Nový zákon o kybernetické bezpečnosti

Novinky a aktuální stav

NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

Jan Hénik
Michaela Henzlová
oddělení regulace veřejného sektoru

13. prosince 2023
TLP: CLEAR

Východiska obsahu návrhu zákona

Směrnice NIS 2.0

Transpozice 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

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

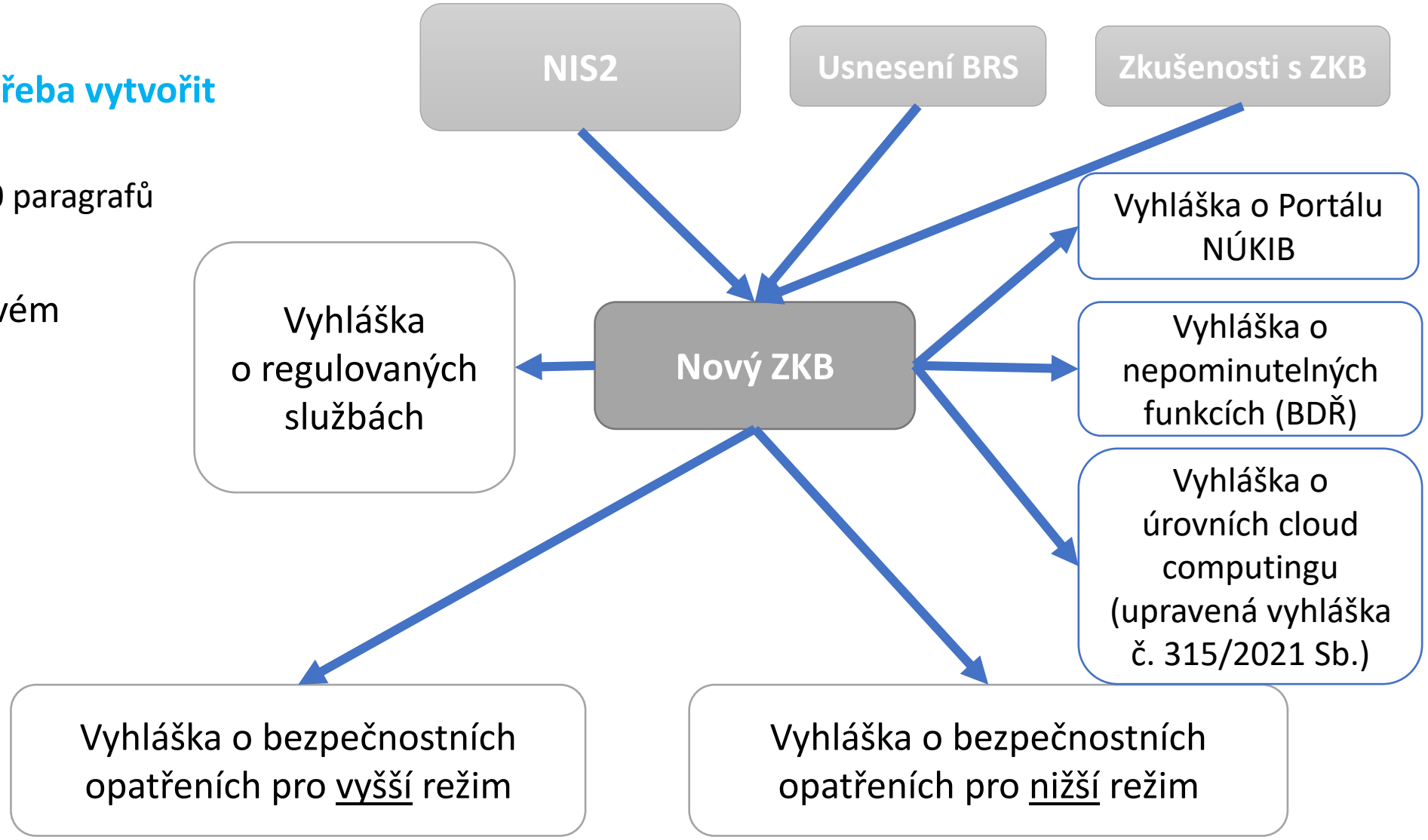
Reflexe poznatků a dosavadních zkušeností, odstranění současných nedostatků, zohlednění podnětů a připomínek a další doplňující úpravy

Nový zákon o kybernetické bezpečnosti (nZKB) v MPŘ

Změn je tolik, že bylo **potřeba vytvořit nový zákon**

= zcela nová úprava – cca 70 paragrafů

Verze v mez. připomínkovém řízení má aktuálně navíc **6 vyhlášek.**



nZKB

Vyhláška o regulovaných službách

Kritéria pro identifikaci regulované služby v odvětvích

- veřejná správa
- energetika
- výrobní průmysl
- potravinářský průmysl
- chemický průmysl
- vodní hospodářství
- odpadové hospodářství
- doprava
- digitální infrastruktura a služby
- finanční trh
- zdravotnictví
- věda, výzkum a vzdělávání
- poštovní a kurýrní služby
- vojenský průmysl
- vesmírný průmysl

