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

NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

Adam Kučínský
ředitel
odbor regulace

Online přednáška portal.nukib.gov.cz
TLP: CLEAR

Informace na úvod

Tento materiál slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů.
Tento materiál se primárně zaměřuje na oblast identifikace poskytovatelů regulovaných služeb a jejich povinnosti.
Tento materiál nenahrazuje a nepokrývá všechny detaily zákona o kybernetické bezpečnosti.

Shrnutí situace

- **Zákon o kybernetické bezpečnosti byl 4. srpna 2025 publikován ve Sbírce zákonů jako zákon č. 264/2025 Sb., a účinnosti nabyde 1. listopadu 2025**

- Základem změn je nová **směrnice NIS2**, ale také potřeba zákon o kybernetické bezpečnosti aktualizovat
- Do zákona jsou promítnuty také vnitrostátní instituty a požadavky
- Směrnice obecně je legislativní akt Evropské unie, který není sám o sobě aplikovatelný **(= musí nejdříve vzniknout národní úprava)**

Směrnice NIS2

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 (**směrnice NIS 2**)

- Směrnice EU je normativním právním aktem – nástroj pro harmonizaci
- Adresátem je členský stát – ten má povinnost promítnout požadavky směrnice do své národního práva
- Směrnice stanovují cíl – cesta a prostředky jsou na státech
- Směrnice zpravidla stanovují minimální požadavky – státy mohou jít nad rámec, ve specifických případech ale může být plná harmonizace

- Většina požadavků nového zákona vychází právě ze směrnice NIS2

- Odkaz na směrnici: Directive - 2022/2555 - EN - EUR-Lex

Hlavní změny v novém zákoně o kybernetické bezpečnosti

- **Rozšíření počtu povinných osob,** a to jak rozšířením regulovaných odvětví, tak rozšířením stávajících regulovaných odvětví o nové regulované služby
- **Změna způsobu identifikace povinných osob**
- Doplnění **nových požadavků na zavádění bezpečnostních opatření**
- Doplnění **nových požadavků na proces hlášení kybernetických bezpečnostních incidentů**
- **Větší odpovědnost vrcholného vedení** za zajišťování kybernetické bezpečnosti
- **Větší důraz na sdílení informací**
- **Prohloubení spolupráce** nejen mezi Úřadem a regulovanými osobami, ale i mezi Úřadem a dalšími orgány veřejné moci
- **Zvýšení pokut** a nové formy správního trestání
- **Nové požadavky na řešení problematiky bezpečnosti dodavatelského řetězce**

