Kybernetická bezpečnost obcí

v kontextu směrnice NIS2

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

4. dubna 2023

TLP: CLEAR

Daniela Procházková
oddělení regulace veřejného sektoru

Disclaimer

- Směrnice NIS2 byla dne 27. prosince 2022 zveřejněna v Úředním věstníku Evropské unie. Publikovaná podoba směrnice NIS2 je oficiální a nebude se již dále měnit.
- Informace v této prezentaci vycházejí z finálního znění směrnice.
- Prezentované informace týkající se budoucí úpravy právních předpisů České republiky v závislosti na obsahu směrnice NIS2 mohou obsahovat názory a plány NÚKIB jako gestora této problematiky.
- Prezentace má informační a osvětových charakter a vychází z aktuálního stavu poznání.

Co potřebujeme vědět na začátku

- Směrnice obecně je legislativní akt Evropské unie, který není sám o sobě aplikovatelný **(= musí nejdříve vzniknout národní úprava)**
- Kybernetická bezpečnost v České republice **je již nyní regulována** (= je z čeho vycházet)
- Základem změn je nově přicházející **směrnice NIS2** (= viz dále), ale také potřeba zákon o kybernetické bezpečnosti aktualizovat
- Národní úřad pro kybernetickou a informační bezpečnost **připravil návrh nového zákona o kybernetické bezpečnosti** (= byl zveřejněn k připomínkám)
- NÚKIB nemůže „podkročit“ směrnici NIS2.
- Předpisy z návrhů se **budou** měnit – zveřejnili jsme je ke konzultaci, proto nyní zapracováváme vstupy a ještě tyto návrhy čeká MPŘ
  - K informacím o změnách se dostanete – NÚKIB je bude komunikovat na webu k NIS2 a poskytne rád i jejich výklad

*zpravidla

Web NÚKIB k směrnici NIS2

- Spuštěn web – dostupný zde: nis2.nukib.cz

Stav směrnice NIS2

- Směrnice byla publikována 27. prosince 2022
- Gestor problematiky (předkladatel návrhu transpozičního zákona) = NÚKIB
- **Transpozice, tj. provedení obsahu směrnice do českého práva je potřeba provést do 17. října 2024 – nová pravidla budou platná.**

=> Návrh odejde do legislativního procesu (LRV, MPŘ, Parlament…) v polovině 2023

Nová směrnice NIS2

Směrnice NIS2 navazuje na obsah směrnice NIS1 přijaté v roce 2016 a poprvé zavádí povinnou regulaci veřejné správy ze strany členských států.

ČR měla již existující úpravu kybernetické bezpečnosti veřejné správy.

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.

