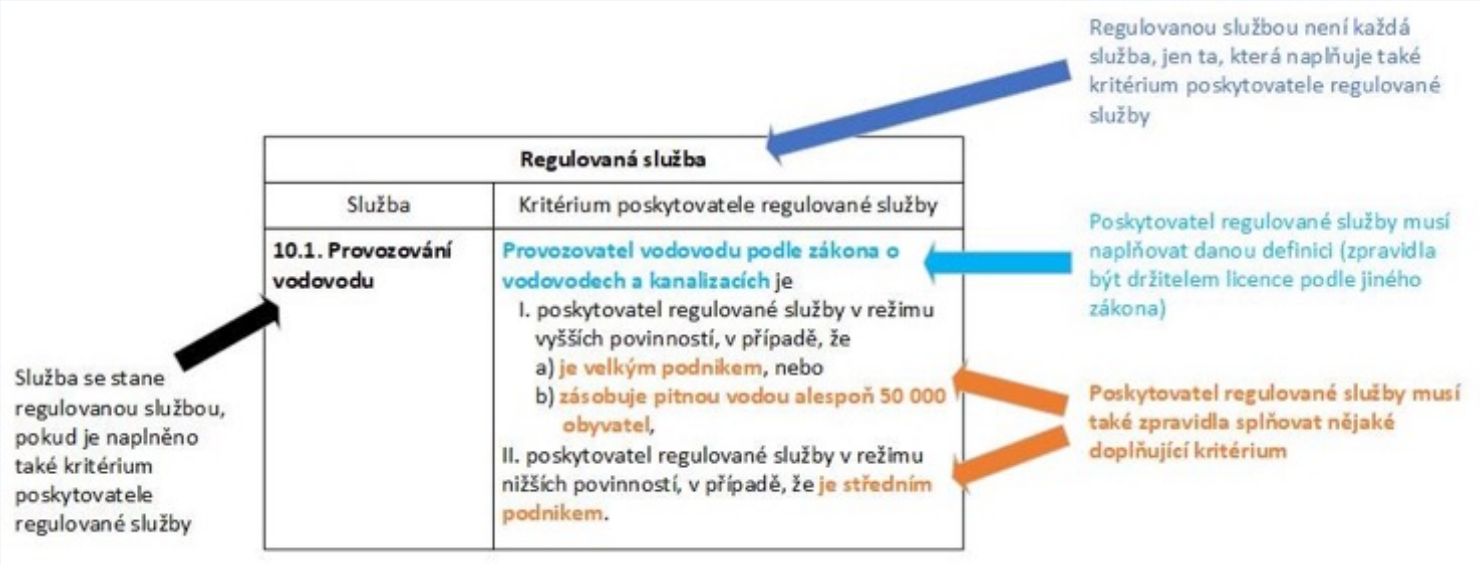


* **Poskytovatelem regulované služby je orgán nebo osoba, která poskytuje jednu nebo více regulovaných služeb (§ X Vymezení pojmů odst. 1 písm. c) nového ZKB).**

