# Kybernetická bezpečnost podle zákona

*Legislativa, řízení rizik, ochrana dat a postupy hlášení kybernetických bezpečnostních incidentů*

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

10. února 2026, Praha
TLP:CLEAR

Sára Vavřičková
Odbor kontroly

## Obsah prezentace

# 1 Legislativa



## Zákon č. 264/2025 Sb., o kybernetické bezpečnosti

- **Publikován 4. srpna 2025** ve Sbírce zákonů jako zákon č. 264/2025 Sb.
- **Účinný od 1. listopadu 2025**

**Základ změn:**

- Nová směrnice NIS2
- Potřeba aktualizace zákona o kybernetické bezpečnosti

- Odkaz na směrnici: Directive - 2022/2555 - EN - EUR-Lex
- Český překlad: Průvodce směrnicí NIS2 | Portál NÚKIB

**Z čeho NÚKIB vycházel:**

- Většina požadavků nového zákona vychází právě ze směrnice NIS2
- Znění zákona č. 181/2014 Sb., o kybernetické bezpečnosti a vyhlášky č. 81/2018 Sb.
- Mezinárodně uznávané standarty a normy (ISO, NIST, ITIL, …)
- Zkušenosti z dosavadních činností NÚKIB (regulace, kontrola, incidenty, …)
- Spolupráce se zahraničními partnery (ekvivalenty NÚKIB)
- Další dotazy, konzultace, podněty, …

## Zákon č. 264/2025 Sb., o kybernetické bezpečnosti

**Hlavní změny:**

- **rozšíření působnosti** – více povinných subjektů,
- **dvoustupňový režim povinností** – vyšší a nižší režim povinností,
- **změna způsobu identifikace povinných osob,**
- doplnění **nových požadavků na zavádění bezpečnostní opatření,**
- doplnění **nových požadavků na proces hlášení kybernetických bezpečnostních incidentů,**
- **odpovědnost vrcholného vedení** za zajištění kybernetické bezpečnosti,
- **přísnější sankce** a nové formy správního trestání
- a další.



## Prováděcí předpisy

**Vyhláška o regulovaných službách**

- Upravuje kritéria pro určení regulovaných osob
- Upravuje kritéria pro stanovení režimu regulace (vyšší a nižší)

**Vyhláška o bezpečnostních opatřeních pro vyšší režim**

- Stanovuje v detailu bezpečnostní opatření pro povinné osoby
- Každý poskytovatel regulované služby je určen v příslušném režimu podle vyhlášky o regulovaných službách

**Vyhláška o bezpečnostních opatřeních pro nižší režim**

- Stanovuje v detailu bezpečnostní opatření pro povinné osoby
- Každý poskytovatel regulované služby je určen v příslušném režimu podle vyhlášky o regulovaných službách
- Obsahuje také způsob identifikace incidentů s významným dopadem

**Vyhláška o Portálu NÚKIB**

- Upravuje technické a procesní náležitosti řešení automatizace a elektronizace procesů NÚKIB
- Definuje procesní a technické náležitosti pro hlášení údajů, incidentů, přístupu k informacím a elektronickým službám poskytovaným NÚKIB ze strany povinných subjektů

# Povinnosti poskytovatele regulované služby



## Hlavní povinnosti vyplývající ze zákona

1. Ohlásit regulovanou službu
2. Hlásit kontaktní údaje
3. Stanovit rozsah řízení kybernetické bezpečnosti
4. Zavádět bezpečnostní opatření
5. Hlásit kybernetické bezpečnostní incidenty
6. Informovat uživatele o incidentech a hrozbách
7. Zavádět bezpečnostní opatření vydaná NÚKIB

Průvodce novým zákonem o kybernetické bezpečnosti | Portál NÚKIB

## Do kdy co plnit?




## Rozsah řízení kybernetické bezpečnosti

- Nezbytná **prerekvizita pro funkční řízení bezpečnosti** – co poskytuji a na čem to je závislé
- Součástí rozsahu řízení kybernetické bezpečnosti jsou aktiva související s poskytováním regulované služby = stanovený rozsah
- Pokud/dokud rozsah není stanoven = rozsahem je celá organizace