Návrh nového zákona o kybernetické bezpečnosti

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

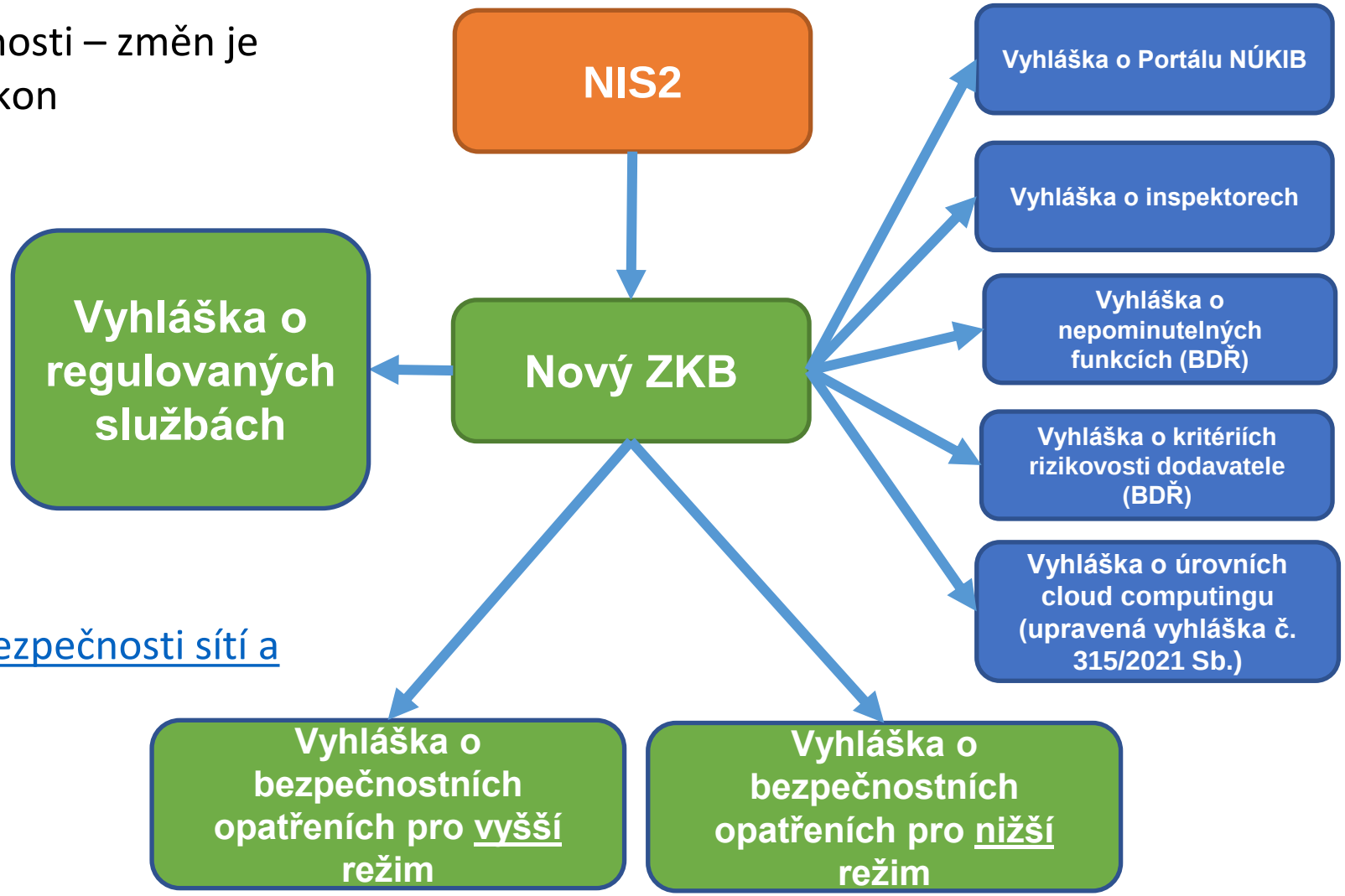
Nový zákon o kybernetické bezpečnosti (NZKB)

Nový zákon o kybernetické bezpečnosti – změn je tolik, že bylo třeba vytvořit nový zákon

zcela nová úprava – cca 60 paragrafů

Zveřejněný návrh má aktuálně navíc 8 vyhlášek

Celý návrh zveřejněn zde: Course: Nová směrnice EU o bezpečnosti sítí a informací (nukib.cz)



