

Kybernetická bezpečnost liniových staveb

**Nová směrnice NIS2 a právní
požadavky české implementace**

**Mgr. Pavel Amler
Mgr. Ondřej Dostál**

23. dubna 2026

Obsah

1. Úvod do NIS2
2. Implementace v České republice
3. Specifika české implementace
4. Dopady na odvětví a vztah k dalším právním předpisům
5. Role NÚKIB
6. Diskuse

ÚVOD DO NIS2

Co je NIS2

- Směrnice EU o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti a o zrušení směrnice NIS1
- Změna regulatorního rámce
 - strategická úroveň (*povinnosti zejm. pro NÚKIB, ENISA*)
 - regulace povinných osob (*nová odvětví a služby*)



Hlavní regulační změny v NIS2

- zásadní **rozšíření počtu regulovaných** (povinných) subjektů
- povinné **vzdělávání a odpovědnost** vrcholového **managementu**
- zásadní **zvýšení pokut** a nové druhy sankcí
- důraz na sdílení informací mezi povinnými subjekty
- prohloubení spolupráce mezi regulátorem a povinnými subjekty

IMPLEMENTACE V ČR

Stav implementace směrnice NIS2 v ČR

- Implementace zavedena **zákonem č. 264/2025 Sb., o kybernetické bezpečnosti** ze dne 11. 6. 2025
- Zákon nabyl účinnosti 1. 11. 2025

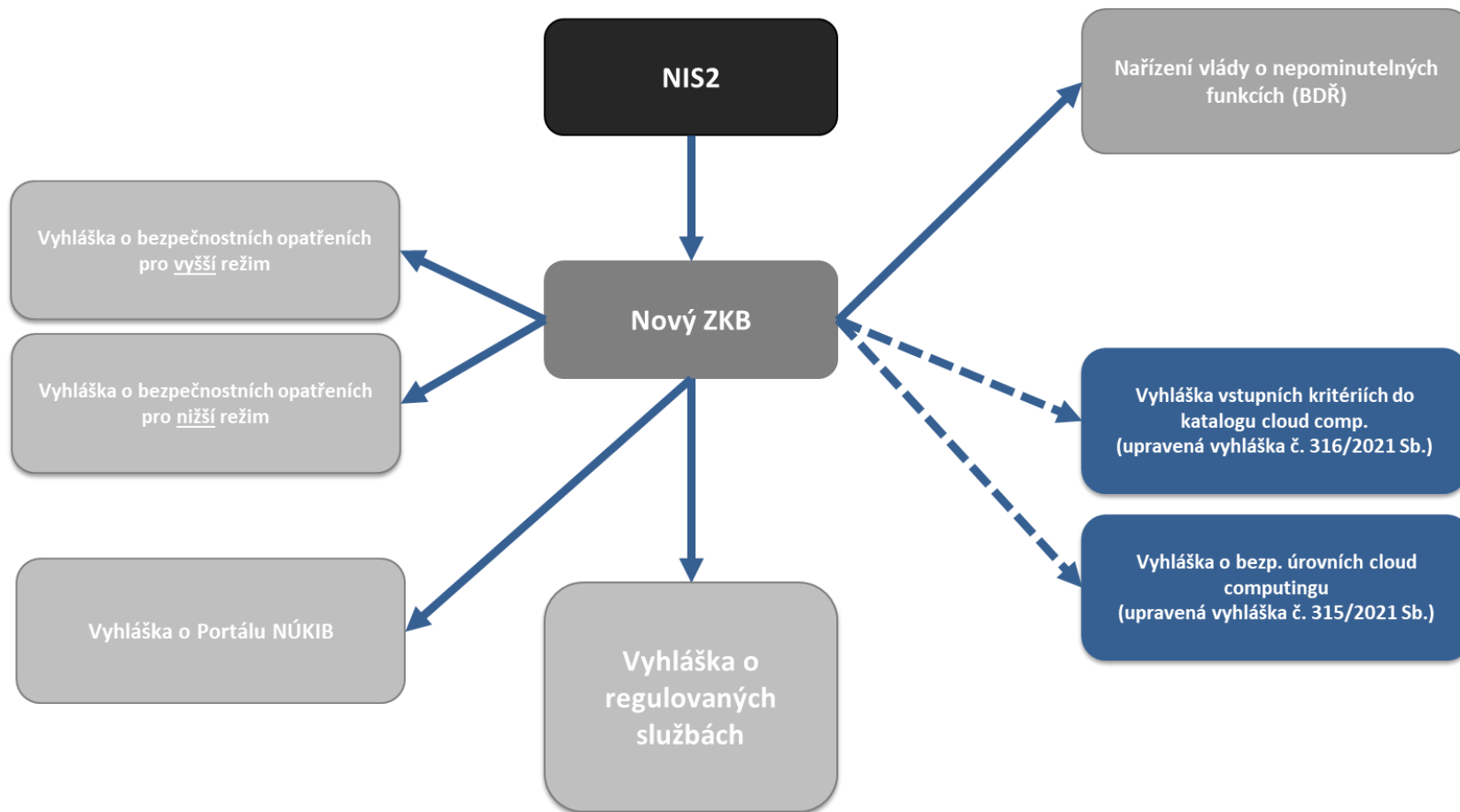
Hlavní změny v novém zákoně o kybernetické bezpečnosti