Návrh nového zákona o kybernetické bezpečnosti



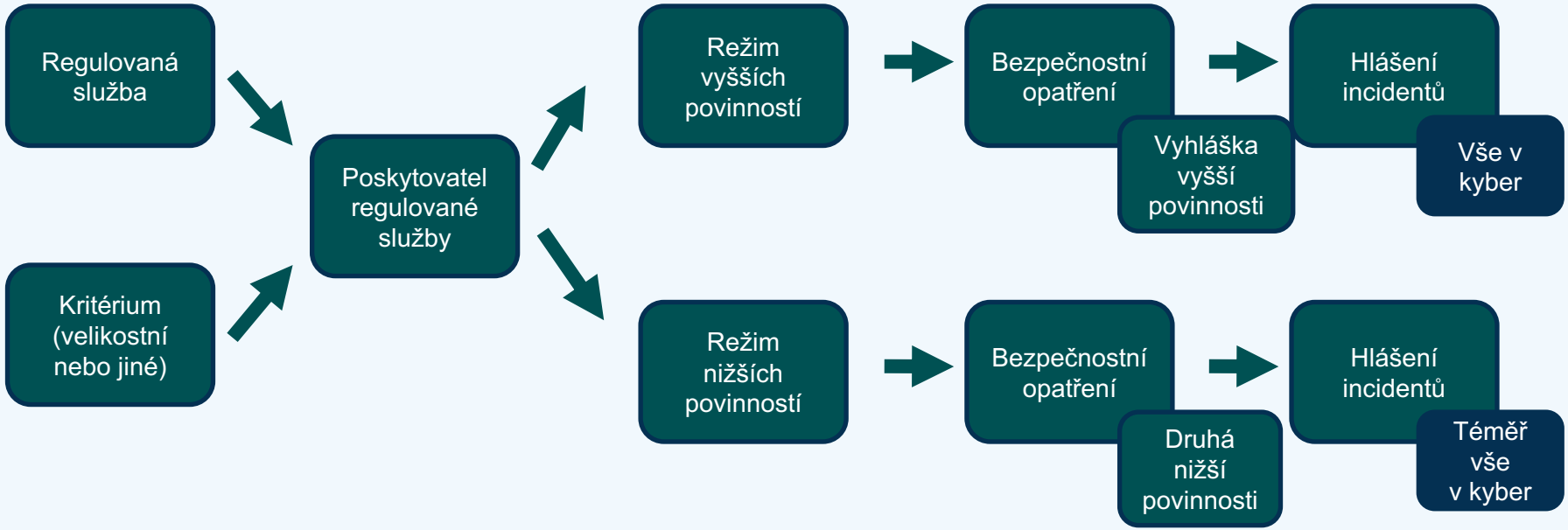
Vyhláška o regulovaných službách



Zdroj: web NÚKIB

Služba	Kritérium poskytovatele regulované služby
16.1. Poskytování veřejně dostupné služby elektronických komunikací	Podnikatel poskytující veřejně dostupnou službu elektronických komunikací podle zákona o elektronických komunikacích je: poskytovatel regulované služby **v režimu vyšších povinností**, v případě, že a) je velkým podnikem, b) je středním podnikem, c) je operátorem podle zákona o elektronických komunikacích poskytujícím veřejně dostupnou službu elektronických komunikací skrze **nejméně 350 000 aktivních mobilních SIM karet** na maloobchodním trhu na území České republiky, nebo d) je poskytovatelem nejméně **100 000 aktivních pevných internetových přípojek na území České republiky**, II. poskytovatel regulované služby v režimu **nižších povinností**, v případě, že a) je malým podnikem, b) je mikropodnikem.

Shrnutí stanovení povinných osob



Ohlašovací povinnost

Poskytovatel regulované služby

Režim vyšších povinností	Režim nižších povinností
Hlásí vše (s původem v kybernetickém prostoru)	Hlásí vše co je úmyslné – nehledě na význam dopadu – a to, co je významné, i kdyby to bylo neúmyslné* (s původem v kybernetickém prostoru)

*významnost stanoví sám subjekt dle co nejjednoduššího postupu v prováděcím právním předpise