Nový ZKB

Pravidla pro identifikaci a určení poskytovatelů regulovaných služeb

Povinnosti poskytovatelů regulovaných služeb

Bezpečnost dodavatelského řetězce

Oprávnění Úřadu, dozor

Vyhlášky o bezpečnostních opatřeních

Technická a organizační bezpečnostní opatření

Stanovení významnosti dopadu kybernetického bezpečnostního incidentu

Podrobnosti k likvidaci dat

Nový zákon o kybernetické bezpečnosti

Aktuální stav

NÚKIB

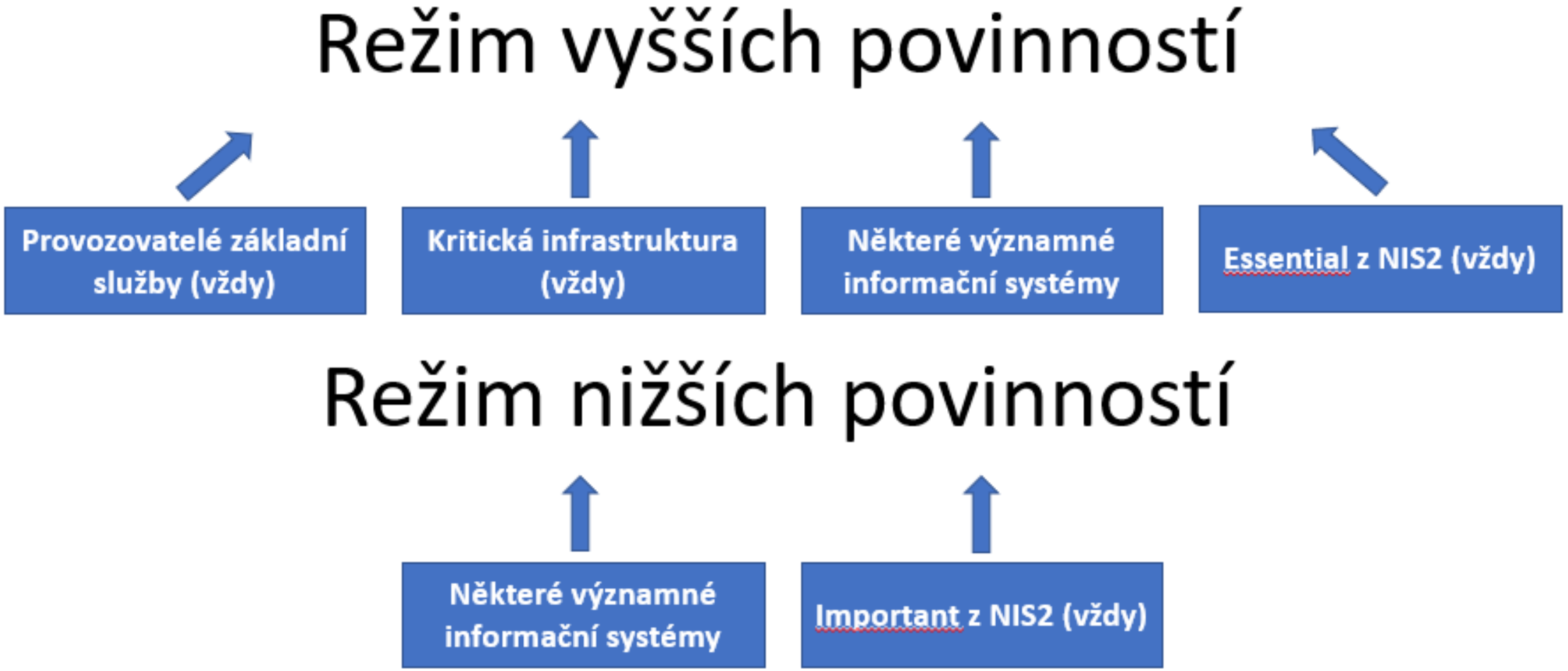
Národní úřad
pro kybernetickou
a informační
bezpečnost

nZKB – povinné osoby

Jedna jediná povinná osoba*:

*Pro primární sadu některých povinností spojených s prevencí – zavádění bezpečnostních opatření, hlášení incidentů, apod.

nZKB – povinné osoby



Regulovaná služba a její režim

Regulovanou službou je služba

- **naplňující** alespoň jedno **kritérium pro identifikaci** regulované služby **podle vyhlášky o regulovaných službách (objektivní naplnění kritérií)**

nebo

- **určená rozhodnutím NÚKIBu** na základě **kritéria pro určení** regulované služby

Režim poskytovatele regulované služby stanovuje **míru jemu uložených povinností**
(tzn. dvojrychlostní kybernetická bezpečnost).
Režim poskytovatele regulované služby je stanoven vyhláškou o regulovaných službách, s výjimkou služeb určených NÚKIBem, pak je režim jejího poskytovatele vždy režimem vyšších povinností.

Každý poskytovatel regulované služby má pro všechny poskytované regulované služby stanoven jen jeden režim. Poskytovatel regulované služby, kterému je stanoven režim vyšších povinností pro alespoň jednu jím poskytovanou regulovanou službu, má stanoven režim vyšších povinností pro všechny jím poskytované regulované služby (jednotnost).

NIS2 – regulované služby

Směrnice NIS1:

7 odvětví

Kritéria dopadu incidentu

⇒ **cca 400 povinných osob**

Směrnice NIS2:

18 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, 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.

Povinné osoby – odvětví, služby

- Vše podle NIS2
- Nad rámec požadavků NIS2
  - Vybrané subjekty v odvětví **letectví** – po konzultaci s ÚCL
  - Vybrané subjekty v oblasti **výzkumu a vývoje** (nekomerční užití, veřejné financování, citlivá činnost, velké výzkumné infrastruktury; vysoké školy)
  - **Vojenský průmysl** – vojenský materiál, zboží a technologie dvojího užití
  - **Vybrané instituce veřejné správy**
- Celkem 107 služeb v 22 odvětvích (mírně odlišná taxonomie než NIS2)

NIS2 – velikost podniku

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

Kategorie podniku	Počet zaměst-nanců: roční pracovní jednotka (RPJ)	Roční obrat	nebo	Bilanční
Střední podnik	< 250	≤ 50 milionů EUR	nebo	≤ 4
Malý podnik	< 50	≤ 10 milionů EUR	nebo	≤ 1
Mikropodnik	< 10	≤ 2 miliony EUR	nebo	≤

TLP: CLEAR

DEFINICE MALÉHO A STŘEDNÍHO PODNIKU

Při posuzování statutu malého a středního podniku (MSP) je nutné posuzovat i vztah k tzv. propojeným podnikům. Při výpočtech tak záleží na výši vlastnického podílu každého jednotlivého podniku, který má vlastnickou vazbu na zkoumaný podnik a naopak. Pro stanovení celkového počtu zaměstnanců, ročního obratu či bilanční sumy roční rozvahy zkoumaného podniku se tak započítávají i údaje propojených podniků.

3 DRUHY PROPOJENÝCH PODNIKŮ

1. SAMOSTATNÝ PODNIK
Každý podnik, který vlastní méně než 25 % základního kapitálu nebo hlasovacích práv jiného podniku. **Údaje za tento podnik se nepřičítají.**

2. PARTNERSKÝ PODNIK
Každý podnik, který vlastní 25 % - 50 % základního kapitálu nebo hlasovacích práv jiného podniku. **Údaje za tento podnik se přičítají ve výši procentuálního vlastnického podílu.**

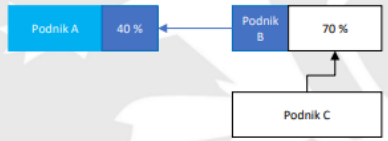
3. SPOJENÝ PODNIK
Každý podnik, který vlastní více než 50 % základního kapitálu nebo má právo uplatňovat rozhodující vliv v jiném podniku. **Údaje za tento podnik se přičítají v plné výši bez ohledu na procentuální vlastnický podíl.**

VÝJIMKY
Podnik se může považovat za nezávislý, a nemít tudíž žádné partnerské podniky, i tehdy, je-li 25% práh dosažen nebo překročen některým z investorů uvedených v doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků.