- Nové požadavky, reprezentované především požadavky směrnice NIS2, vedou k tomu, že návrh zákona musí zohlednit:
 - **rozšíření počtu povinných osob**, a to jak rozšířením regulovaných odvětví, tak rozšířením stávajících regulovaných odvětví o nové regulované služby,
 - **změnu 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**.

Prováděcí vyhlášky k novému zákonu

- **O regulovaných službách (408/2025 Sb.) – účinnost od 1. 11. 2025**
 - Kritéria pro určení regulovaných osob a režimu (vyšší/nížší)
- **O bezpečnostních opatřeních pro vyšší režim (409/2025 Sb.) – účinnost od 1. 11. 2025**
 - Detailní požadavky na subjekty ve vyšším režimu
- **O bezpečnostních opatřeních pro nižší režim (410/2025 Sb.) – účinnost od 1. 11. 2025**
 - Detailní požadavky na subjekty v nižším režimu
- **O Portálu NÚKIB (334/2025 Sb.) – účinnost od 1. 11. 2025**
 - Hlášení údajů, incidentů, elektronické služby
- **O bezpečnostních úrovních pro využívání cloud computingu (411/2025 Sb.) – účinnost od 1. 11. 2025**
 - Novela vyhlášky č. 315/2021 Sb.
- **O bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu (412/2025 Sb.) – účinnost od 1. 11. 2025**
 - Novela vyhlášky č. 190/2023 Sb.

Ekosystém ZKB – prováděcí předpisy



Navazující nařízení vlády k novému zákonu

Konkretizace povinností pro poskytovatele **strategicky významných služeb**

- **Návrh nařízení vlády o nepominutelných funkcích**
 - Určuje klíčové funkce, které vždy podléhají prověřování dodavatelů, dosud nepřijato
- **Návrh nařízení vlády o strategicky významných službách**
 - Vymezuje služby, na které se vztahuje bezpečnostní prověřování dodavatelského řetězce, dosud nepřijato

SPECIFIKA ČESKÉ IMPLEMENTACE

Nové povinnosti nad rámec směrnice NIS2

- **Zohlednit bezpečnostní požadavky** již při výběru dodavatele a zavést je do smluv
- **Registrovat služby** u NÚKIB i mimo hlavní seznam
- **Umožnit přístup NÚKIB** k daňovým informacím o dodavatelích (přes GFŘ / GŘC)
- **Respektovat usnesení vlády** o zákazu nebo omezení dodavatelů
- **Vzdělávat vrcholový management** a posílit odpovědnost vedení za kybernetickou bezpečnost

Institut strategicky významných služeb

- Regulovaná služba, jejíž narušení může závažně ohrozit bezpečnost státu nebo vnitřní pořádek
- **Seznam určuje vláda ČR** formou nařízení:
 - služby považované za **strategicky významné**
 - tzv. **nepominutelné funkce**, které musí být chráněny vždy
- Povinnost poskytovatele strategicky významné služby:
 - **Prověřit bezpečnost dodavatelů a hlásit informace NÚKIB** do 1 roku od zařazení služby do seznamu
 - Zajistit provoz a dostupnost služby z území ČR

