Nový zákon o kybernetické bezpečnosti:

Dopad regulace na obce

NÚKIB

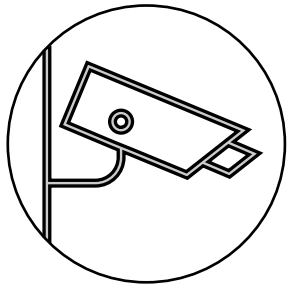
Národní úřad
pro kybernetickou
a informační
bezpečnost

Daniela Procházková
vedoucí
oddělení regulace veřejného sektoru
Adam Kučínský
Ředitel
odboru regulace

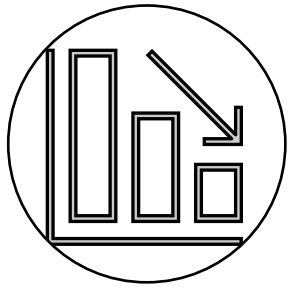
19. března 2024
TLP: CLEAR

Příklady dopadů incidentů na obce dle rozboru NÚKIB

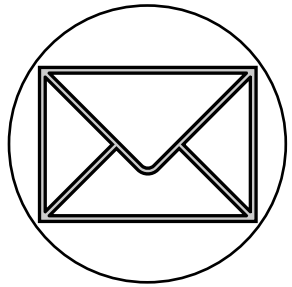
- NÚKIB v letech 2020-2023 eviduje **27 incidentů nahlášených obcemi**
- Dobrovolná hlášení = nekompletní
- Detekce?



Nedostupnost monitorovacího software na jednotky hodin kvůli reinstalaci serveru



Zařazení veřejné IP adresy obce na blacklisty = **poškození reputace obce**

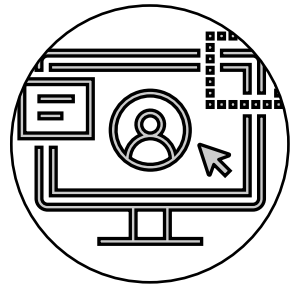


Nedostupnost e-mailových služeb

Potenciální či potvrzená **exfiltrace dat útočníkem**

(potenciální ohrožení zájmů ČR)

Zašifrování dat spojené s nedostupností dat (nedostupnost služeb pro občany)



Nefunkčnost webových stránek obce

Nový zákon o kybernetické bezpečnosti

NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

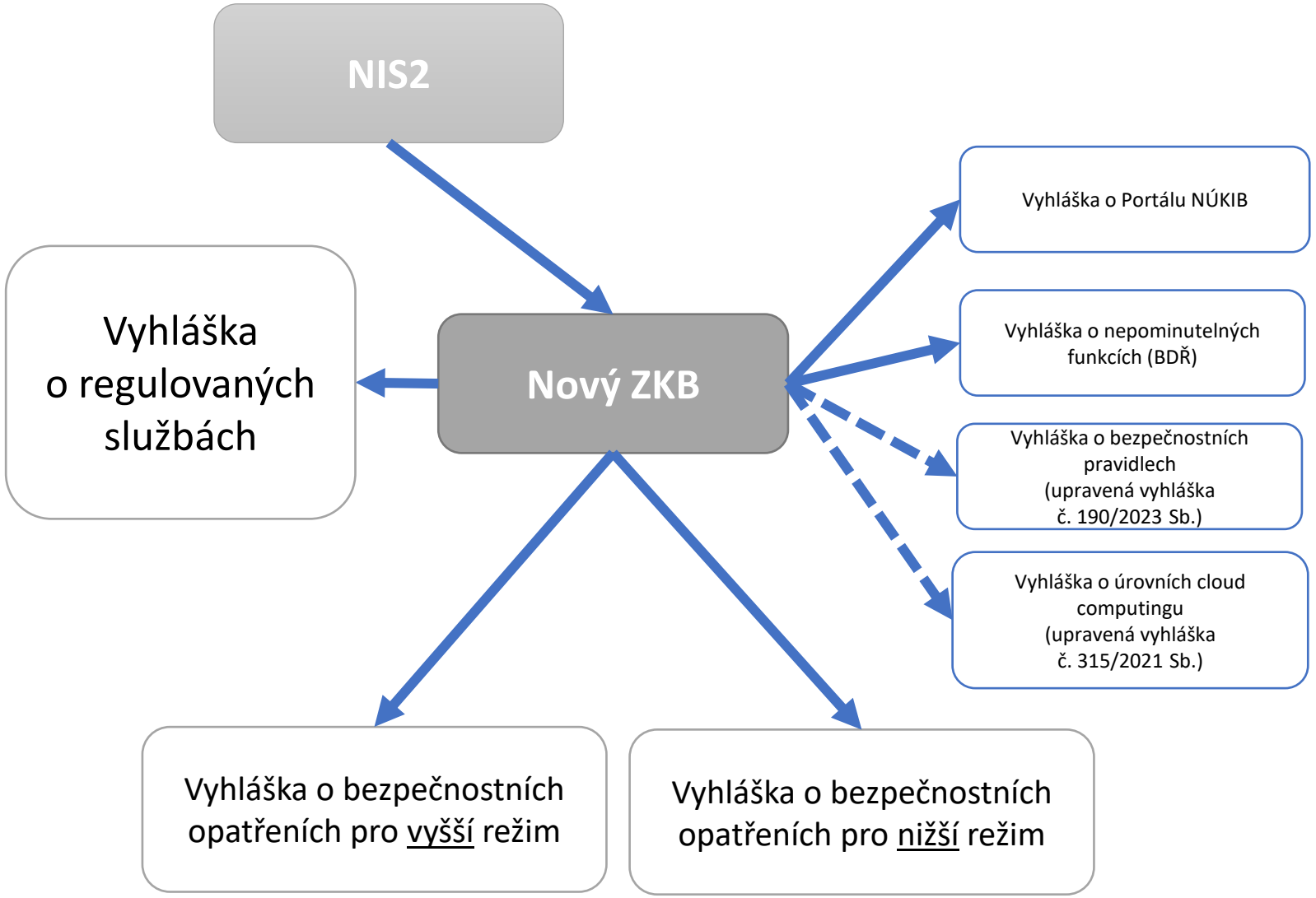
Nový zákon o kybernetické bezpečnosti (nZKB)