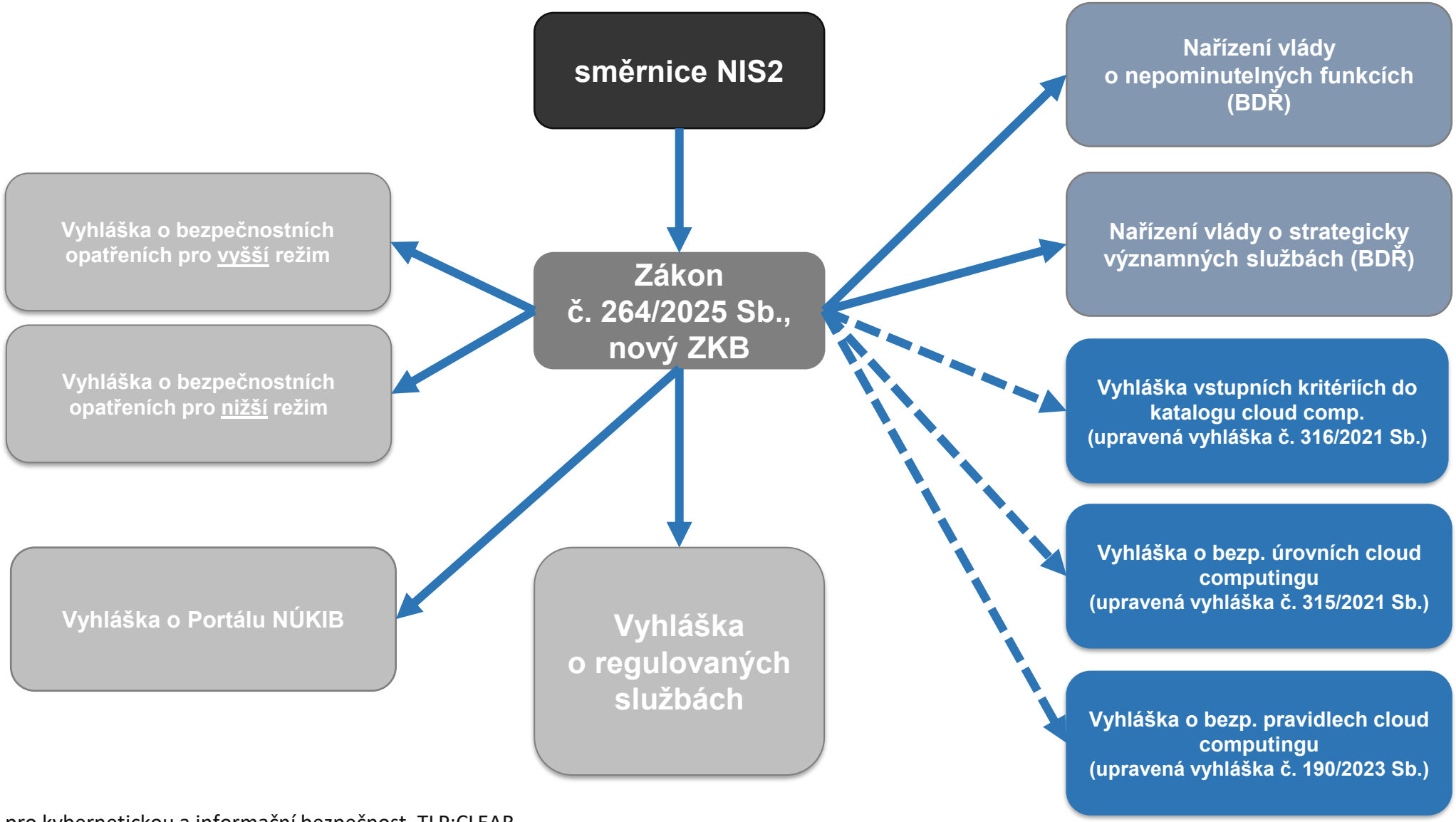
Struktura zákona č. 264/2025 Sb., o KB

ČÁST PRVNÍ KYBERNETICKÁ BEZPEČNOST
Hlava I Základní ustanovení
Hlava II Poskytovatel regulované služby
Díl 1 Regulovaná služba a režim jejího poskytovatele
Díl 2 Povinnosti poskytovatele regulované služby
Díl 3 Vztah poskytovatele regulované služby a jeho dodavatelů
Díl 4 Strategicky významná služba
Díl 5 Mechanismus prověřování bezpečnosti dodavatelského řetězce
Díl 6 Zajištění dostupnosti strategicky významné služby
Hlava III Osoba poskytující službu registrace jmen domén a subjekt spravující a provozující registr domén nejvyšší úrovně
Hlava IV **Další nástroje zajišťování kybernetické bezpečnosti**
Hlava V Výkon veřejné správy a jeho kontrola
Díl 1 Orgány a osoby vykonávající veřejnou správu v oblasti kybernetické bezpečnosti
Díl 2 Kontrola orgánů a osob vykonávajících veřejnou správu v oblasti kybernetické bezpečnosti
Díl 3 Nástroje výkonu veřejné správy
Hlava VI Kontrola vykonávaná Úřadem, nápravná opatření, přestupky a sankce

ČÁST DRUHÁ USTANOVENÍ SPOLEČNÁ, PŘECHODNÁ A ZÁVĚREČNÁ

+ doprovodný zákon č. 265/2025 Sb., kterým se mění některé zákony v souvislosti s návrhem zákona

Ekosystém nZKB – prováděcí předpisy



Ekosystém nZKB – prováděcí předpisy

Vyhláška o regulovaných službách

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

Vyhláška o bezpečnostních opatřeních pro vyšší režim

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

Vyhláška o bezpečnostních opatřeních pro nižší režim

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

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 a plněným vůči NÚKIB ze strany povinných subjektů

Ekosystém nZKB – prováděcí předpisy

Nařízení vlády o nepominutelných funkcích stanoveného rozsahu

- Týká se Mechanismu prověřování bezpečnosti dodavatelského řetězce
- Její obsah je jedním ze dvou způsobů, jak identifikovat aktiva, na kterých se bude Mechanismus prověřování bezpečnosti dodavatelského řetězce realizovat

Nařízení vlády o strategicky významných službách

- Upravuje, koho se bude týkat mechanismus prověřování bezpečnosti dodavatelského řetězce a povinnost zajištění dostupnosti strategicky významné služby.

Vyhláška o bezpečnostních úrovních pro využívání cloud computingu

- V souvislosti s přesunem zmocnění ze ZKB do ZoISVS dojde ke zrušení stávající vyhlášky č. 315/2021 Sb., a je tedy nutné vydat vyhlášku znova i s úpravami, které reflektují změny definic v zákoně apod.

Vyhláška o vstupních kritériích do katalogu cloud computingu

- Zároveň bylo třeba upravit vyhlášku č. 316/2021 Sb., například návaznost na přestupky v nZKB a další detaily

Vyhláška o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu

- V souvislosti se změnami v novém zákoně o kybernetické bezpečnosti je nutno provést úpravy vyhlášky č. 190/2023 Sb.

Identifikace a určení povinných osob

Koho se regulace týká?

Regulovanou službou je

- služba naplňující podmínky pro registraci (podle § 4) = alespoň jedno „**kritérium pro identifikaci“ regulované služby podle vyhlášky o regulovaných službách**

  = **samoidentifikace**

nebo

- služba naplňující podmínky pro registraci (podle § 5) = **služba stanovená rozhodnutím** Národního úřadu pro kybernetickou a informační bezpečnost na základě kritéria pro určení regulované služby.

  = **určení regulátorem**

Samoidentifikace

Střední nebo velký podnik

- Při počítání velikosti subjektu se postupuje v souladu s doporučením komise 2003/361/ES o definici mikropodniků, malých a středních podniků
- Pro posouzení velikosti subjektu musí být naplněn zaměstnanecký nebo finanční ukazatel – počet zaměstnanců nebo rozvaha nebo obrat
- **Střední podnik** (50 a více zaměstnanců/10 mil. EUR rozvaha/10 mil. EUR obrat)
- **Velký podnik** (250 a více zaměstnanců/43 mil. EUR rozvaha/50 mil. EUR obrat)
- Partnerské podniky (25-50% účasti) / Propojené podniky (nad 50% účasti) **se z pohledu velikosti sčítají**

Poskytuje regulovanou službu

- Viz vyhláška o regulovaných službách – vychází z příloh směrnice NIS2

Typicky velké podniky ve vybraných odvětvích vyšší režim, střední podniky nižší režim, ale pozor na **výjimky**