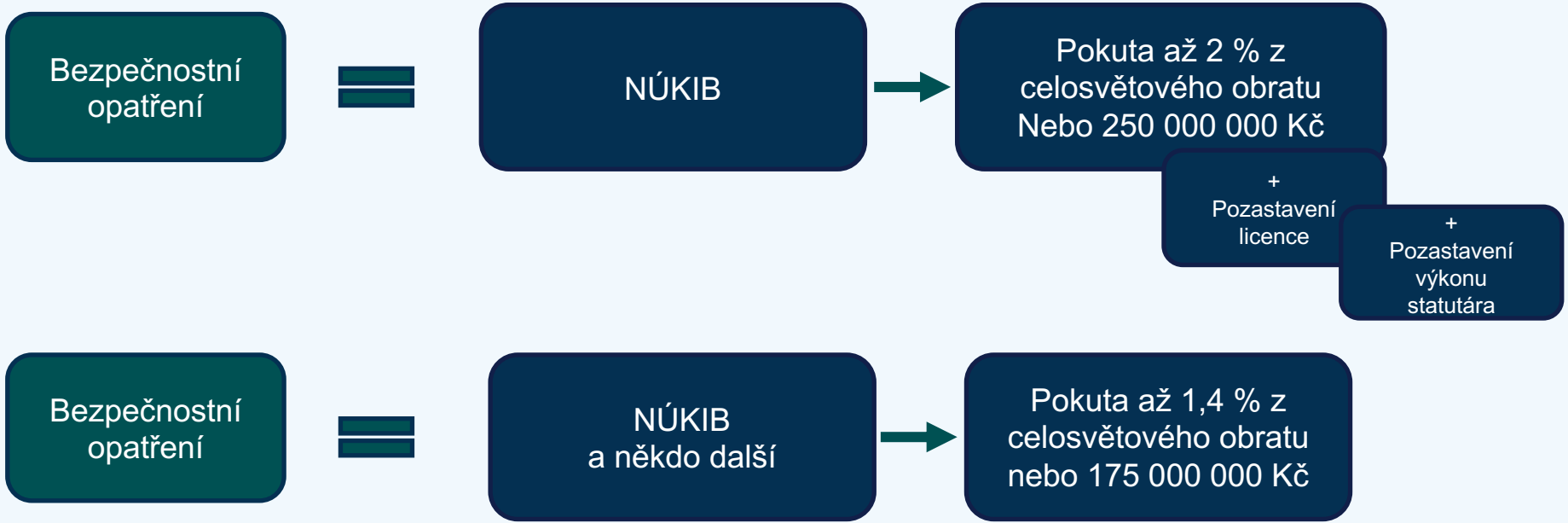
Registrace

- NÚKIB bude spolupracovat s odvětvovými regulátory a informace o poskytovatelích regulované služby bude **sám vyhledávat a tyto organizace bude upozorňovat na potřebu registrace**, **tato činnost však nenahrazuje povinnost organizace se sama registrovat, pokud identifikační kritéria naplní**

LHŮTY

- 90 dní od okamžiku, kdy organizace naplní daná kritéria (tj. do 90 dní od účinnosti zákona, případně kdykoliv v budoucnu, pokud organizace začne poskytovat některou z regulovaných služeb, nebo překročí daná kritéria)
- 30 dní od okamžiku, kdy zjistí, že kritéria naplňuje (tato lhůta se uplatní v rámci výše uvedených 90 dní).
- Po registraci následuje zápis do evidence poskytovatelů regulované služby

Kontrola a sankce



Mechanismus prověřování bezpečnosti dodavatelského řetězce

- Bezpečnostní rada státu svým usnesením ze dne **21. června 2022** uložila NÚKIB připravit návrh zákona k navýšení bezpečnosti dodavatelských řetězců strategické infrastruktury státu (vnitrostátní zadání)
- Mechanismus má řešit tzv. **strategické hrozby** pocházející z dodavatelského řetězce a rizika z nich plynoucí
- V rámci mechanismu se prověřuje **tzv. důvěryhodnost dodavatele**
- Cílem je identifikovat **hrozby** plynoucí **ze strany dodavatele či země**, mající na něj vliv, pro bezpečnost České republiky nebo vnitřní či veřejný pořádek
- V případě identifikace možné významné hrozby má NÚKIB možnost povinným osobám **stanovit podmínky či zakáže** využívání plnění dodavatele
- Dopadne na podmnožinu osob s vyššími povinnostmi (cca 150 subjektů)

Kdo bude prověřován?

- Dodavatelé **bezpečnostně významných dodávek** pro poskytovatele regulované služby v režimu vyšších povinností, kterým plynou povinnosti z mechanismu prověřování (povinné osoby mechanismu specifikované v § 6 vyhlášky o regulovaných službách)

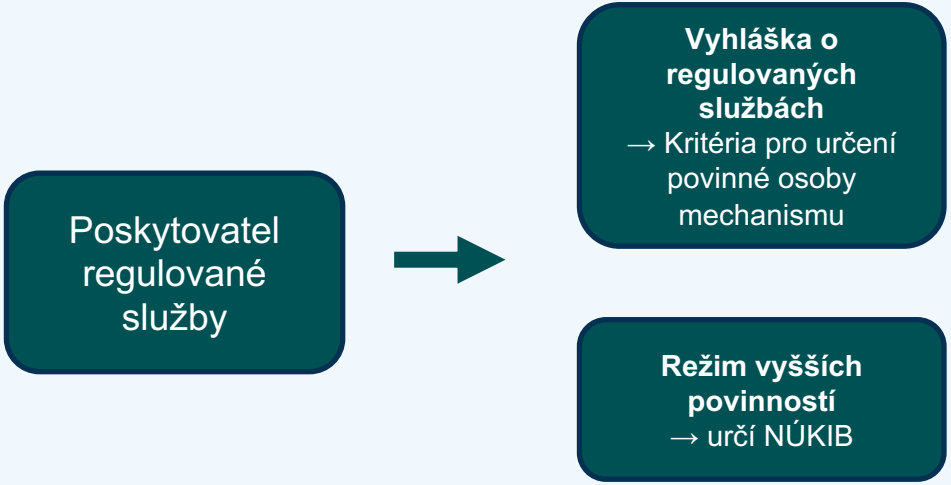
- Dodavatelem bezpečnostně významné dodávky je každý, kdo povinné osobě mechanismu prověřování poskytne přímo či jako poddodavatel **bezpečnostně významnou dodávku**

Co bude prověřováno?

