

# Obce a kyberbezpečnost

Konference ISSS, Hradec Králové

NÚKIB



Národní úřad  
pro kybernetickou  
a informační  
bezpečnost

**Daniela Procházková**  
oddělení regulace veřejného sektoru

13.05.2025



### **UPOZORNĚNÍ:**

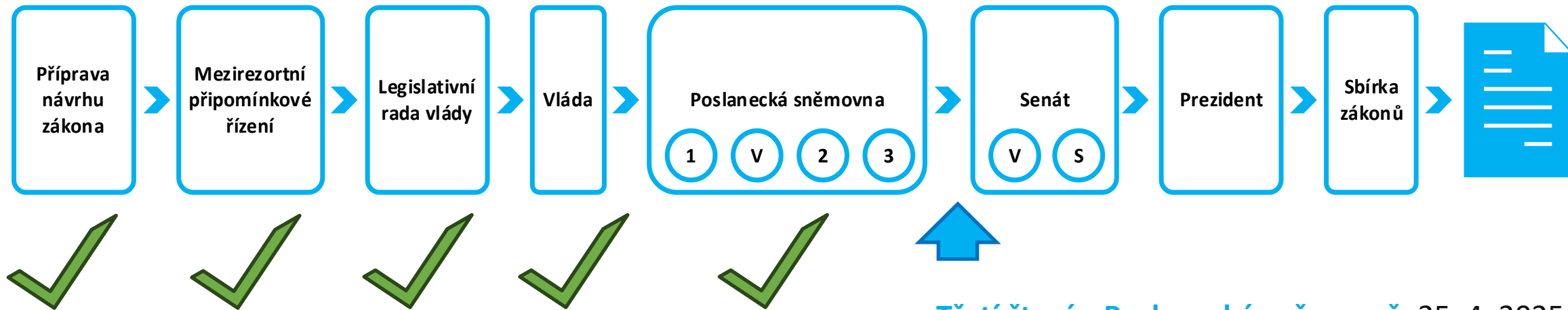
Transpozice NIS2 do českého právního řádu není finalizována.  
Informace obsažené v této prezentaci se mohou změnit v rámci legislativního procesu.

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

# Stav legislativního procesu

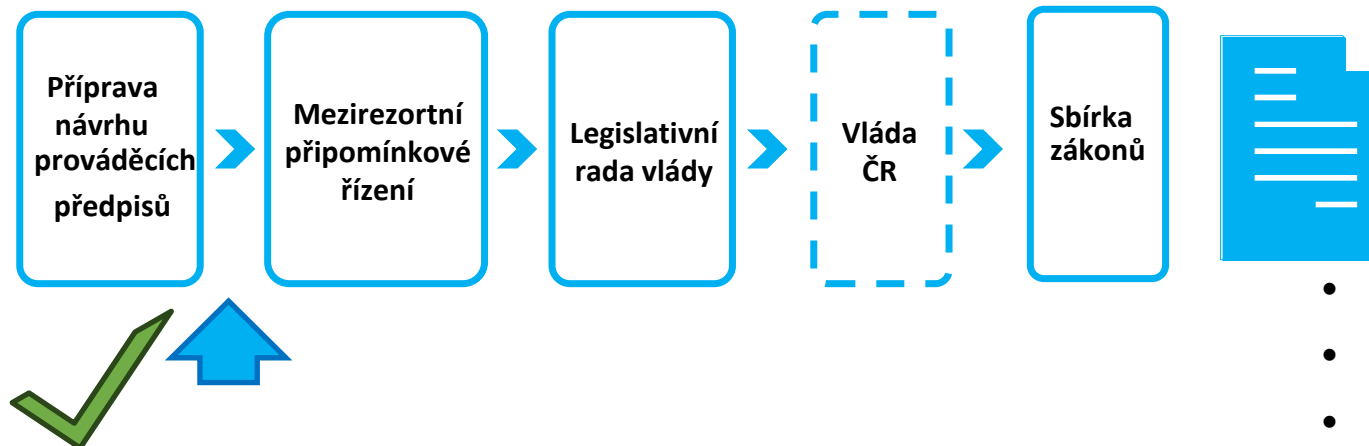


nZKB



- **Třetí čtení v Poslanecké sněmovně:** 25. 4. 2025
- **Senátu doručeno:** tento týden
- **Účinnost:** Q3 2025