NZKB – povinné osoby

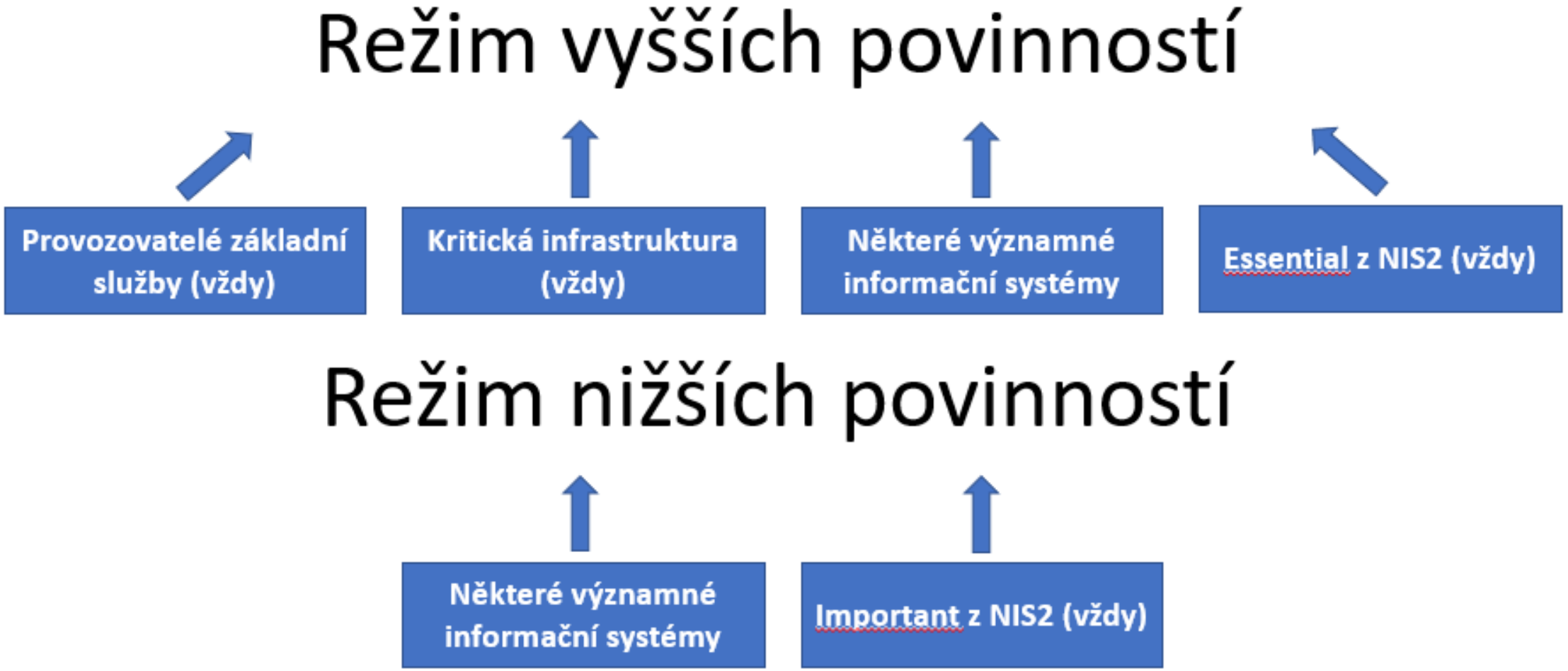
- **Poskytovatel regulované služby**
  - Jediná povinná osoba
  - Jedno IČO = jedna povinná osoba
  - **Poskytuje regulovanou službu = služba splňující kritéria stanovená vyhláškou o regulovaných službách**
  - **Primárně se orientuje na velikost podniku – (Střední a velký tzn. 50 zaměstnanců, obrat 10 mil. EUR)**
- **Režim poskytovatele regulované služby – vyhláška o regulovaných službách**
  - Stanovuje míru povinností – vyšší režim / nižší režim
  - Ke každému režimu bude vyhláška, která bude definovat povinnosti
- **Pokud bude jeden subjekt poskytovat služby v různých režimech – přednost má vyšší režim na všechny služby (tedy služby, které by byly v nižším režimu budou povýšeny do vyššího)**
- **Naplnění kritérií je povinen hlásit poskytovatel služby = každý si musí vyhodnotit kritéria sám**
  - Do 30 dnů od doby, kdy naplnění zjistí, nejpozději do 90 kdy k naplnění došlo
- **V případě naplnění kritérií se zaregistruje u NÚKIB**
- **NÚKIB muže zaregistrovat i sám dozví-li se o naplnění kritérií**

NZKB – povinné osoby

Jedna jediná povinná osoba*:

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

NZKB – povinné osoby



Poskytovatel regulované služby ve veřejné správě

Regulovaná služba	
Služba	Kritérium poskytovatele regulované služby
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) správním úřadem s celostátní působností, 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) Kanceláří Veřejného ochránce práv, g) Českou národní bankou, h) Nejvyšším kontrolním úřadem, i) Policejním prezidiem, j) útvarem policie s celostátní působností, k) orgánem soudní moci, l) státním zastupitelstvím, m) zdravotní pojišťovnou, n) krajem, o) hlavním městem Praha, nebo p) 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, c) vysokou školou, d) Akademií věd České republiky, nebo e) obcí s rozšířenou působností s počtem obyvatel do 125 000.

Poskytovatel regulované služby

10. Vodní hospodářství

Regulovaná služba	
Služba	Kritérium poskytovatele regulované služby
10.1. Provozování vodovodu	Provozovatel vodovodu podle zákona o vodovodech a kanalizacích je I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že a) je velkým podnikem, nebo b) zásobuje pitnou vodou alespoň 50 000 obyvatel, II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je středním podnikem.
10.2. Provozování kanalizace	Provozovatel kanalizace podle zákona o vodovodech a kanalizacích je I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že a) je velkým podnikem, nebo b) poskytuje služby odvádění nebo čištění odpadních vod alespoň 50 000 obyvatelům, II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je středním podnikem.

18. Zdravotnictví

Regulovaná služba	
Služba	Kritérium poskytovatele regulované služby
18.1. Poskytování zdravotní péče	Poskytovatel zdravotní péče podle zákona o zdravotních službách je I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že a) je velkým podnikem, b) disponuje počtem lůžek akutní péče nejméně 270, II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je středním podnikem.

11. Odpadové hospodářství

Regulovaná služba	
Služba	Kritérium poskytovatele regulované služby
11.1. Provoz zařízení určeného pro nakládání s odpady	Provozovatel zařízení určeného pro nakládání s odpady podle zákona o odpadech, který je středním nebo velkým podnikem, je poskytovatel regulované služby v režimu nižších povinností.
11.2. Obchodování s odpadem	Obchodník s odpady podle zákona o odpadech, který je středním nebo velkým podnikem, je poskytovatel regulované služby v režimu nižších povinností.
11.3. Zprostředkování nakládání s odpadem	Zprostředkovatel nakládání s odpady podle zákona o odpadech, který je středním nebo velkým podnikem, je poskytovatel regulované služby v režimu nižších povinností.
11.4. Přeprava odpadu	Dopravce odpadu podle zákona o odpadech, který je středním nebo velkým podnikem, je poskytovatel regulované služby v režimu nižších povinností.