Povinnosti v řízení dodavatelského řetězce

- **Zavést procesy řízení rizik** v dodavatelském řetězci
- **Stanovit pravidla pro dodavatele** dle požadavků bezpečnostního řízení a zajistit jejich dodržování
- **Evidovat významné dodavatele** a písemně je o zařazení informovat
- **Provádět pravidelné přezkumy smluv** s důrazem na bezpečnostní opatření
- **Realizovat bezpečnostní audity:**
 - před uzavřením smlouvy
 - během celé doby spolupráce

DOPADY NA ODVĚTVÍ A VZTAH K DALŠÍM PRÁVNÍM PŘEDPISŮM

Dopady nové regulace a překryv s dalšími předpisy

- **Rozšiřuje působnost** o dosud neregulované sektory (výroba, pojišťovnictví, řízené IT služby, odpadové hospodářství)
- **Zpřísňuje požadavky** pro subjekty již regulované sektorově (banky, energetika), což vede k možné dvojí regulaci
- **Zavádí speciální pravidla** pro poskytovatele digitálních služeb dle prováděcích nařízení EK k NIS2
- **Překrývá se s dalšími regulacemi:**
 - DORA (finanční sektor)
 - CER směrnice (kritická infrastruktura)
 - GDPR (hlášení incidentů, zamezení dvojímu trestání)
 - Zákon o krizovém řízení

Směrnice CER

- směrnice o posílení odolnosti kritických subjektů (2022/2557)
 - Implementováno zákonem č. 266/2025 Sb. o kritické infrastruktuře
- stanoví kritické subjekty poskytující základní služby v 9 odvětvích (mj. doprava, energetika, bankovníctví, digitální infrastruktura)
- CER upravuje ochranu i vůči jiným hrozbám než jen kybernetickým:
 - tři prioritní oblasti: *připravenost, reakce a mezinárodní spolupráce*
- **povinný subjekt dle CER je automaticky pod NIS2** (např. některé dopravní podniky)

REGULOVANÉ SUBJEKTY

Regulované subjekty

		Příloha NIS2	
		I	II
Velikost organizace	Velká	ESSENTIAL	IMPORTANT
	Střední	IMPORTANT	IMPORTANT

- Dvě kategorie povinných osob:
 1. **Režim vyšších povinností / základní subjekty (*essential*)** - přísnější požadavky
 2. **Režim nižších povinností / důležité subjekty (*important*)** - mírnější požadavky
- Konkrétní kritéria pro identifikaci režimu povinností jsou stanoveny **v příloze vyhlášky o regulovaných službách** u každé jednotlivé regulované služby
- Rozdíl mezi nimi spočívá **v rozsahu bezpečnostních opatření, úrovni dohledu a pravidlech hlášení incidentů**
 - **Režim vyšších povinností:** Zahrnuje 25 bezpečnostních opatření (14 organizačních, 11 technických), včetně povinnosti jmenování specializovaných rolí (manažer kyberbezpečnosti, architekt, auditor).
 - **Režim nižších povinností:** Zahrnuje 13 základních bezpečnostních opatření.

Samoidentifikace a ohlašovací povinnost

- Posouzení dopadu nového zákona se provádí na základě samoidentifikace
- Subjekt posoudí:
 - zda poskytuje některou **z 104 regulovaných služeb v 22 regulovaných odvětvích**
 - zda splňuje **velikostní kritéria** (počet zaměstnanců, obrat)
 - Identifikuje režim povinností - nižší/vyšší podle vyhlášky
- Po identifikaci:
 - ohlašovací povinnost
 - **do 60 dnů od splnění kritérii** (u existujících subjektů půjde de facto o 60 dní od účinnosti zákona), a to
 - prostřednictvím **elektronického formuláře na Portálu NÚKIB**
- NÚKIB doručí rozhodnutí o registraci regulované služby
- Posouzení je **nutné pravidelně opakovat**