- **DNS, registr internetových domén nejvyšší úrovně, veřejná správa, případně dle národní implementace**
- **ISP padají do regulace všichni** – jejich velikost má vliv na režim

Zvláštní ustanovení o určování velikosti podniku

§ 7 zákona o kybernetické bezpečnosti - Zvláštní ustanovení o určování velikosti podniku

Odchylně od pravidel doporučení Komise 2003/361/ES pro účely tohoto zákona platí, že

a) čl. 3 odst. 4 doporučení Komise 2003/361/ES se neuplatní, */nesčítají se veřejné subjekty – obce, kraje/*

b) za podnik se nepovažují organizační složky státu, územní samosprávné celky a Česká národní banka,

c) za partnerský nebo propojený podnik se nepovažují osoby, jejichž technická aktiva jsou zcela oddělena od technických aktiv, která používá posuzovaná osoba při poskytování regulované služby, a

d) pro určování velikosti poskytovatele regulované služby v odvětví věda, výzkum a vzdělávání, který není podnikem, se pravidla pro určování velikosti podniku podle doporučení Komise 2003/361/ES, včetně speciálních pravidel upravených tímto zákonem, použijí obdobně.

Vyhláška o regulovaných službách - samoidentifikace

2. Energetika – Elektřina

Regulovaná služba	
Služba	**Podmínky významnosti poskytovatele regulované služby a jeho režim**
2.1 Výroba elektřiny podle energetického zákona[13] s výjimkou výroby elektřiny ve výrobně elektřiny z obnovitelných zdrojů energie o celkovém instalovaném elektrickém výkonu do 1 MW	Držitel licence na výrobu elektřiny podle energetického zákona je I. poskytovatelem regulované služby v režimu vyšších povinností v případě, že a) je podnikem, který přesahuje hodnoty vymezující střední podnik podle doporučení Komise 2003/361/ES o definici mikropodniků a malých a středních podniků (dále jen „velký podnik“), nebo b) disponuje výrobnou s celkovým instalovaným elektrickým výkonem nejméně 100 MW, nebo II. poskytovatelem regulované služby v režimu nižších povinností v případě, že je středním podnikem.
2.2 Provoz přenosové soustavy elektřiny podle energetického zákona	Držitel licence na přenos elektřiny podle energetického zákona je poskytovatelem regulované služby v režimu vyšších povinností.
2.3 Provoz distribuční soustavy elektřiny podle energetického zákona	Držitel licence na distribuci elektřiny podle energetického zákona je I. poskytovatelem regulované služby v režimu vyšších povinností v případě, že

Pro zjištění zda se vás regulace týká využijte kalkulačku NÚKIB na Kalkulačka | Portál NÚKIB

Určení ze strany NÚKIB

§ 5 zákona o kybernetické bezpečnosti

Podmínky pro registraci regulované služby jsou dále splněny v případě, že

a) jde o službu podle § 4 odst. 1 písm. a) a
   1. její poskytovatel je jediným poskytovatelem této služby v České republice a tato služba je zásadní pro zabezpečení důležitých společenských nebo ekonomických činností nebo pro bezpečnost v České republice,
   2. narušení této služby by mohlo mít významný dopad na bezpečnost České republiky, vnitřní pořádek nebo život a zdraví,
   3. narušení této služby by mohlo vyvolat významná systémová rizika, zejména v odvětvích, kde by takové narušení mohlo mít přeshraniční dopad, nebo
   4. její poskytovatel je kvůli svému specifickému významu na regionální nebo celostátní úrovni zásadní pro konkrétní odvětví, ve kterém působí, nebo typ služby, kterou poskytuje anebo pro jiná vzájemně propojená odvětví v České republice,

b) jde o službu, jejíž narušení může způsobit závažný zásah do života více než 125 000 osob, a to prostřednictvím ohrožení bezpečnosti České republiky, vnitřního pořádku, života a zdraví, majetkové hodnoty nebo životního prostředí,

c) jde o službu, jejíž narušení může způsobit závažný zásah do schopnosti poskytovat jinou regulovanou službu poskytovatele v režimu vyšších povinností, nebo

d) jde o službu, jejíž poskytovatel 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.

Tato kritéria vyhodnocuje NÚKIB ve správním řízení

Režim poskytovatele regulované služby

Režim poskytovatele regulované služby stanovuje míru jemu uložených povinností.

Režim poskytovatele regulované služby je:

- **režim vyšších povinností,**

nebo

- **režim nižších 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.

Strategicky významná služba – specialita vyššího režimu

Strategicky významné služby

- **Nejkritičtější služby,** u nichž je významný spillover efekt
- Jsou to vybrané služby z odvětví **veřejná správa, energetika, telekomunikace a doprava**
- Definovány v **nařízení vlády o strategicky významných službách**
- **Provádějí samoidentifikaci (naplní kritéria, tedy jsou strategicky významnou službou)**
- Pro tyto služby platí **mechanismus bezpečnosti dodavatelského řetězce** a **zajištění dostupnosti**

NAŘÍZENÍ VLÁDY
ze dne …

o regulovaných službách, které splňují podmínky strategicky významné služby a o částech strategicky významných služeb tvořících nezbytný rozsah zajištění dostupnosti strategicky významných služeb (nařízení o strategicky významných službách)

Vláda nařizuje podle § 25 odst. 1 a § 33 odst. 4 zákona č. .../... Sb., o kybernetické bezpečnosti:

§ 1

Předmět právní úpravy

Toto nařízení upravuje v návaznosti na přímo použitelné předpisy Evropské unie[1])

a) regulované služby, které splňují podmínky strategicky významné služby podle § 25 zákona, a
b) části strategicky významných služeb tvořící nezbytný rozsah strategicky významných služeb a způsob jejich vymezení podle § 33 odst. 4 zákona.