PŘÍKLADY VÝPOČTŮ

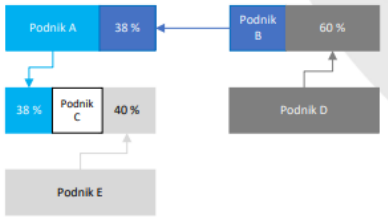
PŘÍKLAD 1
Posuzovaný podnik A je vlastněn ze 40 % podnikem B. K údajům za podnik A tedy přičítáme 40 % zaměstnanců a 40 % ročního obratu a aktiv podniku B.
Výsledek = 100 % A + 40 % B

PŘÍKLAD 2
Posuzovaný podnik A je vlastněn ze 40 % podnikem B. Podnik B je navíc vlastněn podnikem C ze 70 %. Jelikož je mezi podnikem B a C spojenecký vztah, musíme k údajům za podnik A přičíst nejen 40 % zaměstnanců a 40 % ročního obratu a aktiv podniku B, ale rovněž podniku C.
Výsledek = 100 % A + 40 % B + 40 % C



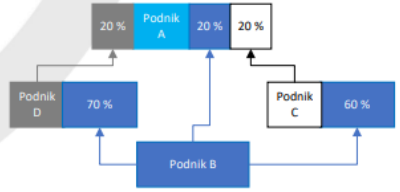
PŘÍKLAD 3
Posuzovaný podnik A vlastní z 51 % podnik B. K údajům za podnik A tedy přičítáme 100 % zaměstnanců a 100 % ročního obratu a aktiv podniku B.
Výsledek = 100 % A + 100 % B

PŘÍKLAD 4
Posuzovaný podnik A je vlastněn z 38 % podnikem B. Zároveň podnik A vlastní 38 % podniku C. Podnik B je vlastněn podnikem D z 60 %, a podnik C je vlastněn podnikem E ve výši 40 %. K údajům za podnik A tedy přičítáme 38 % zaměstnanců a 38 % ročního obratu a aktiv podniku B, dále 38 % z podniku C. Jelikož je podnik D ve spojeneckém vztahu k podniku B, musíme přičíst i 38 % z podniku D ve výši vlastněného podílu podniku B v posuzovaném podniku A. Údaje za podnik E nepřičítáme, protože se jedná o partnerský podnik námi vlastněného podniku C.
Výsledek = 100 % A + 38 % B + 38 % C + 38 % D



PŘÍKLAD 5
Posuzovaný podnik A je vlastněn z 60 % podnikem B. Podnik B má dva partnery, a to podnik C, který vlastní 32 % podniku B, a podnik D, který vlastní 25 % podniku B. K údajům za podnik A tedy přičítáme 100 % zaměstnanců a 100 % ročního obratu a aktiv podniku B, dále 32 % podniku C, a 25 % podniku D.
Výsledek = 100 % A + 100 % B + 32 % C + 25 % D

PŘÍKLAD 6
Posuzovaný podnik A je vlastněn podniky B, C a D, jejichž podíl je u každého roven 20 %. Při letmém posouzení našeho vztahu k podnikům by se mohlo zdát, že se jedná o samostatný podnik, jelikož jednotlivé podíly nepřekračují hranici 25 %. Jelikož jsou ale podniky B, C a D vzájemnými spojenci, musíme jejich podíly na našem podniku A sečíst. Tím se dostáváme přes hranici 50% podílu na vlastnictví a všechny tři podniky se stávají našimi spojenci. Z toho vyplývá, že při výpočtu musíme přičíst údaje za celou skupinu.
Výsledek = 100 % A + 100 % B + 100 % C + 100 % D



Podrobnější výpočty a informace o tom, co vše započítat do velikosti zkoumaného podniku lze nalézt v uživatelské příručce k definici malých a středních podniků: **https://osveta.nukib.cz/pluginfile.php/58365/mod_page/content/311/Priloha-4_U%C5%BEivatelsk%C3%A1%20p%C5%99%C3%ADru%C4%8Dka%20k%20definici%20mal%C3%BDch%20a%20st%C5%99edn%C3%ADch%20podnik%C5%AF.pdf**

verze 1.0, platná ke dni 14.11.2022

Dostupné z: Uživatelská příručka k definici malých a středních podniků (nukib.cz), 2022-11-14_Pocitani-velikosti-podniku_Zjednodusene_v1.0_final.pdf (nukib.cz)

veřejné správě

1. Veřejná správa

Regulovaná služba	
Služba	**Kritérium poskytovatele regulované služby a jeho režim pro tuto službu**
1.1. Výkon svěřených pravomocí	Orgán nebo osoba je I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že je a) ústředním orgánem státní správy, b) jiným správním úřadem s celostátní působností neuvedeným v písm. a), a to včetně ústředí a generálního ředitelství územně dekoncentrovaných (specializovaných) orgánů státní správy, c) Kanceláří prezidenta republiky, d) Kanceláří Senátu, e) Kanceláří Poslanecké sněmovny, f) Českou národní bankou, g) Policejním prezidiem, h) útvarem policie s celostátní působností,¶ i) Generální inspekcí bezpečnostních sborů ~~ij~~) Generálním ředitelstvím hasičského záchranného sboru, ~~jk~~) krajským ředitelstvím hasičského záchranného sboru, ~~kl~~) Kanceláří Veřejného ochránce práv, ~~lm~~) Nejvyšším kontrolním úřadem,¶ n) Úřadem pro zastupování státu ve věcech majetkových¶ o) Správou úložišť radioaktivních odpadů,¶ p) orgánem soudní moci, q) státním zastupitelstvím, r) zdravotní pojišťovnou, s) krajem, nebo t) hlavním městem Praha.~~, nebo~~¶ ~~rs) obcí s rozšířenou působností s nejméně 125 000 obyvateli,~~ II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je a) územně dekoncentrovaným (specializovaným) orgánem státní správy, b) profesní komorou[5], c) vysokou školou, d) Akademií věd České republiky, nebo e) obcí s rozšířenou působností. ~~s počtem obyvatel do 125 000.~~