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

= zcela nová úprava – 74 paragrafů

Verze v mez. připomínkovém řízení má aktuálně navíc **7 vyhlášek**

Celý návrh zveřejněn na webu **nis2.nukib.cz**



Legislativní proces: stav

Mezirezortní připomínkové řízení (MPŘ) – skončeno

Legislativní rada vlády – prosinec 2023 – duben 2024 (Jednání „velké“ LRV – 4. dubna 2024)

Poslanecká sněmovna, Senát, prezident – Q2 2024

Vydání zákona – leden 2025 (transpoziční lhůta je stanovena na říjen)

Vyhlášky budou mít samostatný legislativní proces, který bude spuštěn v Q2/Q3 2024

Vyhláška o regulovaných službách

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 j) Generálním ředitelstvím hasičského záchranného sboru, k) krajským ředitelstvím hasičského záchranného sboru, l) Kanceláří Veřejného ochránce práv, m) 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. 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, f) městským obvodem nebo městskou částí, která vykonává rozšířenou působnost.

Vyhláška o regulovaných službách

	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, f) městským obvodem nebo městskou částí, která vykonává rozšířenou působnost.

Vyhláška o regulovaných službách

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,

Vymezení rozsahu řízení bezpečnosti informací: výkon svěřených pravomocí

Přenesená působnost obcí

- Evidence obyvatel
- Matrika
- Vidimace a legalizace
- Poskytování informace
- Stavební a silniční správní úřad
- Dopravní agenda
- Životní prostředí
- Přestupky
- Místní poplatky
- Právo shromažďování
- Sociální agenda
- Krizové řízení

Samostatná působnost obcí

- Správa vlastního majetku
- Místní referenda
- Vyřizování petic a stížností
- Poskytování dotací
- Odpadové hospodářství
- Poskytování informací
- Zřizování příspěvkových organizací a obecní policie
- Vydávání obecně závazných vyhlášek

Vymezení rozsahu řízení bezpečnosti informací: obce

- Obce často vykonávají agendy v přenesené působnosti prostřednictvím přístupu do systémů řízených centrálně -> za jejich zajištění by měl být zodpovědný ÚOSS
- **Obce by měly zabezpečovat ty systémy, kterými disponují -> užší rozsah aktiv, na která budou zaváděna opatření**

Systémy typicky spravované obcemi

Spisová služba | Elektronická pošta | Úřední deska | Ekonomický systém

Základní povinnosti obce s rozšířenou působností

Registrace

- Zákon o kybernetické bezpečnosti
- Registrace obce a nahlášení kontaktní osoby
- Portál NÚKIB
- 30 dní od zjištění, 90 dní od naplnění kritérií