## Stanovení rozsahu řízení kybernetické bezpečnosti

**Stanovení rozsahu řízení kybernetické bezpečnosti ve třech krocích:**

1. Určení všech primárních aktiv v organizaci
2. Posouzení primárních aktiv
3. Určení podpůrných aktiv

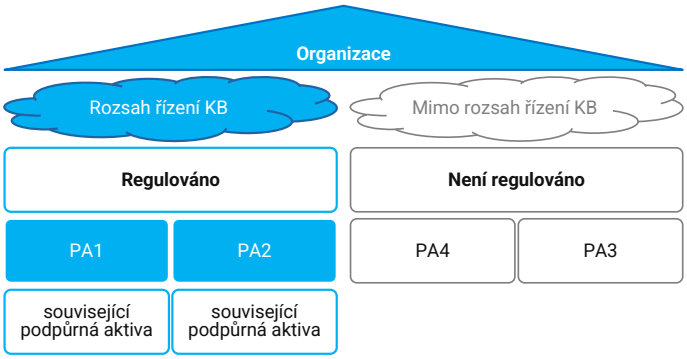
Aktivum = fyzický nebo digitální prostředek, osoba nebo činnost související se zpracováváním informací a dat v elektronické podobě

Primární aktivum = podobě zpracovávané informace nebo poskytované služby

Podpůrné aktivum = zajišťující fungování primárních aktiv, zejména zaměstnanec, dodavatel, technické aktivum, budova a jiný ohraničený prostor, ve kterém se nachází aktivum regulované služby



## Stanovení rozsahu řízení kybernetické bezpečnosti




Stanovení rozsahu řízení kybernetické bezpečnosti | Portál NÚKIB

## Organizační a technická bezpečnostní opatření

**Pro poskytovatele regulované služby v režimu vyšších povinností jsou**

**Organizační opatření**
a) systém řízení bezpečnosti informací,
b) povinnosti vrcholného vedení,
c) bezpečnostní role,
d) řízení bezpečnostní politiky a bezpečnostní dokumentace,
e) řízení aktiv,
f) řízení rizik,
g) řízení dodavatelů,
h) bezpečnost lidských zdrojů,
i) řízení změn,
j) akvizice, vývoj a údržba,
k) řízení přístupu,
l) zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,
m) řízení kontinuity činností a
n) audit kybernetické bezpečnosti

**Technickými opatření**
a) fyzická bezpečnost,
b) bezpečnost komunikačních sítí,
c) správa a ověřování identit,
d) řízení přístupových oprávnění,
e) detekce kybernetických bezpečnostních událostí,
f) zaznamenávání bezpečnostních a relevantních provozních událostí,
g) vyhodnocování kybernetických bezpečnostních událostí,
h) aplikační bezpečnost,
i) kryptografické algoritmy,
j) zajišťování dostupnosti regulované služby a
k) zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv.

**Pro poskytovatele regulované služby v režimu nižších povinností jsou bezpečnostními opatřeními**

**Organizační a technická opatření**
a) systém zajišťování minimální kybernetické bezpečnosti,
b) požadavky na vrcholné vedení,
c) řízení aktiv,
d) řízení rizik,
e) bezpečnost lidských zdrojů,
f) řízení kontinuity činností,
g) řízení přístupu,
h) řízení identit a jejich oprávnění,
i) detekce a zaznamenávání kybernetických bezpečnostních událostí,
j) řešení kybernetických bezpečnostních incidentů,
k) bezpečnost komunikačních sítí,
l) aplikační bezpečnost a
m) kryptografické algoritmy

*„na základě cílů systému řízení bezpečnosti informací, bezpečnostních potřeb a řízení rizik **zavede přiměřená bezpečnostní opatření …**“*



## Vyšší režim – změny oproti vyhlášce č.82/2018 Sb.

**Organizační opatření:**

- **Úprava struktury a textace** pro lepší srozumitelnost a jednotný výklad
- **Zánik pojmu provozovatel** informačního nebo komunikačního systému
- **Odstranění § 10** (Řízení provozu a komunikací)
  - Povinnosti rozprostřeny do jednotlivých §
- **Odebrána příloha č. 1**, která specifikovala doporučené požadavky na bezpečnostní role
- **Odebrána příloha č. 5**, která upravovala požadavky na dokumentaci
  - Méně administrativní zátěže
  - Vedení relevantních politik a dokumentace
  - Nově vznikne jako podpůrný materiál (doporučená struktura)
- **Nová příloha**
  - Doporučená témata pro rozvoj bezpečnostního povědomí (Příloha č. 7)

## Vyšší režim – změny oproti vyhlášce č.82/2018 Sb.

**Technická opatření**

- Fyzická bezpečnost
  - dokumentace perimetrů
- Bezpečnost komunikačních sítí
  - dokumentace segmentace a topologie
- Správa a ověřování identit
  - evidence autentizačních mechanismů pouze na bázi hesla
- Detekce kybernetických bezpečnostních událostí
  - součástí ochrana před škodlivým kódem
- Zaznamenávání událostí
  - nástroj pro sběr a uchovávání
- Aplikační bezpečnost
  - podpora, skenování zranitelností
- Kryptografické algoritmy
  - zabezpečení komunikace
- Zajišťování dostupnosti regulované služby
  - zálohování