Regulovaná služba a její režim

Kritéria pro

§ 5

Kritéria pro určení regulované služby

1) Regulovanou službou je dále služba určená orgánu nebo osobě rozhodnutím Úřadu v případě, že
   a) jde o službu uvedenou ve vyhlášce Úřadu stanovující kritéria pro identifikaci regulovaných služeb a
      1. orgán nebo osoba je jediným poskytovatelem této služby v České republice a tato služba je zásadní pro zachování nezbytných společenských nebo ekonomických činností v České republice,
      2. narušení této služby by mohlo mít významný dopad na bezpečnost České republiky, vnitřní či veřejný pořádek nebo veřejné zdraví,
      3. narušení této služby by mohlo vyvolat významná systémová rizika, zejména v odvětvích, kde by takové narušení mohlo mít přeshraniční dopad, nebo
      4. orgán nebo osoba je kvůli svému specifickému významu na regionální nebo celostátní úrovni zásadní pro konkrétní odvětví nebo typ služby nebo pro jiná vzájemně propojená odvětví v České republice,
   b) její narušení může způsobit závažný zásah do života postihující více než 125 000 osob, a to prostřednictvím ohrožení života, zdraví, majetkové hodnoty, vnitřního či veřejného pořádku, bezpečnosti nebo životního prostředí,
   c) její narušení může způsobit závažný zásah do schopnosti poskytovat jinou regulovanou službu stejného nebo jiného poskytovatele regulované služby v režimu vyšších povinností, nebo
   d) orgán nebo osoba 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.

Hlavní povinnosti poskytovatele regulované služby

Registrovat regulovanou službu

Hlásit kontaktní a další údaje

Stanovit rozsah řízení kybernetické bezpečnosti

Zavádět bezpečnosti opatření

- Vyšší režim
- Nižší režim

Hlášení kybernetických bezpečnostních incidentů

- Vyšší režim
- Nižší režim

Protiopatření

- Výstraha, varování, reaktivní opatření

Informační povinnost poskytovatele regulované služby

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**.

Úřad je oprávněn poskytovateli regulované služby uložit povinnost informovat uživatele regulované služby o tomto incidentu.

Poskytovatel regulované služby je **povinen** bez zbytečného odkladu vhodným a srozumitelným způsobem **informovat uživatele regulované služby**, který může být ovlivněn významnou hrozbou, **o takových krocích, které může uživatel učinit v reakci na tuto hrozbu, aby byl případný dopad její realizace na tohoto uživatele co nejmenší**.

Lhůty pro plnění povinností

Registrovat regulovanou službu

→ **Do 30, resp. 90 dnů od naplnění identifikačních kritérií**

Hlásit kontaktní a další údaje

→ **Do 30 dnů (nové), resp. 15 dnů (změny)**

Stanovit rozsah řízení kybernetické bezpečnosti

→ **Kdykoli (ALE do doby stanovení je rozsahem celá organizace)**

Zavádět bezpečnosti opatření

- Vyšší režim
- Nižší režim

→ **Do 1 roku od vyrozumění od zařazení do evidence**

Hlášení kybernetických bezpečnostních incidentů

- Vyšší režim
- Nižší režim

→ **Do 1 roku od vyrozumění od zařazení do evidence**

Protiopatření

- Výstraha, varování, reaktivní opatření

→ **Ihned (lhůty v protiopatření)**

Informační povinnost poskytovatele regulované služby

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**.

Úřad je oprávněn poskytovateli regulované služby uložit povinnost informovat uživatele regulované služby o tomto incidentu.

Poskytovatel regulované služby je **povinen** bez zbytečného odkladu vhodným a srozumitelným způsobem **informovat uživatele regulované služby**, který může být ovlivněn významnou hrozbou, **o takových krocích, které může uživatel učinit v reakci na tuto hrozbu, aby byl případný dopad její realizace na tohoto uživatele co nejmenší**.

→ **Ihned (ALE vychází z bezpečnostních opatření a hlášení incidentů)**

Bezpečnostní opatření – rozdíly vyšší a nižší režim

- Redukovaná bezpečnostní opatření pro nižší režim

organizační opatření – **vyšší** režim

1. systém řízení bezpečnosti informací,
2. povinnosti pro vrcholové vedení,
3. bezpečnostní role,
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 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, řídící a obdobná specifických aktiv

bezpečnostní opatření – **nižší** režim

1. povinnosti vrcholového vedení
2. bezpečnost lidských zdrojů
3. řízení kontinuity činností
4. řízení přístupu
5. řízení identit a jejich oprávnění
6. detekce a zaznamenávání kybernetických bezpečnostních událostí
7. řešení kybernetických bezpečnostních incidentů
8. bezpečnost komunikačních sítí
9. aplikační bezpečnost
10. kryptografické algoritmy

Rozdíl mezi bezpečnostními opatřeními pro nižší a vyšší režim

NIŽŠÍ REŽIM

§ 7
Řízení kontinuity činností

Povinná osoba v rámci řízení kontinuity činností

1. v rámci primárních aktiv stanoví jejich prioritu a pořadí a postupy jejich obnovy,
2. stanoví odpovědnosti a povinností při obnově podle písm. a),
3. vytváří pravidelné zálohy nastavení technických aktiv, informací a dat nezbytných zejména pro účely obnovy regulované služby pro případ kybernetického bezpečnostního incidentu.

VYŠŠÍ REŽIM

§ 16
Řízení kontinuity činností

1. Povinná osoba v rámci řízení kontinuity činností
2. stanoví metodiku pro provedení analýzy dopadů,
3. pomocí analýzy dopadů vyhodnotí a dokumentuje možné dopady kybernetických bezpečnostních incidentů a zohlední hodnocení rizik podle § 9, v rámci kterého posoudí možná rizika související s ohrožením kontinuity činností,
4. na základě výstupů analýzy dopadů a hodnocení rizik podle písmene b) stanoví cíle řízení kontinuity činností formou určení
    5. minimální úrovně poskytovaných služeb, která je přijatelná pro užívání, provoz a správu regulované služby,
    6. doby obnovení chodu, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb regulované služby a
    7. bodu obnovení dat jako časové období, za které musí být zpětně obnovena data po kybernetickém bezpečnostním incidentu nebo po selhání,
8. stanoví politiku řízení kontinuity činností, která obsahuje naplnění cílů podle písmene c) a stanoví práva a povinnosti administrátorů a osob zastávajících bezpečnostní role,
9. vypracuje, aktualizuje a pravidelně testuje plány kontinuity činností a plány obnovy související s poskytováním regulované služby a
10. realizuje bezpečnostní opatření pro zvýšení odolnosti podle § 27.
11. Cíle řízení kontinuity podle odst. 1 písm. c) tohoto ustanovení jsou stanoveným časem a kvalitou regulované služby podle § X [Zajištění dostupnosti strategicky významné služby] zákona. Stanoveným časem je doba obnovení chodu podle odst. 1 písm. c) bod ii) tohoto ustanovení a stanovenou kvalitou regulované služby je minimální úroveň poskytovaných služeb podle odst. 1 písm. c) bod i) tohoto ustanovení.