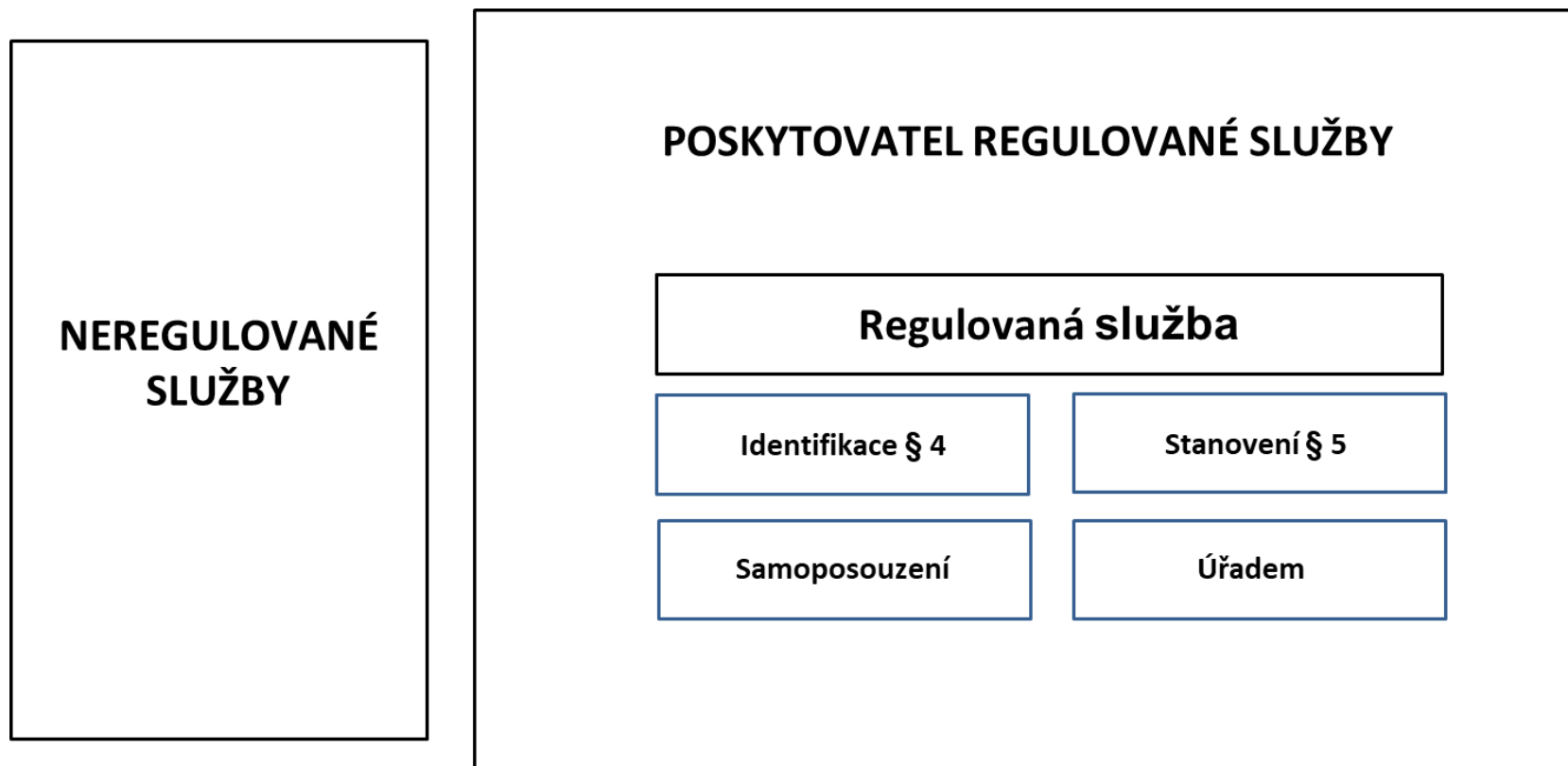
Kdy se subjekt stává regulovaným podle zákona?