§ 2

Regulované služby splňující podmínky strategicky významné

Povinnosti poskytovatele regulované služby

Hlavní povinnosti vyplývající z návrhu zákona

V případě **všech poskytovatelů regulované služby**

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 protiopatření vydaná Národním úřadem pro kybernetickou a informační bezpečnost

V případě těch, kteří jsou zároveň tzv. poskytovateli **strategicky významné služby navíc**

8. Mechanismus prověřování bezpečnosti dodavatelského řetězce
9. Zajištění dostupnosti strategicky významné služby

Do kdy co plnit?

1. Ohlášení regulované služby

- Je nutné regulovanou službu ohlásit přes portál
- Následně dojde k potvrzení o registraci regulované služby a poskytovatele
- Doručením registrace startují přechodné lhůty pro ostatní povinnosti

1. Ohlášení regulované služby prakticky

- Provádí se přes **Portál NÚKIB**
- **Statutár** musí udělat sám, nebo pověřit osobu – **zástupce**
  - První krok musí udělat **statutár** – přihlásí se přes NIA (bankovní identita a další způsoby)
  - Pokud **statutár** nemá NIA – lze první registraci a určení zástupce provést datovou schránkou – bude na to formulář
  - Pokud chce zástupce musí mít číslo jeho občanky
  - Statutár má právo zástupce měnit, zástupce nemůže sám delegovat
- **Zástupce**
  - Musí být fyzická osoba
  - Musí být v základních registrech
    - Občanství, povolení k pobytu
  - Muže provést ohlášení regulované služby nebo její změnu
  - Muže jich být více, můžou být různí pro různé regulované služby
  - Dostane informaci, že je zástupcem jak se má přihlásit – přihlášení přes NIA

Může si stáhnout export a potvrzení o digitálním úkonu

U změny stejně

Statutár i zástupce musí být fyzická osoba

2. Hlášení kontaktních údajů

Cílem je

- **zpřehlednění vztahu mezi úřadem a povinnou osobou** (regulované služby, režim,…)
- **nastavení přímé komunikační linky** mezi úřadem a povinnou osobou

- Hlášení má probíhat skrze **Portál NÚKIB** (Portál NÚKIB (gov.cz))
- Co se hlásí je upraveno vyhláškou o Portálu NÚKIB, vyhláška upravuje jak se přes systém bude řešit:
  - Registrace poskytovatele regulované služby a související změny
  - Pověřování osob aby mohly jednat s NÚKIB
  - Hlášení kontaktních a dalších údajů
  - Hlášení incidentů
  - Hlášení provedení protiopatření
  - Hlášení provedení nápravných opatření
  - Výmaz regulované osoby z registru
  - Hlášení informací o dodavatelích (BDŘ)

2. Hlášení kontaktních údajů prakticky

- Zástupce nebo statutár vyplní formulář – po přihlášení skrze NIA
- Může si stáhnout export a potvrzení o digitálním úkonu
- U změny stejně
- Subjekt může mít kontaktních osob kolik chce
- Mohou být různé u různých služeb
- Zástupce = automaticky kontaktní osoba, kontaktní osoba ≠ zástupce
- Musí být fyzická osoba

3. Stanovení rozsahu řízení kybernetické bezpečnosti

Nezbytná prerekvizita pro funkční řízení bezpečnosti – je nutno vědět jaké služby jsou poskytovány a na čem jsou závislé

Součástí rozsahu řízení kybernetické bezpečnosti jsou **aktiva související s poskytováním regulované služby.**

= stanovený rozsah

Postup:

Za účelem vymezení stanoveného rozsahu poskytovatel regulované služby

a) **určí všechna svá primární aktiva,**

b) **posoudí, zda** primární aktiva **souvisí s poskytováním regulované služby**, **a**

c) u primárních aktiv podle písmene b) **určí podpůrná aktiva.**

V rámci stanoveného rozsahu se jsou pak plněny povinnosti ze zákon.

Fikce stanovení rozsahu = Pokud/dokud rozsah není stanoven má se za to, že je rozsahem celá organizace.

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

Primární aktivům = aktivum v podobě zpracovávané informace nebo poskytované služby

3. Stanovení rozsahu řízení kybernetické bezpečnosti prakticky

- Vyberu co budu považovat za primární aktiva
  - informace nebo služby (případně procesy)
  - Určím granularitu (IT služby pro řízení bloku, e-mail, web, spisovka, evidence smluv, zákaznická podpora, data o zákaznících, informace z výroby, data pacientů…),
- Vytvořím evidenci **všech** primárních aktiv v organizaci
- Namapuji aktiva na regulované služby
- Určím ty, které souvisí s regulovanou službou a ty které ne
- Rozhodnu se, zda budu zavádět zákon na všechna aktiva nebo jen na ta, která souvisí s regulovanou službou
- U těch primárních aktiv, které souvisí s regulovanou službou provedu mapování podpůrných aktiv
- Tím mám definován rozsah
- V rozsahu plním povinnosti

4. Organizační a technická bezpečnostní opatření

Pro poskytovatele regulované služby v režimu <u>vyšších</u> 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

Viz samostatná přednáška

4. Bezpečnostní opatření prakticky

Vyšší režim

- Vyhodnotím rizika – provedu analýzu rizik
- Rizika, která nejsou akceptovatelná musím řešit – stanovím si plán řešení = plán zvládání rizik
- K rizikům namapuji opatření z vyhlášky
- Pokud nějaké opatření nelze zavést ve lhůtě – zdůvodním proč nejde a stanovím plán do kdy a jak provedu
- Zavádím opatření podle plánu, provádím audity…