nZKB – povinnosti PRS – hlášení incidentů

Režim vyšších povinností

Hlásí vše
(s původem v kybernetickém prostoru)

Režim nižších povinností

Hlásí incidenty s významným dopadem*
(s původem v kybernetickém prostoru)

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

nZKB – protiopatření

Opatření (nově Protiopatření)

- K podstatným změnám v logice opatření nedochází, mění se textace a některé detaily
- Staronový institut – **Výstraha**
  - Jde o upozornění, které je veřejné, nezávazné
  - Vydává se z důvodu ochrany, pořádku, bezpečnosti, života a zdraví nebo ekonomiky
  - Muže být vydáno jako info o incidentu nebo o porušování ZKB
- **Varování** – o hrozbě nebo zranitelnosti – veřejné i neveřejné, musí se promítnout do analýzy rizik u vyššího režimu
- **Reaktivní protiopatření** – k řešení incidentu, zabezpečení před incidentem, ke zvýšení ochrany aktiv
  - Konkrétní úkony, technická opatření či postupy – pro adresáty povinné
  - Rozhodnuti – adresné (konkrétní adresát, konkrétní povinnost)
  - Opatření obecné povahy – neadresné (nekonkrétní adresát, konkrétní povinnost)

Povinnosti vyplývající z národních potřeb

Mechanismus prověřování dodavatelského řetězce

- Cíl = stát musí mít mechanismus jak **řešit závislost na nedůvěryhodných dodavatelích** (projev národní suverenity)
- platí **pouze pro vybrané organizace v režimu vyšších povinností (a to nikoli všech)**
- **budou prověřováni dodavatelé do kritické části systému** = aktiva s hodnotou 3 a 4 (vysoká/kritická), kteří dodávají bezpečnostně významnou dodávku = má výpočetní kapacitu
- **stát prověří to, zda dodavatel není hrozbou pro bezpečnost ČR, zájmy ČR, vnitřní a veřejnou bezpečnost**
- **NÚKIB může vydat zákaz dodavatele použít nebo upozornění na riziko** (je řešitelné bezpečnostním opatřením) + **lze udělit výjimku** (např. pokud to nikdo jiný nevyrábí, ohrozilo by to službu apod.) + **přechodné lhůty**

→ **Do 1 roku od vyrozumění o označení služby jako strategické**

Zajištění dostupnosti strategicky významných služeb

- Cíl = kritické služby musíme být **schopni zajistit alespoň omezeně z České republiky**, abychom byli připraveni na mimořádné situace v zahraničí
- poskytovatel strategicky významné služby je **povinen zajistit dostupnost strategicky významné služby v nezbytném rozsahu ve stanoveném čase a kvalitě z území České republiky** + **pravidelné ověřování** schopnosti zajištění

→ **Do 1 roku od vyrozumění o označení služby jako strategické (+ 1x za 2 roky prověřovat)**

Dozor nad dodržováním zákona

Dozorový orgán – NÚKIB

Oprávnění:

- **Kontrola**
- **Nápravná opatření**
- **Zvláštní sankce**
  - Pozastavení platnosti certifikace (NÚKIB)
  - Pozastavení výkonu řídicí funkce (soud)
- **Pokuta za přestupek**
  - Odstupňováno podle režimu a povahy pochybení
  - Až 250 mil. Kč nebo 2 % z celosvětového obratu
  - GDPR – *ne bis in idem*

~~**Doplňkový režim – inspektoři**~~

! Větší důležitost prohlášení o aplikovatelnosti (self-assessment)

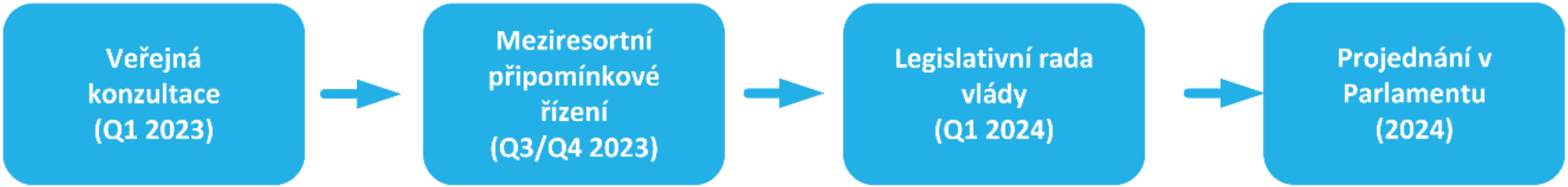
Nový zákon o kybernetické bezpečnosti

Legislativní proces

NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

nZKB – další předpokládané kroky



Vydání zákona říjen 2024 (konec transpoziční lhůty)