Subjekt podléhá regulaci, pokud splňuje **všechny nebo některé z následujících podmínek:**

- **poskytuje regulovanou službu v jednom z regulovaných odvětví**
- **je dostatečně významný** – zejména kritérium velikost podniku
 - obvykle dle **kritéria středního podniku 50+ zaměstnanců a 10mio EUR+** roční obrat)
 - pozor na propojené podniky - velikostní kritéria se sčítají
- **vyjmenované subjekty** (bez ohledu na velikost podniku)
- **zvláštní subjekty určené členským státem**

Posouzení naplnění těchto kritérií musí každá organizace provést samostatně!

Určení povinných osob - shrnutí



POVINNOSTI POSKYTOVATELE REGULOVANÉ SLUŽBY

Povinnosti poskytovatele regulované služby

- V případě **všech poskytovatelů regulované služby**
- **0.** Ohlásit regulovanou službu
 - I. Hlásit kontaktní údaje
 - II. Stanovit rozsah řízení kybernetické bezpečnosti
 - III. Zavádět bezpečnostní opatření
 - IV. Hlásit kybernetické bezpečnostní incidenty
 - V. Informovat uživatele o incidentech a hrozbách
 - VI. Zavádět protiopatření vydaná Národním úřadem pro kybernetickou a informační bezpečnost
- V případě těch, kteří jsou zároveň tzv. poskytovateli **strategicky významné služby navíc**
 - VII. Mechanismus prověřování bezpečnosti dodavatelského řetězce
 - VIII. Zajištění dostupnosti strategicky významné služby
 - IX. Další specifická úprava u strategicky významné služby

II. Stanovení rozsahu řízení kybernetické bezpečnosti

- **Obecně vždy platí – pokud chcete něco skutečně řídit, musíte vědět, že to máte!**
- 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 aktivum = aktivum v podobě zpracovávané informace nebo poskytované služby*

III. 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) zvládnutí 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

III. Hlavní princip obou vyhlášek – přiměřenost

- „*pro stanovený rozsah systému řízení bezpečnosti informací na základě cílů systému řízení bezpečnosti informací, bezpečnostních potřeb a hodnocení rizik **zavede přiměřená bezpečnostní opatření.***“
 - § 3 písm. c) vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti

- „*zavede a provádí přiměřená bezpečnostní opatření směřující k zajištění kybernetické bezpečnosti regulované služby na základě cílů systému řízení bezpečnosti informací, bezpečnostních potřeb a řízení rizik* “
 - § 3 písm. c) vyhlášky o bezpečnostních opatřeních pro vyšší režim

- „*Povinná osoba při zajišťování kybernetické bezpečnosti*
 - 1) *zavede a provádí bezpečnostní opatření, která jsou přiměřená bezpečnostním potřebám, a*
 - 2) *zavede a provádí alespoň bezpečnostní opatření podle odstavců 2 až 6, § 4 až 6 a § 10.* “
 - § 3 odst. 1 vyhlášky o bezpečnostních opatřeních pro nižší režim

III. Bezpečnostní opatření - základní východiska

▪ Bezpečnostní opatření pro **nižší režim**

- Minimum – 8 stran, 16 paragrafů.
- Povinná osoba neprovádí hodnocení rizik ve smyslu současného znění vyhlášky o kybernetické bezpečnosti.
- Obsahuje přehled bezpečnostních opatření, které subjekt má povinnost zavést, pokud některé nemůže zavést – řádně zdůvodní a přijme jiné vhodné bezpečnostní opatření.
- Vhodné technické nástroje/prostředky – doména, firewall, detekce škodlivého kódu a zálohy.

▪ Bezpečnostní opatření pro **vyšší režim**

- Povinnosti vycházejí ze stávající vyhlášky o kybernetické bezpečnosti.
- Zavedení systému řízení bezpečnosti informací.
- Postaveno na standardu ISO 27001.