Prováděcí předpisy

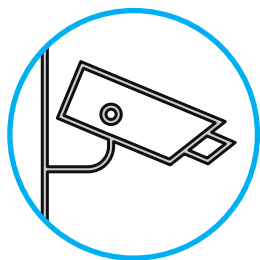


- **Spuštění MPŘ:** v řádu jednotek týdnů
- **Lhůta na připomínky:** 15 dní
- **Účinnost:** Q3 2025 (souběžně se ZKB)

# Příklady dopadů incidentů cílených na obce



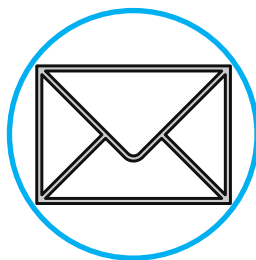
- NÚKIB v letech 2020-2023 evidoval **27 incidentů nahlášených obcemi**
- Dobrovolná hlášení = nekompletní; detekce
- **Kybernetická kriminalita** se v roce 2025 stane 3. největší ekonomikou světa
- Dle zprávy Izraelské INCD mohou základní opatření snížit šance na útok o 30–50 %



**Nedostupnost monitorovacích o 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**



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



**Nefunkčnost webových stránek obce**

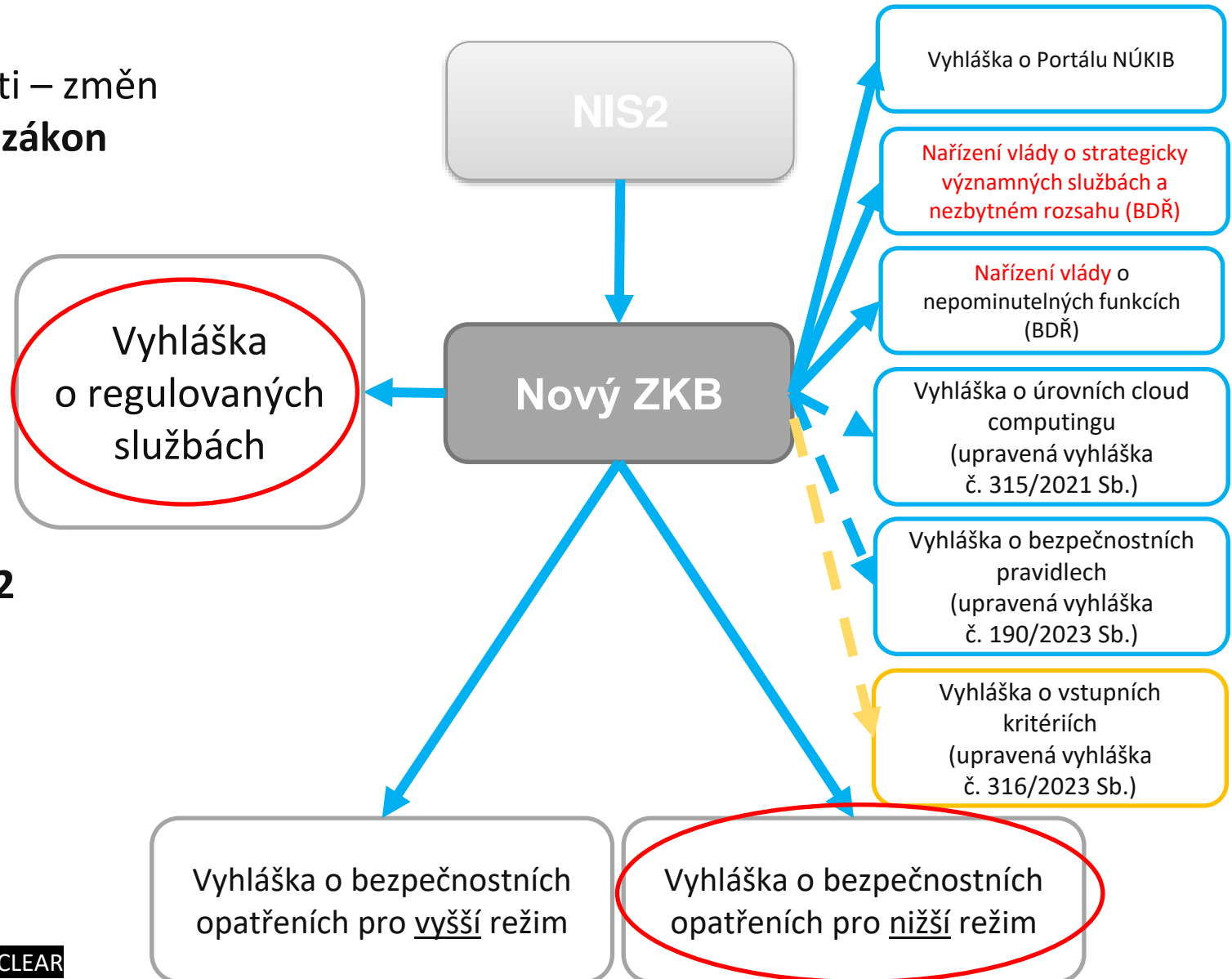
# Nový zákon o kybernetické bezpečnosti



Nový zákon o kybernetické bezpečnosti – změna je tolik, že bylo **potřeba vytvořit nový zákon**  
= zcela nová úprava – 73 paragrafů

Po průchodu poslaneckou sněmovnou jde o **8 vyhlášek a nařízení vlády**.

Reálně se ale bude upravovat ještě jedna vyhláška navíc, ale ne kvůli NIS2 (č.316/2023)



# 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 | <p>Orgán nebo osoba je</p> <p>I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že je</p> <ul style="list-style-type: none"><li>a) ústředním orgánem státní správy,</li><li>b) jiným správním úřadem s celostátní působností neuvedeným v písm. a), a to včetně ústředí a generálního ředitelství územně <u>dekoncentrovaných</u> (specializovaných) orgánů státní