Vyhlášky budou mít samostatný legislativní proces,

který bude spuštěn v roce 2024

Komunikace návrhů a zapojení veřejnosti

V srpnu 2022 spuštěn **informační web věnovaný směrnici NIS2 a nové regulaci**

nis2.nukib.cz*

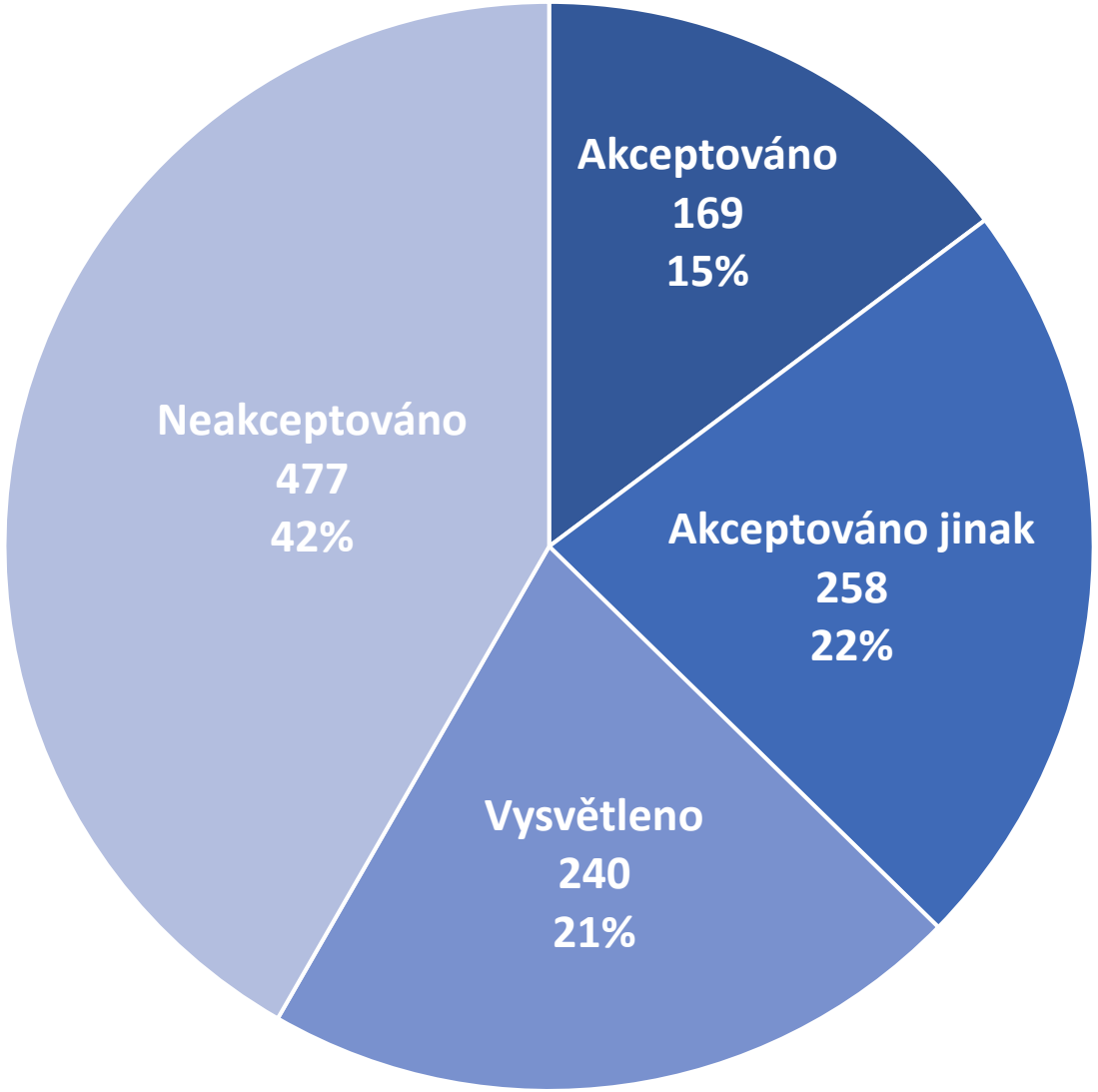
Představení problematiky na desítkách konferencí a bilaterálních jednání se zástupci úřadů a soukromého sektoru

Osloveno a komunikováno **s více než 28 svazy, oborovými sdruženími a komorami**

* na webu je přes 270 000 přístupů

Veřejné konzultace

- zahájeno 26. ledna 2023
- ukončeno 12. března 2023
- NÚKIB obdržel 1144 jedinečných podnětů (od 117 jednotlivých míst)
- zohledněno 58 % z nich
- 100 % autorů informováno o způsobu vypořádání



Veřejné konzultace – hlavní změny

- Formulační změny, zpřehlednění a zpřesnění textu
- Nastavení inspektorů → **Zrušení institutu inspektorů**
- Obsah vyhlášky o bezpečnostních opatřeních pro režim nižších povinností → **zeštíhlení, zjednodušení – do MPŘ byla následně předložena zcela přepracovaná verze**
- Lokalizace informací a dat při zpracování v zahraničí → **zcela přepracováno, nově zajištění dostupnosti strategicky významných služeb z České republiky**
- Určovací a identifikační kritéria ve vyhlášce → **Přesun určovacích kritérií, určení změny režimu do zákona a výčet odvětví pro identifikaci přímo v zákoně**
- Zákon rozdělen na dva → **hlavní zákon a změnový zákon (měnící jiné předpisy)**
- Dílčí změny v mechanismu prověřování bezpečnosti dodavatelského řetězce
- Stav kybernetického nebezpečí → **koncepční změny, provázání s krizovým řízením**

Mezirezortní připomínkové řízení

- zahájeno 19. června 2023
- ukončeno 26. července 2023
- NÚKIB obdržel vyšší stovky připomínek
  - připomínky zaslalo **41 řádných připomínkových míst**
  - dalších **11 organizací zaslalo své připomínky i bez toho, aby byli osloveni** (ale jejich připomínky byly také přijaty a řešeny)
  - Připomínky vypořádány písemně + další jednání

Nejčastější připomínkované oblasti

- legislativně-technické úpravy, obsah doprovodných materiálů, definice apod.
- mechanismus bezpečnosti dodavatelského řetězce a zajištění dostupnosti strategicky významné služby
- nastavení vztahu zákon – vyhlášky
- pravomoci Úřadu a Národního CERT
- stav kybernetického nebezpečí

MPŘ – hlavní změny

- Formulační změny, zpřehlednění a zpřesnění textu
- Změna v regulaci poskytovatelů digitálních služeb (viz dále)
- Zajištění poskytování strategicky významné služby z ČR – nově jen **v nezbytném rozsahu** (stanoví vyhláška) a **ve stanoveném čase a kvalitě** (stanoví poskytovatel)
- Registrace a evidence poskytovatele → **registrace a evidence regulované služby**
- Dílčí změny v mechanismu prověřování bezpečnosti dodavatelského řetězce – **řeší se** zapojení regulátora, životní cyklus technologií, zapojení BRS
- Stav kybernetického nebezpečí – **náhrada škody** provázána s krizovým zákonem

MPŘ – hlavní změny

Zásadní změna pro poskytovatele služeb v odvětví digitální infrastruktury

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

MPŘ – hlavní změny

Zásadní změna pro poskytovatele služeb v odvětví digitální infrastruktury

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

Významné incidenty identifikované podle pravidel prováděcího předpisu Evropské komise

Chemický průmysl

3. Výroba, produkce a distribuce chemických látek		podniky provádějící výrobu látek a distribuci látek nebo směsí ve smyslu čl. 3 bodů 9 a 14 nařízení Evropského parlamentu a Rady (ES) č. 1907/2006 ([2]) a podniky provádějící výrobu předmětů ve smyslu čl. 3 bodu 3 uvedeného nařízení z látek či směsí

([2]) Nařízení Evropského parlamentu a Rady (ES) č. 1907/2006 ze dne 18. prosince 2006 o registraci, hodnocení, povolování a omezování chemických látek (REACH), o zřízení Evropské agentury pro chemické látky, o změně směrnice 1999/45/ES a o zrušení nařízení Rady (EHS) č. 793/93, nařízení Komise (ES) č. 1488/94, směrnice Rady 76/769/EHS a směrnic Komise 91/155/EHS, 93/67/EHS, 93/105/ES a 2000/21/ES (Úř. věst. L 396, 30.12.2006, s. 1).