Nižší režim

- Nemusí dělat analýzu rizik – výhoda i nevýhoda
- Ve vyhlášce jsou stanovená nepominutelná opatření – ty musím zavést každopádně
- U ostatních opatření vyhodnotím, zda je potřebuji a zda se mi vyplatí
- Pokud ne – udělám dokumentovaný záznam se zdůvodněním, proč je nerelevantní – a nezavedu
- Pokud ano – zavedu
- Vedu „přehled bezpečnostních opatření – základní dokument, kde je uvedeno co je zavedeno a co ne a proč

5. 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

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

Pokud významný dopad

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

5. Hlášení incidentů prakticky

- Incident může ohlásit kdokoli – primárně přes portál
- Hlášení není za přihlašovací branou, ohlašovatel se neověřuje ani neautentizuje
- Po nahlášení incidentu budou notifikovány kontaktní osoby o tom, že byl incident nahlášen a bude potvrzeno
- Následuje komunikace s operátorem CERT
  - Vyšší režim – do 24 hodin po oznámení NÚKIB sdělí, zda má významný dopad, když ano pokračuje hlášení
  - Nižší režim – do 72 h bližší info o incidentu…

Digitálové – specifická úprava

Z důvodu speciálního nastavení ve směrnici NIS 2 **existuje množina subjektů, které mají jiná pravidla pro bezpečnostní opatření a hlášení incidentů.**

Pravidla se použijí na ty subjekty, které poskytují

- **službu systému překladu jmen domén,**
- **služby správy a provozu registru domény 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**.

V případě **služby vytvářející důvěru** se pravidla použijí jen pro bezpečnostní opatření.

Digitálové mají bezpečnostní opatření a hlášení incidentů stanoveno prováděcím nařízení komise:

- https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=OJ:L_202402690

Vysvětlení zde:

- https://portal.nukib.gov.cz/informace/legislativa/zakon-o-kyberneticke-bezpecnosti/okruh-regulace-poskytovatelu-digitalnich-sluzeb

V případě jiných regulovaných služeb takového poskytovatele se však prováděcí nařízení Komise nepoužije!

Bezpečnostní opatření viz samostatná přednáška

Hlášení incidentů u digitálů

- Digitálové dle prováděcího nařízení hlásí incidenty v odlišném režimu
- Na rozdíl od incidentu ostatních regulovaných služeb **se nepoužije zúžení podle § 15 odst. 1 nZKB na úmysl a původ v kyberprostoru (§ 18 odst. 2 nZKB)**
- **Použije se obecná definice v NIS2:**
  - *„incidentem“ událost je narušující dostupnost, autenticitu, integritu nebo důvěrnost uchovávaných, předávaných nebo zpracovávaných dat nebo služeb, které jsou nabízeny prostřednictvím sítí a informačních systémů nebo které jsou jejich prostřednictvím přístupné“*
- **Definice incidentu je tedy širší než u ostatních povinných osob.**
- Implementing Act incidenty u digitálů zužuje podle významnosti.
  - Podobně jako u nižšího režimu je už **významnost definována prováděcím předpisem a zhodnotí si ji sám regulovaný subjekt.**
- Existují dva druhy kritérií významnosti – **obecné**, které platí pro všechny a **speciální**, které se dělí podle toho o jakou službu jde.
  - Detail obecných kritérií významnosti v článku 3 a 4 prováděcího nařízení
  - Detail speciálních kritérií významnosti v článku 5 – 14 prováděcího nařízení

Prováděcí nařízení - EU - 2024/2690 - CS - EUR-Lex

6. Informační povinnost – incident a hrozba

Informační povinnost – kybernetický bezpečnostní **incident**

- 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 může poskytovateli regulované služby uložit povinnost informovat uživatele regulované služby o tomto incidentu nebo to naopak zakázat

Informační povinnost – významná **hrozba**

- Poskytovatel regulované služby je **povinen informovat uživatele** regulované služby, který může být ovlivněn významnou hrozbou o této **hrozbě a o krocích k minimalizaci dopadu** hrozby.
- Významnou hrozbou **hrozba, u níž lze na základě jejích technických charakteristik předpokládat, že má potenciál závažně ovlivnit aktiva poskytovatele regulované služby nebo uživatele regulované služby natolik, že způsobí značnou újmu.**

6. Informační povinnost prakticky

- Je potřeba mít proces
- Mít nadefinováno podle čeho rozhodnu co je významná hrozba a incident s významným dopadem
- Mít nadefinováno v jakých případech budu informovat
- Mít nadefinováno jak budu informovat
- Mít nadefinováno koho budu informovat
- Mít nadefinováno kdo rozhodne o informování

7. Protiopatření

Podstatou je v mimořádných případech možnost státu zasáhnout k ochraně aktiv – existují 3 druhy protiopatření

Výstraha

- Vydává NÚKIB.
- **Informování veřejnosti** o kybernetickém bezpečnostním **incidentu či o porušování povinností** daných tímto zákonem.
- Možno uložit, aby to poskytovatel udělal sám.

Varování

- Úřad vydá varování, dozví-li se o **závažné hrozbě nebo zranitelnosti** v oblasti kybernetické bezpečnosti.
- Varování Úřad oznámí dotčeným poskytovatelům regulované služby prostřednictvím Portálu Úřadu a zveřejní jej na úřední desce Úřadu.
- Nově může být varování i neveřejné.