- Rizikovost dodavatele bude posuzována na základě kritérií uvedených ve vyhlášce **o kritériích rizikovosti dodavatele**

- Posuzována budou mj. kritéria vztahující se ke **zemi** sídla dodavatele a jiných států působících na dodavatele, jakož i předchozí závadná aktivita jednak dodavatelů, jednak též zemí, majících na dodavatele vliv

Povinné osoby mechanismu



- Veřejná správa
- Energetika – Elektřina – provoz přenosové soustavy: Provoz distribuční soustavy,
- Energetika – Ropa a ropné produkty: Provoz ropovodu, provoz produktovodu
- Energetika – Plynárenství – provoz přepravní soustavy, provoz distribuční soustavy
- Letecká doprava – řízení letového provozu, letové navigační služby
- Drážní doprava – Stavení vlakových cest na celostátní úrovni
- Digitální infrastruktura (další slide)

- Digitální infrastruktura a služby
  - **Poskytování veřejně dostupné služby elektronických komunikací**
    - střední podniky - operátoři dle zákona o elektronických komunikacích poskytující veřejně dostupnou službu elektronických komunikací skrze **nejméně 350 000 aktivních mobilních SIM karet na maloobchodním trhu na území České republiky**
  - **Zajišťování veřejné komunikační sítě elektronických komunikací**
    - střední podniky - operátoři dle zákona o elektronických komunikacích poskytující veřejně dostupnou službu elektronických **komunikací skrze nejméně 350 000 aktivních mobilních SIM karet na maloobchodním trhu na území České republiky**
  - **Správa a provoz registru internetových domén nejvyšší úrovně**
  - **Poskytování služby cloud computingu**
    - je-li subjekt poskytovatelem státního cloud computingu podle zákona o informačních systémech veřejné správy

Rozsah regulace 1: Kritická část aktiva

Rozsah regulace 2: Bezpečnostně relevantní dodávka

- Bezpečnostně významnou dodávkou se rozumí plnění **směřující do kritické části stanoveného rozsahu** spočívající v **poskytnutí, vývoji, výrobě, sestavení, správě, provozu či servisu**

i) technického prostředku nebo vybavení s výpočetní kapacitou,
ii) programového prostředku nebo vybavení, nebo
iii) informační či komunikační služby,

- Dodavatelem bezpečnostně významné dodávky je každý, kdo povinné osobě mechanismu prověřování **poskytne přímo či jako poddodavatel bezpečnostně významnou dodávku**