IV. 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

- 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)

VII. Bezpečnost dodavatelského řetězce

- Nová oblast, nevyplývá ze směrnice NIS2 ale z národního rozhodnutí
- Platí pouze pro vybrané organizace v režimu vyšších povinností (a to nikoli všechny)
- Organizace v rámci této povinnosti musí nahlásit dodavatele
- Budou prověřováni 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 dojít hned – počítá se s přechodnými lhůtami
- Hlášení dodavatelů do 1 roku od určení poskytovatele regulované služby
- Detail koho přesně se to týká – nařízení vlády o strategicky významných službách
- Jakých aktiv se to týká – Nařízení vlády o nepominutelných částech a těch s hodnocením kritická
- Proces hlášení dodavatelů poskytovatelem reg. služby – Vyhláška o Portálu NÚKIB

VIII. Zajištění dostupnosti strategicky významné služby

- 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.**

IX. Další specifická úprava u strategicky významné služby

- Opatření obecné povahy dle § 29 odst. 1 ZKB:

*„Úřad vydá **opatření obecné povahy**, kterým stanoví poskytovatelům strategicky významných služeb podmínky nebo zakáže využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu, **jestliže se vláda usnese**, že je takové opatření obecné povahy nutné z důvodu ochrany bezpečnosti České republiky nebo vnitřního pořádku.“*

- Nový zákonný důvod pro ukončení závazku zakotvuje v § 32 odst. 1 ZKB:

*„Poskytovatel strategicky významné služby může závazek ze smlouvy vypovědět, **nelze-li v jeho plnění pokračovat, aniž by bylo porušeno opatření obecné povahy podle § 29. [...]**“*

- Je možno využít tzv. blacklist dle ZZVZ?

Výše uvedené není výslovně provázáno s právní úpravou zadávání veřejných zakázek a není tedy zřejmé, jak s takovým dodavatelem naložit v rámci budoucích zadávacích řízení, nicméně lze uvažovat o aplikaci § 48 odst. 5 písm. d) ZZVZ: **„Zadavatel může vyloučit účastníka zadávacího řízení pro nezpůsobilost, pokud prokáže, že se účastník zadávacího řízení dopustil v posledních 3 letech od zahájení zadávacího řízení závažných nebo dlouhodobých pochybení při plnění dřívějšího smluvního vztahu se zadavatelem zadávané veřejné zakázky, nebo s jiným veřejným zadavatelem, která vedla k vzniku škody, předčasnému ukončení smluvního vztahu nebo jiným srovnatelným sankcím,“**

Příklady dopadů v praxi (včetně zadávání veřejných zakázek)

- Povinné smluvní podmínky
 - původně upraveny v Příloze č. 7 vyhlášky č. 82/2018 Sb.
 - převzato do nové právní úpravy:
 - 409/2025 Sb. – příloha č. 5 (vyšší povinnosti)
 - 410/2025 Sb. – příloha č. 2 (nižší povinnosti)

- Příklad – exit plán
 - je třeba reálně si představit jak bude probíhat, nikoliv pouze použít vzorový text
 - pouhá součinnost nestačí – co vše je potřeba? - aktualizace topologie sítě/kritických prvků, dokumentace, přístupových údajů a hesel, včetně jejich zabezpečeného předání
 - otázka náhrady nákladů za exit plán – součást ceny nebo hrazen samostatně?

- Kvalifikační předpoklady
 - certifikace dodavatele
 - osobní certifikace členů realizačního týmu
 - reference – významné zakázky – např. „bylo součástí plnění povinností významného dodavatele, bylo realizováno pro povinný subjekt dle ZKB apod.

- Hodnotící kritéria
 - např. zkušenosti členů realizačního týmu nad rámec kvalifikace
 - POZOR pouze nad rámec zákonných požadavků (!) – nízká cena a nedostatečná kyberbezpečnost

ROLE ÚŘADU

Role NÚKIB

- **Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)** = ústřední správní orgán pro oblast kybernetické bezpečnosti
- V institucionální architektuře nové právní úpravy vystupuje jako **hlavní veřejnoprávní autorita odpovědná za výkon státní správy v této oblasti**, a to jak ve vztahu k regulovaným subjektům, tak ve vztahu ke koordinaci státu při řešení závažných kybernetických incidentů a hrozeb.
- původně zřízen zákonem č. 205/2017 Sb. (změna zákona č. 181/2014 Sb.)
- Význam NÚKIB se v souvislosti s implementací směrnice NIS2 dále posiluje. Nový zákon z něj činí orgán, který není pouze metodickým nebo koordinačním centrem, ale současně:
 1. vykonává regulatorní dohled,
 2. rozhoduje o registraci regulovaných služeb,
 3. ukládá nápravná opatření,
 4. vydává výstrahy, varování a reaktivní protiopatření,
 5. a v případě porušení zákonných povinností ukládá správní sankce.
- NÚKIB plní také úkoly příslušného národního orgánu v rámci evropské architektury kybernetické bezpečnosti. Není tedy pouze vnitrostátním regulátorem, ale i článkem širšího evropského systému spolupráce.