NZKB – povinnosti poskytovatelů regulované služby

Hlášení údajů

- Registrační údaje – info o organizaci
- Kontaktní údaje – info o zástupci, měl by být zastupitelný
- Doplňující údaje – IP rozsahy a další
- Potřeba hlásit i změny (těch údajů, které nelze dohledat v rejstřících)
- Náležitosti – vyhláška o Portálu NÚKIB

Stanovení rozsahu řízení bezpečnosti

- Identifikace primárních aktiv v rámci celé organizace
- Určí, která primární aktiva souvisí s poskytováním regulované služby
- Určí organizační části a podpůrná aktiva, která souvisí s poskytováním regulované služby
- **Ta aktiva a organizační části, která takto určí spadají do rozsahu regulace**
- Dokud/pokud to neudělá = rozsah celá organizace

NZKB – povinnosti PRS

Bezpečnostní opatření

- Zavádí se v rámci stanoveného rozsahu
- Začínají se plnit nejpozději do jednoho roku od registrace služby
- V rámci vyššího/nižšího režimu:

organizační opatření – **vyšší** režim

1. systém řízení bezpečnosti informací,
2. povinnosti pro vrcholné 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.

organizační opatření – **nižší** režim

1. zajišťování minimální úrovně kybernetické bezpečnosti,
2. povinnosti vrcholného vedení
3. bezpečnostní role
4. bezpečnostní politika a dokumentace,
5. řízení aktiv,
6. řízení dodavatelů,
7. bezpečnost lidských zdrojů,
8. řízení změn, akvizice, vývoje a údržby,
9. řízení přístupů,
10. zvládání kybernetických bezpečnostních událostí a incidentů,
11. řízení kontinuity činností.

technická opatření – vyšší režim (nižší režim mimo tučně vyznačené)

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 obdobných specifických aktiv.

NZKB – povinnosti PRS – hlášení incidentů

Režim vyšších povinností	Režim nižších povinností
Hlásí vše (s původem v kybernetickém prostoru)	**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)

… kde začít?

- Při stanovení úrovně zabezpečení a výběru konkrétních bezpečnostních opatření je potřeba v souladu se zákonem a vyhláškami **zohlednit specifika organizace a důležitost jednotlivých systémů a služeb** (není smyslem zavádět nesmyslná a nákladná řešení tam, kde to pro vaši organizaci nemá význam).
- Pokud vaše organizace kybernetickou bezpečnost do této chvíle systematicky neřešila, lze doporučit jako výchozí krok především **zmapováním aktuálního stavu organizace** (tzn. audit aktuálního stavu kybernetické bezpečnosti a potenciálních slabých míst) a vypracováním **business impact analýzy** (zejm. jaké by byly dopady narušení řádného fungování jednotlivých systémů na vaši organizaci; nejde přitom jen o nedostupnost používaných informačních systémů, ale i o narušení důvěrnosti nebo integrity shromažďovaných dat).
- Již v této fázi je dobré se zaměřit na **školení relevantních osob** v organizaci – základní školení pro všechny uživatele, odborné školení pro osoby, které v organizaci řeší/budou řešit kybernetickou bezpečnost, nezapomínat přitom i na vrcholný management (management si musí být vědom důležitosti řízení kybernetické bezpečnosti v organizaci).
- **Rozhodně nedoporučujeme nakupovat služby typu „posoudíme soulad vaší organizace s NIS2“ nebo „zavedeme vám v organizaci NIS2“. Nenechte se napálit „vševědoucími“ implementátory NIS2 na klíč.** Směrnice NIS2 žádné konkrétní požadavky neupravuje, vše bude obsaženo až v novém zákoně o kybernetické bezpečnosti, který je teprve připravován a bude platit až od poloviny roku 2024 a bude mít implementační lhůtu 1 rok.
- Z technických opatření lze obecně doporučit nasadit **firewally** (zejména perimetrové), **antiviry** (zejména sofistikovanější EDR), a **zálohovací řešení.** Společně s prováděním **aktualizací** (tam kde je to možné) se jedná o věci, které by měly být dávno běžnou součástí chodu každé organizace a výše zmiňovanou osvětu a školení.

Děkuji za pozornost

Dotazy k návrhům nových předpisů je možné zasílat na:

regulace@nukib.cz