Povinnost hlášení informací o dodavatelích

- **Povinná osoba mechanismu má povinnost:**

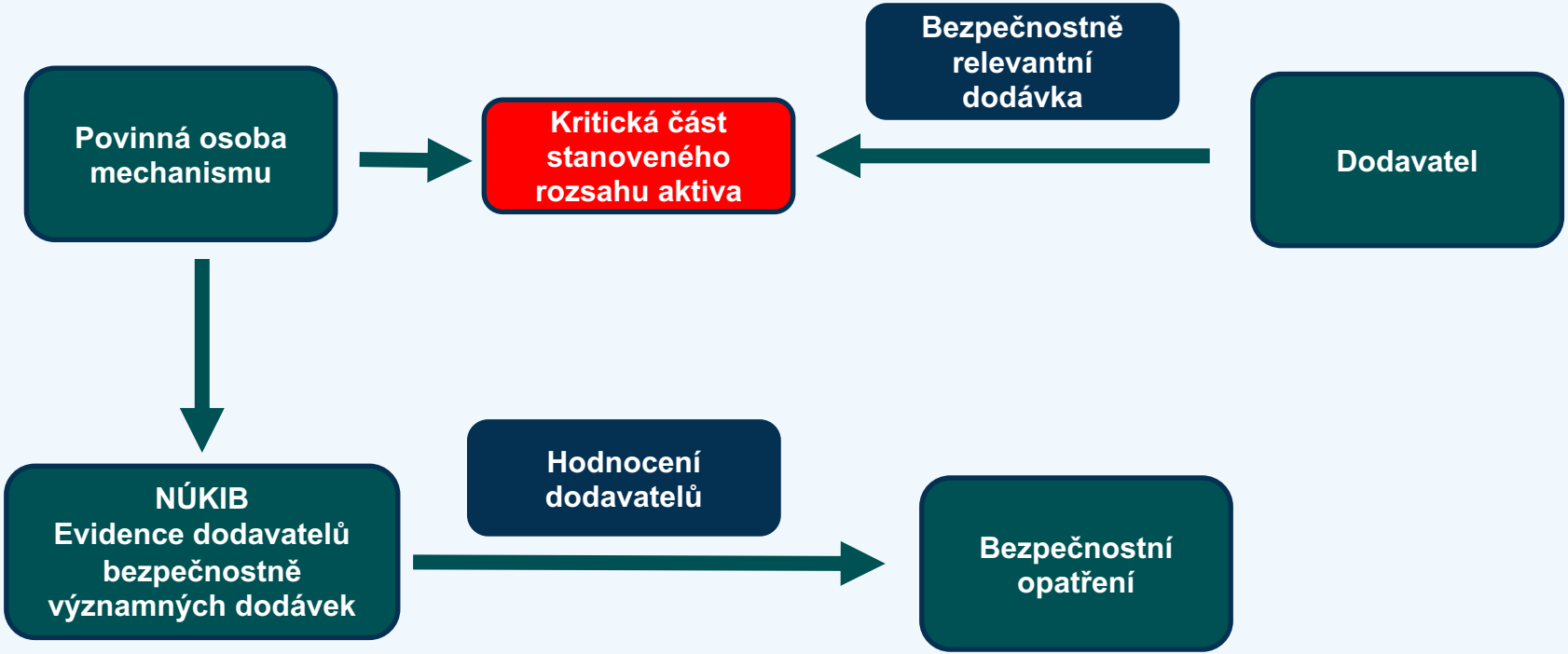
1) **zjišťovat** s vynaložením přiměřeného úsilí **informace o dodavatelích bezpečnostně významných dodávek** a dokumentovat tyto informace alespoň v rozsahu **identifikace všech bezpečnostně významných dodávek a dodavatelů bezpečnostně významných dodávek**

- **Následně má povinnost:**

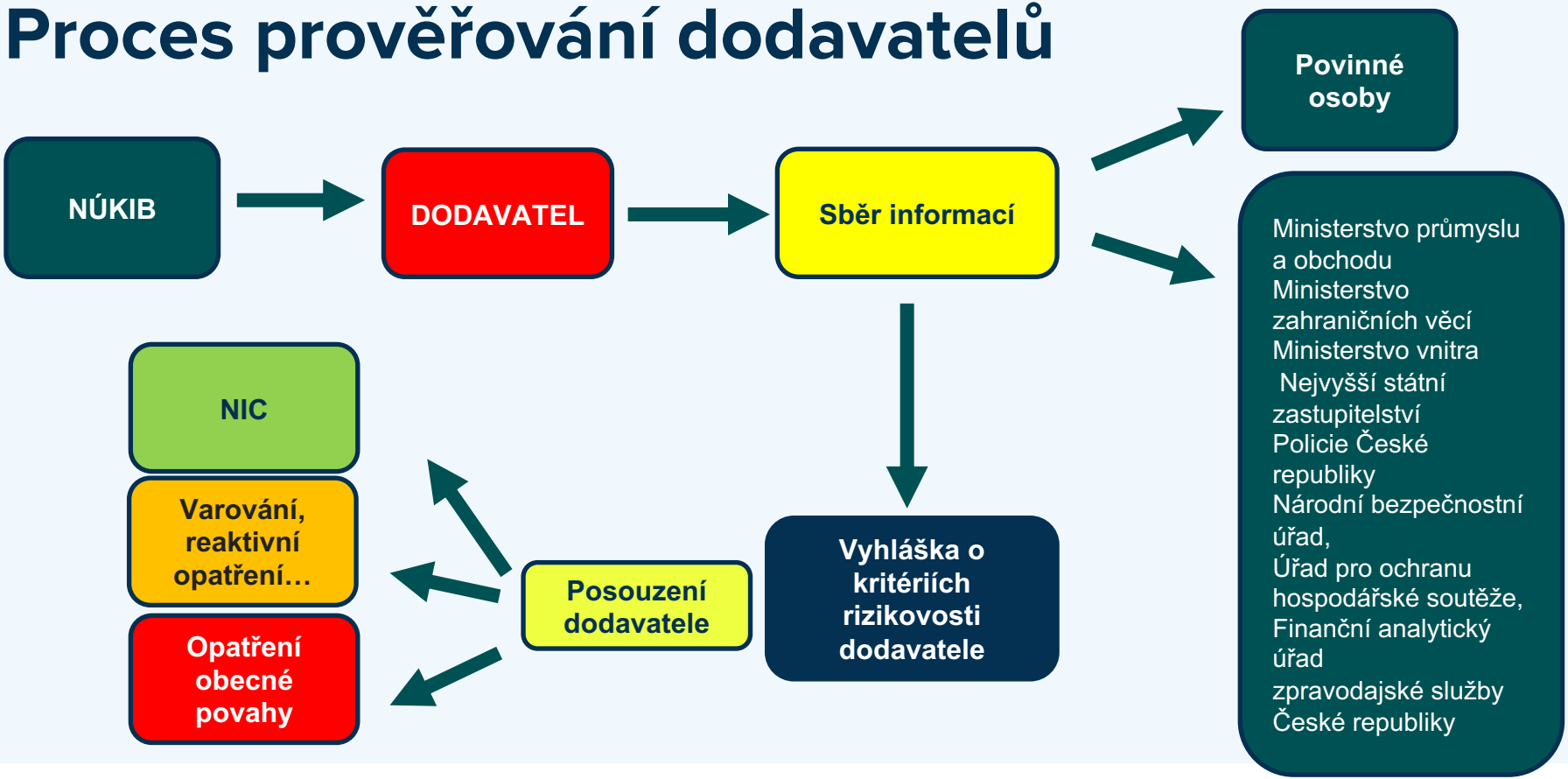
2) Tyto informace hlásit NÚKIB do 10 dní od jejich zjištění (podrobnosti stanoví vyhláška o Portálu NÚKIB)