Dozorové, kontrolní a sankční pravomoci

- **NÚKIB** vykonává dohled nad tím, **zda povinné subjekty**:
 - zavedly požadovaná bezpečnostní opatření,
 - plní oznamovací a informační povinnosti,
 - řádně hlásí kybernetické bezpečnostní incidenty,
 - dodržují pravidla týkající se řízení aktiv, rizik a dodavatelského řetězce, a zda jejich interní governance odpovídá požadavkům zákona.
- **Pravomoc ukládat nápravná opatření**
 - Zjistí-li NÚKIB porušení povinností nebo bezpečnostní nedostatky, může povinnému subjektu uložit nápravné opatření. Smyslem tohoto nástroje je odstranit nedostatky ještě předtím, než dojde k eskalaci situace nebo k uložení sankce. Nápravné opatření proto představuje klíčový mezistupeň mezi dohledem a sankcionováním.
- **Pravomoc vydávat výstrahy, varování a reaktivní protioopatření**
 - Nový ZoKB vybavuje NÚKIB možností reagovat nejen na již existující porušení povinností, ale i na bezprostředně hrozící nebo probíhající bezpečnostní rizika. Právě tato rovina dává NÚKIB silnou operativní funkci.
- **Sankční pravomoc**
 - V případě porušení povinností může NÚKIB ukládat správní pokuty, a to ve velmi významných částkách. Sankční pravomoc je jedním z nejvýraznějších prvků nové úpravy, protože dává zákonným povinnostem skutečnou vymahatelnost.

Kontrola vykonávaná Úřadem

- **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.

Protiopatření

- Nový ZoKB vybavuje NÚKIB možností reagovat nejen na již existující porušení povinností, ale i na bezprostředně hrozící nebo probíhající bezpečnostní rizika. Právě tato rovina dává NÚKIB silnou operativní funkci.

- Protiopatřeními jsou:
 1. **Výstraha** = nástroj, jehož prostřednictvím NÚKIB upozorňuje na skutečnosti relevantní z hlediska kybernetické bezpečnosti, zejména na incident, bezpečnostní problém nebo jinou okolnost vyžadující zvýšenou pozornost dotčených subjektů, má typicky **informativní a preventivní funkci**.
 2. **Varování** = protiopatření určené pro situace, kdy NÚKIB disponuje poznatky o závažné kybernetické hrozbě nebo zranitelnosti. Oproti výstraze má vyšší intenzitu a užší vazbu na konkrétní rizikový scénář.
 3. **Reaktivní protiopatření** = nástroj zásahové povahy, prostřednictvím něhož může NÚKIB uložit konkrétní opatření k řešení probíhajícího incidentu, k omezení jeho dopadů nebo k ochraně dotčených aktiv a služeb.

Přestupky a sankce

- Povinnosti v oblasti kybernetické bezpečnosti musí být **reálně vymahatelné**. Přestupky proto nejsou pojaty jen jako formální porušení regulačních pravidel, ale jako jednání, které může ohrozit bezpečnost regulované služby, její uživatele i širší veřejný zájem.
- Sankční odpovědnost dopadá především na **poskytovatele regulovaných služeb**, a to zejména při:
 1. nezavedení nebo neprovádění bezpečnostních opatření,
 2. nesplnění povinností při hlášení incidentů,
 3. nesplnění registračních a informačních povinností,
 4. neplnění uložených nápravných opatření nebo reaktivních protiopatření,
 5. porušení povinností souvisejících s bezpečností dodavatelského řetězce.
- Výše sankcí je odstupňována podle závažnosti porušení a podle režimu povinností. V nejzávažnějších případech může pokuta dosáhnout až **250 000 000 Kč** nebo **2 % čistého celosvětového ročního obratu**, podle toho, která hodnota je vyšší. Sankční rámec tak zjevně sleduje nejen represivní, ale i preventivní a odrazující účel.