Bezpečnostní opatření

- Vyhláška o bezpečnostních opatřeních – nižší režim
- 13 kategorií opatření, 4 povinná
- 1 rok od vyrozumění o zařazení do evidence

Hlášení incidentů

- Vyhláška o bezpečnostních opatřeních – nižší režim
- Významné incidenty
- 1 rok od vyrozumění o zařazení o evidence

Provedení protiopatření

- Vydá a doručí NÚKIB
- Reaktivní protiopatření
- Lhůty dané protiopatřením

Zavádění bezpečnosti na obci

NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

Jak přistoupit k zavádění bezpečnosti?

Přehled v organizaci

- Jaké vykonávám agendy a poskytuji služby?
- Co pro výkon těchto agend potřebuji?
- Z toho vyplývá rozsah, ve kterém KB řeším.

Aktuální stav KB

- Mám již zavedena některá opatření?
- Zdokumentuji aktuální stav zavedených a nezavedených opatření.

Určení priorit

- Jaké mám finanční a personální kapacity?
- Co je má prioritní služba?
- Stanovím plán zavádění bezpečnostních opatření, odůvodním případné nezavedení nepovinných.

Zavádění opatření

- Určím osobu odpovědnou za KB.
- Priorita je vzdělávání zaměstnanců včetně vedení.
- Vytvořím bezpečnostní politiku, kterou lze fakticky používat.
- Pokračuji dle plánu.

Zásada přiměřenosti:

- Náklady na zaváděné opatření by neměly převyšovat náklady na případnou realizaci kybernetického incidentu.
- Nechci všechno najednou, postupně se zlepšuji.

Praktická použitelnost:

- Šablonovitá dokumentace nikdy nebude používaná a nebude sedět mé organizaci
- Příliš složitý systém nebudu mít kapacitu udržovat

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. Zajišťování kybernetické bezpečnosti
2. povinnosti vrcholového 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

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.

Vyhláška pro režim nižších povinností – **povinná ustanovení**

- **§ 4 Zajišťování kybernetické bezpečnosti:**
  - Princip přiměřenosti (zavádí se přiměřená opatření se zohledněním bezpečnostních potřeb organizace)
  - Ústřední dokument: **Přehled bezpečnostních opatření** (zavedená/nezavedená/kdy budou zavedená + odůvodnění proč nebyla zavedena)
    - S dokumentem seznamuje vrcholové vedení
  - **Určení osoby zodpovědné za KB** (není nutné najímat nového zaměstnance)
  - **Pořízení a schválení bezpečnostní politiky**, vedení bezpečnostní dokumentace
  - **Stanovení pravidel ochrany aktiv a přípustné způsoby jejich používání**
  - Zohlednění **požadavků na dodavatele** ve smluvním vztahu (pomůže příloha vyhlášky)
  - Stanoví bezpečnostní požadavky v souvislosti s **akvizicí, vývojem a údržbou**

Vyhláška pro režim nižších povinností – **povinná ustanovení**

- **§ 5 Povinnosti vrcholového vedení:**
  - Vedení **zná své povinnosti** a odpovědnosti
  - Zajišťuje potřebné **zdroje**
  - **Seznamuje se** s plněním přehledu bezpečnostních opatření (prokazatelně)

- **§ 6 Bezpečnost lidských zdrojů**
  - Vytvoří **politiku bezpečného chování uživatelů** (pomůže příloha č. 4 vyhlášky)
  - Stanoví pravidla rozvoje bezpečnostního povědomí = **školení zaměstnanců**
    - Obsahuje pravidla pro tvorbu hesel
    - Je nutné dbát i na vzdělávání administrátorů a osoby zodpovědné za KB
  - Zajistí kontrolu dodržování bezpečnostní politiky a pravidla a postupy pro řešení porušení

Vyhláška pro režim nižších povinností – **povinná ustanovení**

- **§ 11 Řešení kybernetických bezpečnostních incidentů**
  - Zavede postupy pro **oznamování podezření na incidenty/události**
  - **Metodika pro posuzování incidentů** a událostí + posouzení těch **významných**, které jsou hlášeny
  - Zajistit **řešení incidentů**
  - Hlásí významné incidenty v souladu se ZKB

Kde najít další informace?

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

nis2.nukib.cz

Děkuji za pozornost.

nis2.nukib.cz

regulace@nukib.cz