správy,</li><li>c) Kanceláří prezidenta republiky,</li><li>d) Kanceláří Senátu,</li><li>e) Kanceláří Poslanecké sněmovny,</li><li>f) Českou národní bankou,</li><li>g) Policejním prezidiem,</li><li>h) útvarům policie s celostátní působností,</li><li>i) Generální inspekcí bezpečnostních sborů</li><li>j) Generálním ředitelstvím hasičského záchranného sboru,</li><li>k) krajským ředitelstvím hasičského záchranného sboru,</li><li>l) Kanceláří Veřejného ochránce práv,</li><li>m) Nejvyšším kontrolním úřadem,</li><li>n) Úřadem pro zastupování státu ve věcech majetkových</li><li>o) Správou úložišť radioaktivních odpadů,</li><li>p) orgánem soudní moci,</li><li>q) státním zastupitelstvím,</li><li>r) zdravotní pojišťovnou,</li><li>s) krajem, nebo</li><li>t) hlavním městem Praha.</li></ul> <p>II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je</p> <ul style="list-style-type: none"><li>a) územně <u>dekoncentrovaným</u> (specializovaným) orgánem státní správy,</li><li>b) profesní komorou<sup>2</sup>,</li><li>c) vysokou školou,</li><li>d) Akademií věd České republiky, nebo</li><li>e) obcí s rozšířenou působností,</li><li>f) městským obvodem nebo městskou částí, která vykonává rozšířenou působnost.</li></ul> |



II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je

- a) územně dekoncentrovaným (specializovaným) orgánem státní správy,
- b) profesní komorou<sup>3</sup>,
- c) vysokou školou,
- d) Akademií věd České republiky, nebo
- e) obcí s rozšířenou působností,
- f) městským obvodem nebo městskou částí, která vykonává rozšířenou působnost.