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*

Odpovědnost statutárních orgánů

- Nový zákon o kybernetické bezpečnosti významně **posiluje vazbu mezi kybernetickou bezpečností a odpovědností vrcholného vedení společnosti.**
- Kybernetická bezpečnost je zde koncipována nikoli pouze jako technická nebo provozní otázka, ale jako **součást řádného řízení společnosti, řízení rizik a výkonu funkce statutárních orgánů.**
- Konkrétní povinnosti se liší podle režimu povinností poskytovatele regulované služby. V režimu nižších povinností musí vrcholné vedení zejména:
 1. určit osobu pověřenou řízením kybernetické bezpečnosti v organizaci,
 2. absolvovat školení v oblasti kybernetické bezpečnosti,
 3. zajišťovat dostupnost zdrojů potřebných pro zajišťování kybernetické bezpečnosti,
 4. seznamovat se stavem plnění bezpečnostních opatření,
 5. prosazovat neustálé zlepšování zajišťování kybernetické bezpečnosti, a stanovit prioritu obnovy primárních aktiv.
- V režimu vyšších povinností je výčet povinností vrcholového vedení obsažen v § 5 vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností.

Odpořednost statutárních orgánů

▪ Pozastavení výkonu řídící funkce

- (1) 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.**
- (2) Rozhodnutí podle odstavce 1 lze vydat pouze vůči osobě vykonávající funkci člena statutárního orgánu u poskytovatele regulované služby v režimu vyšších povinností, **a to jen ve vztahu k funkci, která není veřejnou funkcí vymezenou funkčním nebo časovým obdobím a obsazovanou na základě přímé nebo nepřímé volby anebo jmenováním podle jiného právního předpisu.**
- (3) Úřad vydá rozhodnutí o zrušení zákazu výkonu funkce, zjistí-li, že nedostatky byly odstraněny, nejdříve však po uplynutí doby podle odstavce 1.
- (...)
- (5) Je-li členem statutárního orgánu právnická osoba, použije se toto ustanovení i na fyzickou osobu, která tuto právnickou osobu při výkonu funkce zastupuje.
- (...)

PORTÁL.NUKIB.GOV.CZ

- Klíčová platforma pro kybernetickou bezpečnost
- Centralizovaný přístup k informacím a nástrojům pro regulované subjekty
- Komunikační kanál mezi regulovanými subjekty a NÚKIB
- Elektronické hlášení incidentů, registraci poskytovatelů regulovaných služeb a správu kontaktních údajů
- Aktuální informace o hrozbách, zranitelnostech a doporučeních pro zajištění kybernetické bezpečnosti
- Interaktivní nástroje, jako je kalkulačka pro určení regulované služby

ZÁVĚR

S čím můžeme pomoci?

- Školení pro řídicí osoby a zaměstnance
- Revize bezpečnostní dokumentace
- Revize smluvní dokumentace s dodavateli
- Komunikace s NÚKIB a zastupování v řízení před ním
- Koordinace technicko - právního přístupu ke kybernetické bezpečnosti s využitím osvědčených externích expertů
- Koordinace implementace projektů kybernetické bezpečnosti napříč více jurisdikcemi v EU
- Posuzování regulatorních dopadů nových řešení v kontextu nového zákona
- Právní asistence při řešení kybernetického incidentu

Děkujeme za pozornost!

Mgr. Pavel Amler

pavel.amler@havelpartners.cz

Mgr. Ondřej Dostál

ondrej.dostal@havelpartners.cz

Nejúspěšnější kancelář
v ČR a SR dle celkového
počtu nominací a titulů
(2008–2025)



Nejlepší advokátní kancelář
v České republice
(2018–2025)

LEXOLOGY INDEX

TOP 100 nejhodnotnějších
společností pod kontrolou
českých vlastníků
(2024, 2025)



Neprestížnější a nejznámější
značka mezi advokátními
kancelářemi v ČR
(2019–2023)



TOP Zaměstnavatelé
1. místo v kategorii
Advokátní kancelář v ČR
(2015–2025)



Hodnocení
nejvyšší důvěryhodnosti
a ekonomické stability
Dun & Bradstreet