## Nižší režim

- vychází ze základních principů řízení kybernetické bezpečnosti, které vedou k zavádění a provádění **přiměřených bezpečnostních opatření**

### Neopominutelná

Základní bezpečnostní požadavky, které je poskytovatel regulované služby **povinen zavést.**

- § 3 Systém zajišťování minimální kybernetické bezpečnosti
- § 4 Požadavky na vrcholné vedení
- § 5 Bezpečnost lidských zdrojů
- § 6 Řízení kontinuity činností
- § 10 Řešení kybernetických bezpečnostních incidentů

### Vyhodnotitelná

Poskytovatel regulované služby **musí zvážit v jaké míře,** případně zdali vůbec bude daná bezpečnostní opatření zavádět, aby to bylo přiměřené bezpečnostním potřebám organizace.

- § 7 Řízení přístupu
- § 8 Řízení identit a jejich oprávnění
- § 9 Detekce a zaznamenávání kybernetických bezpečnostních incidentů
- § 11 Bezpečnost komunikačních sítí
- § 12 Aplikační bezpečnost
- § 13 Kryptografické algoritmy

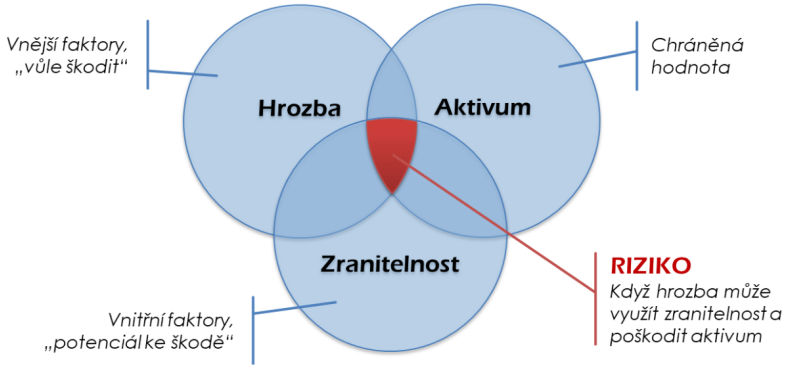
# 2 Řízení rizik



## Řízení rizik

**Řízení rizik** = **proces** zahrnující **hodnocení rizik** (identifikaci, analýzu a vyhodnocení), **zavedení bezpečnostních opatření** ke zvládání rizik a komunikaci rizik.

**Složky rizika:**



## Řízení aktiv

Identifikace primárních a podpůrných aktiv - **určena při stanovení rozsahu** řízení kybernetické bezpečnosti.

**Řízení aktiv**, která jsou ve stanoveném rozsahu řízení kybernetické bezpečnosti
- evidence, přiřazení garantů a ohodnocení

**Správný vstup do řízení rizik**



## Složky rizika - hrozby

**Hrozba** – je síla, událost, aktivita nebo osoba, která má **nežádoucí** vliv na aktiva nebo **může** způsobit **škodu**.

Původ hrozby je
- lidský  Lidská chyba, podvody, krádeže, vydírání, kybernetické útoky, sabotáže, terorismus, válečný stav.
- přírodní  Požár, povodeň, záplava, vliv počasí (vítr, déšť, mráz, horko) zemětřesení.
- technická závada  Selhání napájení, selhání komunikace, selhání HW nebo SW vybavení

Hrozby mohou být **náhodné** nebo **úmyslné**.

Pojem dle zákona

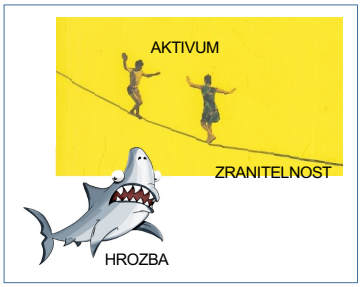
Hrozbou je jakákoliv **potenciální okolnost, událost** nebo **jednání**, které mohou být příčinou kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, a **která mohou poškodit, narušit nebo jinak nepříznivě ovlivnit** aktiva, jejich uživatele nebo další osoby.

## Složka rizika - zranitelnost

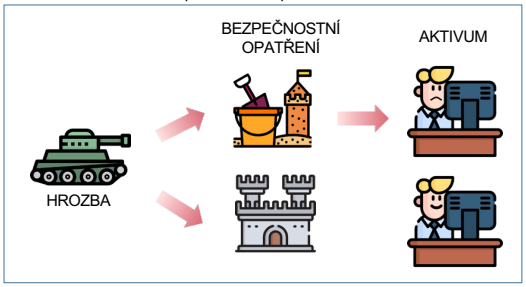
**Zranitelnost** – je **slabé místo aktiva** nebo slabé místo **bezpečnostního opatření**, které **může** být zneužito jednou nebo více hrozbami.