Informace se stávají součástí evidence dodavatelů bezpečnostně významných dodávek

Schéma mechanismu prověřování bezpečnosti dodavatelského řetězce



Proces prověřování dodavatelů



Omezení rizik spojených s dodavatelem

- Opatření obecné povahy (OOP):

NÚKIB povinným osobám **stanoví podmínky** nebo **zakáže** využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu,

zjistí-li možné významné ohrožení bezpečnosti České republiky nebo vnitřního veřejného pořádku v důsledku vyhodnocení kritérii rizikovosti dodavatele

- Návrh OOP NÚKIB doručí veřejnou vyhláškou, kterou vyvěsí na své úřední desce
- Povinné osoby a dodavatele vyzve k podání připomínek, **nestanoví-li NÚKIB jinak**
- NÚKIB přezkoumá alespoň jednou za tři roky trvání skutečností, na jejichž základě bylo OOP vydáno

Připomínky k mechanismu

- Dodavatel se neposuzuje v kontextu konkrétní bezpečnostní dodávky
- Bezpečnostní dodávku lze v tomto ohledu považovat za spouštěč mechanismu
- Případný zákaz dodavatele se dle dikce zákona se bude vztahovat na všechny povinné osoby bez rozdílu
- Proces vydání OOP není správním řízením - povinné osoby ani dodavatelé tak nejsou účastníkem řízení a nepřísluší jim tak práva s tímto postavením spojená

ZDROJE

Primární zdroje:

- návrh nového zákona o kybernetické bezpečnosti a prováděcích vyhlášek
- směrnice EP 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 (směrnice NIS2)
- prezentace Adama Kučínského, NÚKIB
- webové stránky NÚKIB (nis2.nukib.cz)
- informace sdělené NÚKIB v rámci vypořádání připomínek z návrhu nového ZKB

Děkujeme NÚKIB za transparentní jednání v rámci celé přípravy nového zákona

CHRENEK | TOMAN | KOTRBA

Chrenek, Toman, Kotrba advokátní kancelář spol. s r.o.
Těšnov 1/1059, Praha 1, PSČ 110 00,
Česká republika
IČO: 285 05 913
Tel.: (+420) 221 875 402-9
www.chrenektomankotrba.cz

POBOČKA Brno:
Smetanova 19, Brno, PSČ 602 00

POBOČKA Olomouc:
nábř. Přemyslovců 867/8, Olomouc, PSČ 779 00

POBOČKA Bratislava:
Palisády 56, Bratislava - mestská časť Staré Mesto, PSČ 811 06

Zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 146526

CHRENEK | TOMAN | KOTRBA

Děkuji za pozornost

Kontaktní osoba:

Mgr. Šimon Toman

E-mail: s.toman@chtk.cz
Tel.: (+420) 721 521 540