## 1. Veřejná správa

| Regulovaná služba              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Služba                         | Kritérium poskytovatele regulované služby a jeho režim pro tuto službu                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 1.1. Výkon svěřených pravomocí | <p>Orgán nebo osoba je</p> <p>I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že je</p> <p>a) ústředním orgánem státní správy,</p> <p>b) jiným správním úřadem s celostátní působností neuvedeným v písm. a), a to včetně ústředí a generálního ředitelství územně <u>dekoncentrovaných</u> (specializovaných) orgánů státní správy,</p> <p>c) Kanceláří prezidenta republiky,</p> <p>d) Kanceláří Senátu,</p> <p>e) Kanceláří Poslanecké sněmovny,</p> <p>f) Českou národní bankou,</p> <p>g) Policejním prezidiem,</p> <p>h) útvarům policie s celostátní působností,</p> <p>i) Generální inspekcí bezpečnostních sborů</p> <p>j) Generálním ředitelstvím hasičského záchranného sboru,</p> <p>k) krajským ředitelstvím hasičského záchranného sboru,</p> <p>l) Kanceláří Veřejného ochránce práv,</p> <p>m) Nejvyšším kontrolním úřadem,</p> <p>n) Úřadem pro zastupování státu ve věcech majetkových</p> <p>o) Správou úložišť radioaktivních odpadů,</p> <p>p) orgánem soudní moci,</p> <p>q) státním zastupitelstvím,</p> <p>r) zdravotní pojišťovnou,</p> <p>s) krajem, nebo</p> <p>t) hlavním městem Praha.</p> <p>II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je</p> <p>a) územně <u>dekoncentrovaným</u> (specializovaným) orgánem státní správy,</p> <p>b) profesní komorou<sup>2</sup>,</p> <p>c) vysokou školou,</p> <p>d) Akademií věd České republiky, nebo</p> <p>e) obcí s rozšířenou působností,</p> <p>f) městským obvodem nebo městskou částí, která vykonává rozšířenou působnost.</p> |

## Obcí zřizované organizace:

- **Nespadají automaticky „protože obec“**
  - **Typicky tedy ne základní a mateřské školy či městské knihovny**
- **Spadají jen ty zřizované organizace, které samy naplní kritéria v jiném odvětví**
  - **Obce se ale k nim v rámci počítání velikosti podniků nepřiřítávají**
  - *Příklad: Do počtu zaměstnanců pro posouzení velikosti podniku např. vodárny, která je zřízena obcí, ale má samostatné IČO, se počet zaměstnanců obce nepřiřítává.*

## 1. Veřejná správa

| Regulovaná služba              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Služba                         | Kritérium poskytovatele regulované služby a jeho režim pro tuto službu                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 1.1. Výkon svěřených pravomocí | <p>Orgán nebo osoba je</p> <p>I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že je</p> <p>a) ústředním orgánem státní správy,</p> <p>b) jiným správním úřadem s celostátní působností neuvedeným v písm. a), a to včetně ústředí a generálního ředitelství územně <u>dekoncentrovaných</u> (specializovaných) orgánů státní správy,</p> <p>c) Kanceláří prezidenta republiky,</p> <p>d) Kanceláří Senátu,</p> <p>e) Kanceláří Poslanecké sněmovny,</p> <p>f) Českou národní bankou,</p> |

## 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



## 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 opatření nižší režim

1 rok od doručení  
rozhodnutí o registraci

## Hlášení incidentů

Vychází ze zákona a  
vyhlášky o  
bezpečnostních  
opatřeních

Významné incidenty –  
nižší režim

1 rok od doručení  
rozhodnutí o registraci

## Provedení protiopatření

Vydá a doručí NÚKIB

Reaktivní  
protiopatření/varování

Lhůty dané  
protiopatřením

## Režim nižších povinností

### Hlásí incidenty

které se projevily ve stanoveném rozsahu, mají původ v kybernetickém prostoru, mají významný dopad na poskytování regulované služby\* a nelze u nich ve lhůtě podle § 16 odst. 1 vyloučit úmyslné zavinění

## Národní CERT (CZ.NIC)

\*významnost stanoví sám subjekt dle postupu ve vyhlášce o bezpečnostních opatřeních pro nižší režim

## Proces hlášení a lhůty

- Do 24 hodin **od zjištění** incidentu:
  - Prvotní hlášení
- Do 72 hodin od zjištění incidentu:
  - Doplnění informací o incidentu
- Do 30 dnů od hlášení incidentu:
  - Závěrečná zpráva – jak byl incident vyřešen

# Bezpečnostní opatření – rozdíly vyšší a 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, řídicích a obdobných 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

➤ **Redukovaná bezpečnostní opatření pro nižší režim**



## NIŽŠÍ REŽIM

### § 7

#### Řízení kontinuity činností

Povinná osoba v rámci řízení kontinuity činností

- a) stanoví prioritu technických aktiv, pořadí a postupy jejich obnovy a zohlední přitom stanovenou prioritu relevantního primárního aktiva podle § 5 písm. f),
- b) stanoví dílčí odpovědnosti a povinnosti pro zajištění kontinuity činností a k obnově podle písmene a), a
- c) vytváří pravidelné zálohy informací, dat, konfigurací a nastavení technických aktiv 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