Reaktivní protiopatření

- Rozhodnutí, ve kterém **uloží poskytovateli regulované služby povinnost** provést reaktivní protiopatření.
- k řešení incidentu, k zabezpečení aktiv před incidentem, ke zvýšení bezpečnosti na základě incidentu

7. Protiopatření prakticky

Varování

- U vyššího režimu vstupuje do analýzy rizik – mění parametr hrozby nebo zranitelnosti (R=D x H x Z)
- U nižního režimu – nemá povinnost dělat analýzu rizik – použít ho nemusí, ale může
  - Pokud varování chce zohlednit ve veřejných zakázkách provede analýzu rizik jako vyšší režim

Reaktivní protiopatření

- Konkrétní adresáti i úkony
- pokud dostanu povinnost tak aplikuji
- Vždy zatím byla možnost neprovést pokud tomu brání vážní a relevantní důvody

8. Bezpečnost dodavatelského řetězce

- Cílem je omezit strategickou závislost České republiky na nedůvěryhodných dodavatelích
- Nová oblast, nevyplývá ze směrnice NIS2 ale z národního rozhodnutí
- Platí pouze pro strategicky významné služby
- Organizace v rámci této povinnosti musí nahlásit dodavatele
- Budou prověřování dodavatelé do kritické části systému = aktiva s hodnotou 4 (kritická), kteří dodávají bezpečnostně významnou dodávku = má výpočetní kapacitu
- Stát prověří
- NÚKIB k tomu vyžaduje informace a součinnost řady orgánů (PČR, SLUŽBY, FAU, NSZ, MPO, MV, NBÚ, ÚOHS…)
- Vláda může vydat zákaz dodavatele použít nebo upozornění na riziko (je řešitelné bezp. opatřením)
- Lze udělit výjimku (např. pokud to nikdo jiný nevyrábí, ohrozilo by to službu apod.)
- K vyřazení již dodaných technologií nemusí dojí hned – počítá se s přechodnými lhůtami
- Hlášení dodavatelů do 1 roku od určení poskytovatele regulované služby

8. Bezpečnost dodavatelského řetězce prakticky

- Vyhodnotit, zda jsem strategicky významná služba – zda se mě to týká
- Vydefinovat kritickou část stanoveného rozsahu
  - kritická aktiva + aktiva zajišťující nepominutelné funkce – viz nařízení vlády
- Zjišťovat informace o dodavatelích bezpečnostně významných dodávek – mít proces
  - Zeptat se dodavatele na subdodavatele, případně dodavatele subdodavatelů – prohlášení dodavatele
- Informovat o dodavatelích NÚKIB – skrze portál
- Proces jak implementovat případné omezení
  - Vyhodnocení relevance
  - Vyhodnocení proveditelnosti vč. časového hlediska
  - Komunikace s regulátorem, pokud je to neproveditelné – možnost udělení vyjímky
  - Nastavení plánu
  - Realizace

9. Zajištění dostupnosti strategicky významných služeb

Poskytovatel **strategicky významné služby** je povinen zajistit její dostupnost:

- **v nezbytném rozsahu,**
- **ve stanoveném čase a kvalitě,**
- **z území České republiky.**

Nezbytný rozsah dostupnosti strategicky významné služby stanoví nařízení vlády

Stanovený čas a kvalitu služby stanoví sám poskytovatel strategicky významné služby, zejména s ohledem na charakter a specifika jím poskytované strategicky významné služby, účel, pro nějž je poskytována, a závažnost dopadů narušení jejího řádného poskytování na uživatele služby.

Poskytovatel strategicky významné služby je povinen testovat schopnost zajištění poskytování strategicky významné služby v rozsahu kritické části stanoveného rozsahu z území České republiky nejméně jednou za dva roky.

9. Zajištění dostupnosti strategicky významných služeb

Východiska:

- zajištění dostupnosti **směruje na službu**, nikoli nutně na její dílčí aktiva (a už vůbec ne na všechna),
- zajištění dostupnosti služby je **možné i mimo kyberprostor,**
- kvalita služby může být snížena – míru snížení si definuje sám poskytovatel v rámci řízení kontinuity služby,
- úroveň služby může být snížena – míru snížení si definuje sám poskytovatel v rámci řízení kontinuity služby,

Cíl:

- kritické služby musíme být schopni zajistit alespoň omezeně z České republiky, abychom byli připraveni na mimořádné situace v zahraničí.

Prakticky to tedy znamená, že:

- je potřeba být schopen službu poskytovat z území ČR, tedy bez zajištění služeb ze zahraničí,
- zjištění služby může být i mimo ICT, např. náhradním postupem fyzicky - pokud to splní stanovený rozsah, čas a kvalitu.
- Čas a kvalitu si stanoví poskytovatel sám

9. Zajištění dostupnosti strategicky významných služeb prakticky

- Vyhodnotit zda mám strategicky významnou službu – viz nařízení vlády
- Vyhodnotit co je třeba abych ji mohl poskytovat z ČR
  - Co musí fungovat, aby **služba** fungovala?
  - Vyhodnotit co mám v zahraničí a týká se služby
  - Vyhodnotit co se stane když o dodávky/služby ze zahraničí přijdu
  - Co mám v zahraničí a co z toho nemohu postrádat, aby služba fungovala?
  - Co mohu to vyřadit tím, že snížím kvalitu služby (nebude tak dostupná, nebude tak bezpečná, nebude tak pohodlná…)?
    - Úroveň kvality je na poskytovateli služby
  - Jak rychle budu službu schopen obnovit pokud o zahraničí přijdu?
    - Doba obnovy je na poskytovateli služby
  - Jsem schopen něco nahradit mimo ICT, které je mimo ČR z ČR – např. fyzicky? Do kdy?
- Mít posouzení dokumentované
- Mít postupy dokumentované
- Mít odpovědnosti dokumentované
- Udělat si na to pravidelně (table top) cvičení - dokumentované