1. Pro účely této směrnice se za základní subjekty považují:

a) subjekty, jejichž druh je uveden v příloze I, které překračují stropy pro střední podniky stanovené v čl. 2 odst. 1 přílohy doporučení 2003/361/ES;

b) kvalifikovaní poskytovatelé služeb vytvářejících důvěru, registry domén nejvyšší úrovně a provozovatelé DNS bez ohledu na jejich velikost;

c) poskytovatelé veřejných sítí elektronických komunikací nebo veřejně dostupných služeb elektronických komunikací, kteří jsou považováni za střední podniky podle článku 2 přílohy doporučení 2003/361/ES;

d) subjekty veřejné správy podle čl. 2 odst. 2 písm. f) bodu i);

e) jakékoli jiné subjekty druhu, který je uveden v příloze I nebo II, jež členský stát označí za základní subjekty podle čl. 2 odst. 2 písm. b) až e);

f) subjekty určené jakožto kritické subjekty podle směrnice (EU) 2022/2557, jež jsou uvedeny v čl. 2 odst. 3 této směrnice;

g) pokud tak členský stát stanoví, subjekty, které tento členský stát označil před 16. lednem 2023 za provozovatele základních služeb v souladu se směrnicí (EU) 2016/1148 nebo s vnitrostátním právem.

2. Pro účely této směrnice se za důležité subjekty považují subjekty druhu uvedeného v příloze I nebo II, které nelze považovat za základní subjekty podle odstavce 1 tohoto článku. Patří k nim i subjekty, jež členské státy označily za důležité podle čl. 2 odst. 2 písm. b) až e).