- a) stanoví metodiku pro provedení analýzy dopadů,
- b) 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,
- c) na základě výstupů analýzy dopadů a hodnocení rizik podle písmene b) stanoví cíle řízení kontinuity činností formou určení
  - i) minimální úroveň poskytovaných služeb, která je přijatelná pro užívání, provoz a správu regulované služby,
  - ii) doby obnovení chodu, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb regulované služby a
  - iii) bodu obnovení dat jako časové období, za které musí být zpětně obnovena data po kybernetickém bezpečnostním incidentu nebo po selhání,
- d) stanoví politiku řízení kontinuity činností, která obsahuje naplnění cílů podle písmene c) a stanoví práva a povinnosti administrátorů a osob zastávajících bezpečnostní role,
- e) vypracuje, aktualizuje a pravidelně testuje plány kontinuity činností a plány obnovy související s poskytováním regulované služby a
- f) realizuje bezpečnostní opatření pro zvýšení odolnosti podle § 27.

2. 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) bodu i) tohoto ustanovení.



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.

## Přehled v organizaci

- Jaké vykonávám agendy a poskytují služby?
- Co pro výkon agend potřebuji?

= rozsah, ve kterém KB řeším

## Aktuální stav KB

- Mám již některá opatření?
- = aktuální stav zavedených a nezavedených opatření

## Určení priorit

- Jaké mám finanční a personální kapacity?
- Co je má prioritní služba?

= provedu analýzu, stanovím plán

## Zavádění opatření

- Osoba zodpovědná za KB.
- Vzdělávání zaměstnanců (i vedení)
- Bezpečnostní politika

= pokračuji dle plánu

## Zásada přiměřenosti:

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

## Vzdělávání:

- E-learning zdarma od NÚKIB



## Podpůrný materiál k zavádění kybernetické bezpečnosti obcí

## FAQ k zákonu se zaměřením na ORP



### Kybernetická bezpečnost obcí

TLP: CLEAR

6. prosince 2024, verze 1.0

#### 3.4 Identifikujte aktiva nesouvisející s Výkonem svěřených pravomocí

V § 12 nového zákona o KB je také uveden postup umožňující vymezení se vůči tomu, kde obec nebude zavádět bezpečnostní opatření uvedená dále v tomto materiálu. V případě řádného odůvodnění je tak možné například uvést vybrané služby poskytované obcí, které nesouvisí s výkonem svěřených pravomocí a není tedy ani účelem zákona je mít tzv. v rozsahu.

**Takto identifikovaná primární a podpůrná aktiva určují rozsah řízení KB, ve kterém se následně zavádí bezpečnostní opatření dle vyhlášky.**

#### Obecný příklad:

|          |                  |                    |
|----------|------------------|--------------------|
| Agenda 1 | Primární aktivum | Podpůrné aktivum 1 |
| Agenda 2 |                  | Podpůrné aktivum 2 |
| Agenda 3 |                  | Podpůrné aktivum 3 |



[Úvod](#) > [Informační servis](#) > [Často kladené otázky](#) > Otázky ke kybernetické bezpečnosti obcí

## Otázky ke kybernetické bezpečnosti obcí

### Obce s rozšířenou působností

Co budou muset plnit obce s rozšířenou působností? >

Je třeba zabezpečovat úplně všechno? ▾

**Není povinné zabezpečovat úplně celou organizaci, resp. všechna její aktiva.** Zabezpečuje se vždy minimálně v rozsahu daném regulovanou službou, pro kterou organizace spadá do působnosti nového ZKB. Stanovení rozsahu řízení kybernetické bezpečnosti je povinným krokem, od kterého se odvíjí rozsah veškerých dalších povinností, pokud by nebyl rozsah stanoven, zabezpečuje se celá organizace. Podrobný návod ke stanovení rozsahu regulované služby „Výkon svěřených pravomocí“ je obsažen v materiálu [Kybernetická bezpečnost obcí](#).

Kdy je potřeba začít novou regulaci řešit? >





# Děkuji za pozornost

**Kam s dotazy?**

**Stánek č. 55 - přízemí**

**Diskuzní blok samospráv 12:50-13:05, Malý sál**

**[regulace@nukib.gov.cz](mailto:regulace@nukib.gov.cz)**

**! <https://portal.nukib.gov.cz/> !**