Vztah k odvětvovým právním předpisům Evropské unie

Pokud přímo použitelný předpis Evropské unie nebo jiný **právní předpis stanoví** orgánům nebo osobám **povinnosti v oblasti** zavádění a provádění **bezpečnostních opatření nebo hlášení kybernetických bezpečnostních incidentů** a tyto povinnosti mají alespoň **srovnatelný účinek** jako povinnosti, které jsou těmto orgánům nebo osobám stanoveny podle tohoto zákona, ustanovení tohoto zákona upravující povinnosti zavést a provádět bezpečnostní opatření a hlásit kybernetické bezpečnostní incidenty se vůči těmto orgánům a osobám **neuplatní,** a to včetně ustanovení o dozoru nad dodržováním uvedených povinností.

Za ustanovení se srovnatelným účinkem se považují taková ustanovení, která

a) ve vztahu k povinnosti zavést a provádět **bezpečnostní opatření** odpovídají alespoň požadavkům stanoveným v **§ 14 a 15**, nebo

b) ve vztahu k povinnosti hlásit **kybernetické bezpečnostní incidenty** odpovídají alespoň požadavkům stanoveným

§ 16 a 17.

Za ustanovení se srovnatelným účinkem jako povinnosti obsažené v tomto zákoně podle odstavce 1 se dále považují **taková ustanovení** přímo použitelného předpisu Evropské unie, **o nichž to** přímo použitelný právní předpis Evropské unie **sám stanoví**.

Další obsah nového zákona o kybernetické bezpečnosti

Další obsah nového zákona o kybernetické bezpečnosti

ČÁST PRVNÍ KYBERNETICKÁ BEZPEČNOST
Hlava I Základní ustanovení
Hlava II Poskytovatel regulované služby
Díl 1 Stanovení regulované služby a režimu jejího poskytovatele
Díl 2 Povinnosti poskytovatele regulované služby
Díl 3 Vztah poskytovatele regulované služby a jeho dodavatelů
Díl 4 Strategicky významná služba
Díl 5 Mechanismus prověřování bezpečnosti dodavatelského řetězce
Díl 6 Zajištění dostupnosti strategicky významné služby
Hlava III **Osoba poskytující službu registrace jmen domén a subjekt spravující a provozující registr domén nejvyšší úrovně**
Hlava IV Další nástroje zajišťování kybernetické bezpečnosti
Hlava V **Výkon veřejné správy a jeho kontrola**
Díl 1 Orgány a osoby vykonávající veřejnou správu v oblasti kybernetické bezpečnosti
Díl 2 Kontrola orgánů a osob vykonávajících veřejnou správu v oblasti kybernetické bezpečnosti
Díl 3 Nástroje výkonu veřejné správy
Hlava VI Kontrola vykonávaná Úřadem, nápravná opatření, přestupky a sankce

ČÁST DRUHÁ USTANOVENÍ SPOLEČNÁ, PŘECHODNÁ A ZÁVĚREČNÁ

Vztah poskytovatele regulované služby a jeho dodavatelů

Úřad **může v případě hrozícího nebo probíhajícího kybernetického bezpečnostního incidentu**, který by mohl mít závažný vliv na poskytování regulované služby s dopadem na zachování bezpečnosti České republiky, vnitřního pořádku, života a zdraví, majetkových hodnot nebo životního prostředí, **na podnět poskytovatele regulované služby v režimu vyšších povinností**, který marně vyzval svého dodavatele k předání informací a dat, **uložit tomuto dodavateli povinnost předat poskytovateli regulované služby informace a data související s provozem aktiv sloužících k poskytování regulované služby**. Pokud tento dodavatel informacemi nebo daty souvisejícími s provozem aktiv sloužících k poskytování regulované služby nedisponuje nebo vzhledem ke skutkovým okolnostem není účelné jejich opatření a vydání po něm požadovat, může Úřad povinnost podle věty první uložit každému, kdo požadovanými informacemi a daty disponuje.

Úřad může v rozhodnutí určit formát, rozsah, způsob a lhůtu předání těchto informací a dat a stanovit povinnost po jejich předání tyto informace a data a všechny jejich kopie bezpečně zlikvidovat.

Dodavatel … má nárok na úhradu účelně vynaložených nákladů… ze strany poskytovatele regulované služby.

Stav kybernetického nebezpečí

- Stav, kdy je ve velkém rozsahu ohrožena bezpečnost informací v kybernetickém prostoru, což by mohlo vést k ohrožení zájmů České republiky
- Vyhlášení jen s uvedením důvodu na nezbytnou dobu, max 30 dní, ředitel NÚKIB
- Rozhodnutí o vyhlášení musí obsahovat mimo jiné krizová opatření a jejich rozsah
- Nelze-li odvrátit ohrožení v rámci SKN, požádá se vláda o vyhlášení nouzového stavu
- Opatření v rámci SKB
  - Poskytnutí věcných prostředků NÚKIBu
  - Poskytnutí informací o prostředcích a materiálu
  - Poskytnutí personálních kapacit a věcných prostředků ze smlouvy s NÚKIB (pokud je)
  - Nařídit pohotovosti
  - Vyžádání informací o personálních kapacitách, materiálů, zásob a dalších
  - Zákaz používání technických aktiv
  - Zavedení opatření nařízených NÚKIB
  - Provedení pentestu nebo skenu zranitelností
  - Zpřístupnění komunikačních sítí (i neveřejných)