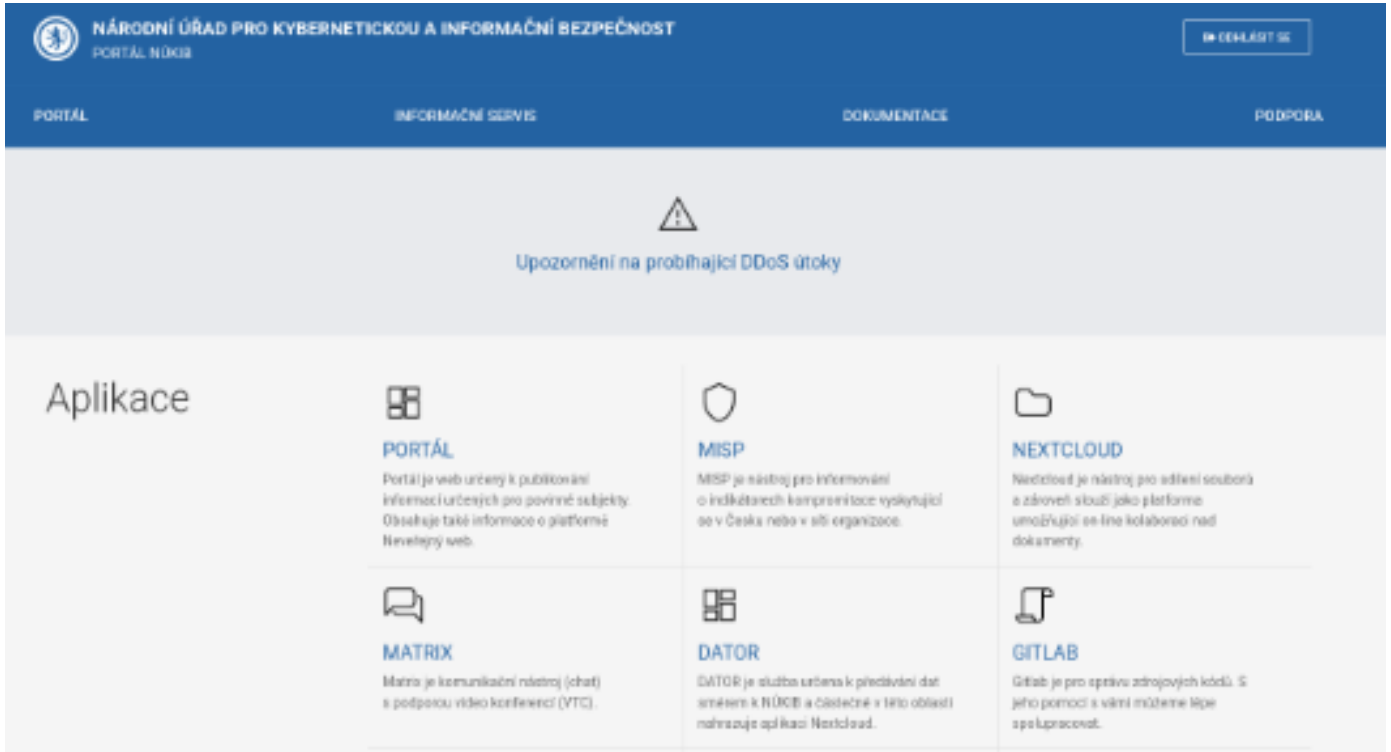
Chemický průmysl

9. Chemický průmysl

Regulovaná služba	
Služba	**Kritérium poskytovatele regulované služby a jeho režim pro tuto službu**
9.1. Výroba nebezpečných chemických látek, směsí nebo přípravků nebo látky	Výrobce nebezpečných chemických látek, směsí nebo přípravků nebo látky podle přímo použitelného předpisu Evropské unie[5] je I. poskytovatel regulované služby v režimu vyšších povinností v případě, že je provozovatelem nebo uživatelem objektu zařazeného do skupiny B podle zákona o prevenci závažných havárií, II. poskytovatel regulované služby v režimu nižších povinností v případě, že a) je velkým podnikem, b) je střední podnikem, nebo c) je provozovatelem nebo uživatelem objektu zařazeného do skupiny A podle zákona o prevenci závažných havárií.
9.2. Zpracování nebezpečných chemických látek, směsí nebo přípravků nebo látky	Zpracovatel nebezpečných chemických látek, směsí nebo přípravků nebo látky podle přímo použitelného předpisu Evropské unie[6] je I. poskytovatel regulované služby v režimu vyšších povinností v případě, že je provozovatelem nebo uživatelem objektu zařazeného do skupiny B podle zákona o prevenci závažných havárií, II. poskytovatel regulované služby v režimu nižších povinností v případě, že a) je velkým podnikem, b) je střední podnikem, nebo c) je provozovatelem nebo uživatelem objektu zařazeného do skupiny A podle zákona o prevenci závažných havárií.
9.3. Skladování nebo distribuce nebezpečných chemických látek, směsí nebo přípravků nebo látky	Distributor nebo osoba skladující nebezpečné chemické látky, směsi nebo přípravky nebo látky podle přímo použitelného předpisu Evropské unie[7] je I. poskytovatel regulované služby v režimu vyšších povinností v případě, že je provozovatelem nebo uživatelem objektu zařazeného do skupiny B podle zákona o prevenci závažných havárií, II. poskytovatel regulované služby v režimu nižších povinností v případě, že a) je velkým podnikem, b) je střední podnikem, nebo c) je provozovatelem nebo uživatelem objektu zařazeného do skupiny A podle zákona o prevenci závažných havárií.
9.4. Výroba předmětů uvedených v čl. 3 bodě 3 přímo použitelného předpisu Evropské unie[8] z látek nebo směsí	Výrobce předmětů podle přímo použitelného předpisu Evropské unie[9] z látek nebo směsí je I. poskytovatel regulované služby v režimu vyšších povinností v případě, že je provozovatelem nebo uživatelem objektu zařazeného do skupiny B podle zákona o prevenci závažných havárií, II. poskytovatel regulované služby v režimu nižších povinností v případě, že a) je velkým podnikem, b) je střední podnikem, nebo c) je provozovatelem nebo uživatelem objektu zařazeného do skupiny A podle zákona o prevenci závažných havárií.

Portál NÚKIB

- Připravujeme tzv. Portál NÚKIB
- Portál bude rozhraní sloužící administraci povinností, poskytování služeb a sdílení informací
  - Registrace organizace
  - Hlášení kontaktních údajů
  - Hlášení incidentů
  - Další hlášení (provádění opatření apod.)
  - Přístup k registru zranitelností
- Provázáno s vyhláškou o Portálu NÚKIB
- Vystavěn na platformě Neveřejného webu
- Tvoříme interním vývojem



Návrh zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti

NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

Zákon o bankách

- prolamuje bankovní tajemství, § 29 odst. 6 návrhu ZKB

Zákon o poštovních službách

- poskytovatelé poštovních služeb mají nově podléhat směrnici NIS 2
- vymezení kompetencí mezi ČTÚ a NÚKIB
- díky navrhované změně by nemělo docházet k duplicitnímu hlášení bezpečnostních incidentů

Zákon o informačních systémech veřejné správy

- zrušení bezpečnostních pravidel (nZKB nestanoví pro OVM povinnost zajistit dodržování bezpečnostních pravidel pro OVM využívající služby cloud computingu, zařadit poptávaný cloud computing do bezpečnostní úrovně před uzavřením smlouvy s poskytovatelem cloud computingu) - nutné přidat do ZoISVS

Zákon o elektronických komunikacích

- ČTÚ identifikovalo problém, že nemá v současné době procesní nástroj, jak změnit nebo zrušit regulační opatření, které uložilo rozhodnutím a kterým například přidělilo rádiové kmitočty

- Dále pak došlo k vyjasnění vztahu tohoto zákona a nZKB.
  - Podnikatelé zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací spadnou jak pod tuto regulaci, pak pod nZKB. Úprava má za cíl, aby se povinnosti nedublovali.

Zákon o provádění mezinárodních sankcí

- prolomení mlčenlivosti Finančního analytického úřadu, § 29 odst. 5 písm. b) návrhu ZKB

Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu

- prolomení mlčenlivosti Finančního analytického úřadu, § 29 odst. 5 písm. b) návrhu ZKB

Zákon o Policii České republiky

- prolomení mlčenlivosti Finančního analytického úřadu, § 29 odst. 5 písm. a) návrhu ZKB

Daňový řád

- prolomení mlčenlivosti správce daně podle daňového řádu, § 29 odst. 5 písm. c) návrhu ZKB

Zákon o Celní správě České republiky

- prolomení mlčenlivosti orgánu Celní správy České republiky, § 29 odst. 5 písm. d) návrhu ZKB

Zákon o prověřování zahraničních investic

- změna spočívá ve stanovení jediné povinné osoby - poskytovatele regulované služby (nyní vyjmenovány stávající povinné osoby dle ZKB)

Závěr

NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

Dopady na dosud regulované subjekty

- Primárně v režimu vyšších povinností
- Dílčí změny v dosavadním fungování
- Rozsah ISMS – rozšíření podle služeb, defaultní rozsah celá organizace
  - Bezpečnostní opatření – víceméně shodná
  - Hlášení incidentů – principiálně shodné
  - Způsob určení – primárně samoidentifikace
  - Sankce – významně vyšší (+ 2 nové)
  - Komunikace s NÚKIB – speciální IS

… kde začít?

Analýza stávajícího stavu

- **Zmapováním aktuálního stavu organizace**
- Vypracování **business impact analýzy** (z pohledu narušení důvěrnosti, dostupnosti a integrity).

Stanovení výběru konkrétních bezpečnostních opatření

- **Nutno zohlednit specifika organizace a důležitost jednotlivých systémů a služeb**
- Není smyslem zavádět nesmyslná a nákladná řešení tam, kde to pro vaši organizaci nemá význam.

Stanovení jednotlivých priorit a bezpečnostních projektů

- **Analýza rizik**
- **Školení relevantních osob**
- Řešení největších problémů
- Stanovení plánu od budoucna
- Technická opatření – typicky **firewally**, **antiviry** a **zálohovací řešení.**

V případě nejasností – zeptejte se NÚKIB

Děkuji za pozornost.

Nis2.nukib.cz

regulace@nukib.cz