Zranitelnost je **vlastností aktiva** nebo bezpečnostního **opatření** na jeho ochranu.

Zranitelnost vlastností aktiva




Zranitelnost vlastností bezpečnostního opatření





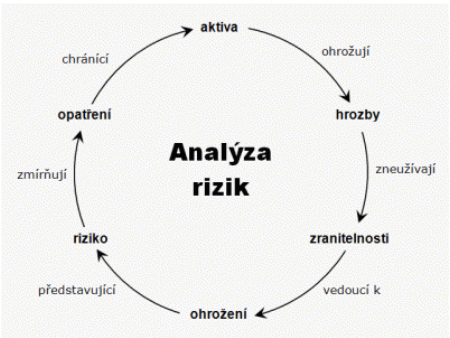

## Hodnocení rizik

Co to je to hodnocení rizik?

- část procesu řízení rizik → zjištění a stanovení úrovně rizika
- zahrnuje → určení rizik, analýzu rizik a vyhodnocení rizik

- Jedná se o soustavný a systematický proces
- Hodnocení rizik je prováděno v pravidelných intervalech definovaných VKB

Hodnocení rizik vs. analýza rizik
Je tam rozdíl?



## Hodnocení rizik – proces dle vyhlášky

- Metodika pro identifikaci a hodnocení rizik
  - Přizpůsobená potřebám organizace
  - Proces hodnocení rizik by měl být formalizovaný, prokazatelný a opakovatelný
- Stanovení kritérií pro akceptovatelnost rizik
- Identifikace
  - Aktiv (co vlastně chráním)
  - hrozeb a zranitelností
- Hodnocení rizik

Riziko = dopad (hodnota aktiva) x hrozba x zranitelnost



## Zvládání rizik – proces dle vyhlášky

**Zvládání rizik:**

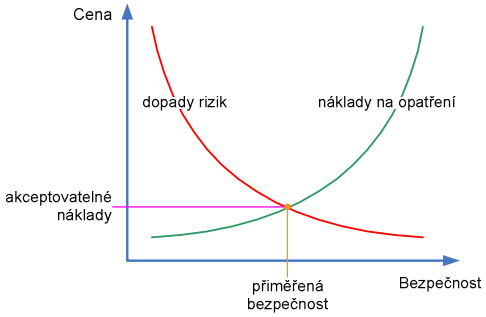
1. Akceptace rizika
2. Redukce a eliminace
3. Vyhnutí se riziku
4. Přenesení nebo sdílení rizik

**Zpracování:**

- zprávy o hodnocení aktiv a rizik,
- prohlášení o aplikovatelnosti (PoA) a
- plánu zvládání rizik (RTP).

## Přiměřená opatření

- Náklady na bezpečnostní opatření by měly být vždy přiměřené a neměly by převýšit náklady spojené s následky realizace rizika






## 3 Hlášení kybernetických bezpečnostních incidentů

## Hlášení kybernetických bezpečnostních incidentů

Poskytovatel regulované služby **v režimu vyšších povinností** je povinen:

- v rámci stanoveného rozsahu
- hlásit Úřadu
- všechny kybernetické bezpečnostní incidenty, které
  - **mají původ v kybernetickém prostoru a**
  - **nelze u nich do maximálně 24 hodin vyloučit úmyslné zavinění**
- významný dopad – do 24 hodin vyhodnotí NÚKIB a vrátí odpověď

Pokud významný dopad
- Do 72 hodin další hlášení
- Na výzvu průběžná zpráva o řešení
- Do 30 dnů závěrečná zpráva (do 60 pokud incident trvá)

Poskytovatel regulované služby **v režimu nižších povinností** je povinen:

- v rámci stanoveného rozsahu
- hlásit Národnímu CERT
- všechny kybernetické bezpečnostní incidenty, které
  - mají původ v kybernetickém prostoru,
  - nelze u nich do maximálně 24 hodin vyloučit úmyslné zavinění
  - **mají významný dopad na poskytování regulované služby**
- významný dopad - vyhodnotí sám podle vyhlášky



# Děkuji za pozornost

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

regulace@nukib.gov.cz

Ing. Sára Vavřičková

Referent bezpečnosti státu, Odbor kontroly

Email: sara.vavrickova@nukib.gov.cz
Telefon: +420 601 070 467