Subjekt poskytující službu registrace jmen domén a subjekt spravující a provozující registr domén nejvyšší úrovně

Osoba poskytující služby registrace doménových jmen hlásí bez zbytečného odkladu, nejpozději do 30 dnů ode dne, kdy začala poskytovat služby registrace doménových jmen, Úřadu následující údaje:

- název osoby,
- adresu hlavní provozovny a jejích dalších provozoven na území členských států Evropské unie nebo smluvních států Dohody o Evropském hospodářském prostoru, popřípadě zástupce osoby podle § 67,
- aktuální kontaktní údaje včetně adres elektronické pošty a telefonních čísel osoby, popřípadě jejího zástupce podle § 67,
- členské státy Evropské unie nebo smluvní státy Dohody o Evropském hospodářském prostoru, v nichž osoba poskytuje své služby, a
- rozsah veřejných IP adres osoby.
- Aktualizace údajů do 90 dnů od změny

Dále zákon definuje požadavky na to jak má vypadat databáze, kterou registrátoři vedou

Výjimka z práva na informace

- **Informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti**, nebo informace, které jsou vedené v evidencích vedených Úřadem, **se podle právních předpisů upravujících svobodný přístup k informacím a právo na informace o životním prostředí neposkytují**.

- Metodický materiál NÚKIB - Doporučení k (ne)poskytování informací

Kontrola vykonávaná Úřadem a sankce

Kontrola

- Úřad vykonává kontrolu v oblasti kybernetické bezpečnosti. Při výkonu kontroly Úřad zjišťuje, jak jsou plněny povinnosti stanovené tímto zákonem nebo na jeho základě a přímo použitelnými předpisy Evropské unie v oblasti kybernetické bezpečnosti.

Nápravná opatření

- Zjistí-li Úřad, že poskytovatel regulované služby nebo jiná osoba neplní povinnosti stanovené tímto zákonem nebo na základě tohoto zákona, může jim uložit, aby zjištěné nedostatky ve stanovené lhůtě odstranili, popřípadě určit jakým způsobem. Úřad může v rozhodnutí uložit povinnost oznámit Úřadu provedení nápravného opatření a jeho výsledek ve stanovené lhůtě.

Pozastavení platnosti certifikace

- Úřad může v případě **nesplnění povinnosti odstranit zjištěné nedostatky uložené nápravným opatřením** poskytovateli regulované služby v režimu vyšších povinností, který je držitelem evropského certifikátu kybernetické bezpečnosti podle aktu o kybernetické bezpečnosti nebo jiného certifikátu nebo osvědčení souvisejícího se zajištěním kybernetické bezpečnosti regulované služby, **pozastavit** tomuto poskytovateli regulované služby **platnost evropského certifikátu kybernetické bezpečnosti vydaného Úřadem nebo uložit subjektu posuzování shody povinnost pozastavit platnost jím vydaného certifikátu nebo osvědčení, a to až do doby odstranění zjištěných nedostatků, nejméně na 6 měsíců**.

Pozastavení výkonu řídící funkce

- Úřad **může členovi statutárního orgánu, který v přímé souvislosti s plněním nápravného opatření**, kterým byla poskytovateli regulované služby v režimu vyšších povinností uložena povinnost odstranit zjištěné nedostatky, **opakovaně nebo závažně porušil své povinnosti při výkonu funkce**, v důsledku čehož bylo zmařeno řádné splnění rozhodnutí Úřadu, **zakázat až do doby odstranění zjištěných nedostatků, nejméně po dobu 6 měsíců, výkon této funkce**.

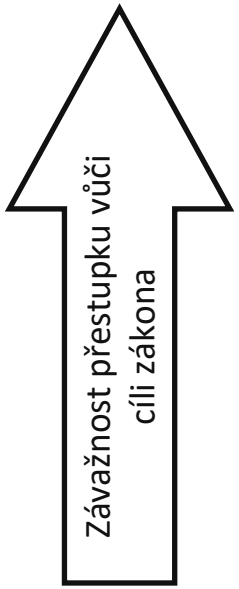
Přestupky a sankce

Nerozlišují veřejnoprávní nebo soukromoprávní povahu organizace.

Rozlišuje se postavení poskytovatele regulované služby v režimu vyšších nebo režimu nižších povinností.

Výše přestupků a rozdělení je dáno směrnicí NIS2, případně se od ní proporcionálně odvíjí.

Výše přestupků je dána jako maximální, vše probíhá v řízení o uložení pokuty, zohledňují se standardní polehčující a přitěžující okolnosti a přestupky nesmí být z povahy věci likvidační.



- **250 000 000 Kč** nebo až do výše **2 % čistého celosvětového ročního obratu dosaženého podnikem**
  - *vyšší režim = např. záměrné vyhýbání se ohlášení regulované služby, nezavádění bezpečnostních opatření,…*
- **175 000 000 Kč** nebo až do výše **1,4 % čistého celosvětového ročního obratu dosaženého podnikem**
  - *nižší režim = např. záměrné vyhýbání se ohlášení regulované služby, nezavádění bezpečnostních opatření,…*
- **100 000 000 Kč**
- **50 000 000 Kč**
- **35 000 000 Kč**
- **20 000 000 Kč**
  - *pokračování v roli vrcholného vedení i přes vydaný zákaz*

Děkuji za pozornost

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

regulace@nukib.gov.cz