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

NÚKIB
Národní úřad pro kybernetickou a informační bezpečnost

Zdravotnické prostředky ČR
23. října 2025
TLP: CLEAR

Petra Lompejová
Oddělení regulace soukromého sektoru
Odbor regulace

Národní úřad pro kybernetickou a informační bezpečnost

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

Účinnost od **1. listopadu 2025**
9 prováděcích právních předpisů
stovky jednání
3 roky, 8 měsíců a 9 dní
(od přípravy po účinnost)

Východiska obsahu návrhu zákona

Národní úřad pro kybernetickou a informační bezpečnost

Směrnice NIS 2.0

Mechanismus BDŘ

Úkol z usnesení Bezpečnostní rady státu č. 41 ze dne 21. června 2022 k Bezpečnosti dodavatelských řetězců strategické infrastruktury státu, č. j. 28261/2022-UVCR

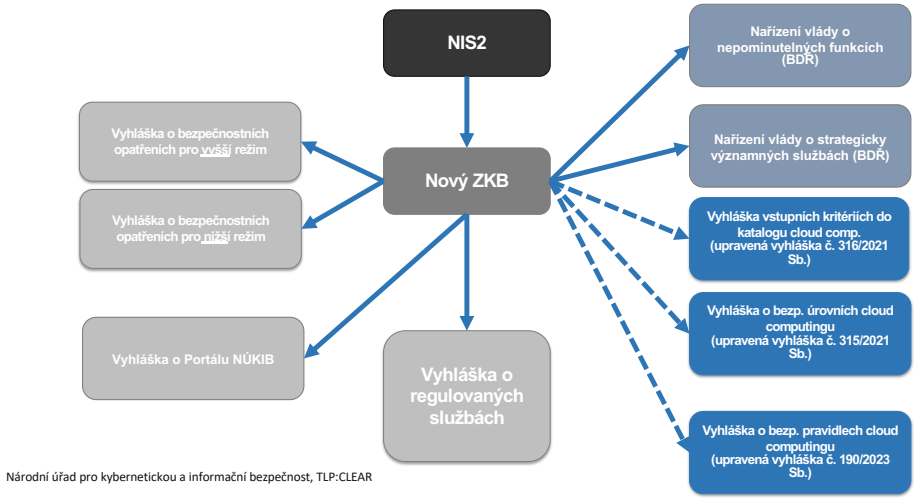
Zlepšení a zkušenosti

Reflexe poznatků a dosavadních zkušeností, odstranění současných nedostatků, zohlednění podnětů a připomínek a další doplňující úpravy

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 NÚKIB a regulovanými osobami, ale i mezi NÚKIB a dalšími orgány veřejné moci,
- **zvýšení pokut** a nové formy správního trestání,
- **nové požadavky na řešení problematiky bezpečnosti dodavatelského řetězce.**

Ekosystém ZKB – prováděcí předpisy



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** NÚKIB na základě kritéria pro určení regulované služby.
  - = **určení regulátorem**

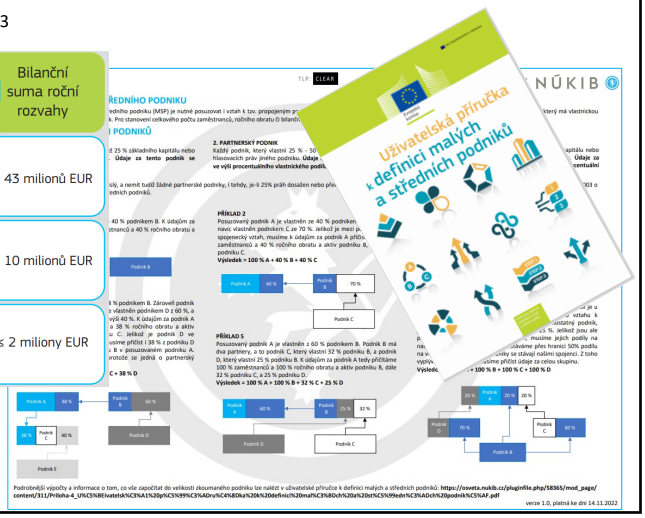
Samoidentifikace

- Střední nebo velký podnik
  - pro posouzení velikosti subjektu musí být naplněn zaměstnanecký nebo finanční ukazatel – počet zaměstnanců nebo rozvaha nebo obrat
  - střední podnik (nad 50 zaměstnanců/10 mil. EUR rozvaha/10 mil. EUR obrat)
  - velký podnik (nad 250 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
  - výjimky
    - DNS, registr internetových domén nejvyšší úrovně, veřejná správa, případně dle národní implementace
    - **ISP padají do regulace všichni** – jejich velikost má vliv na režim

Podmínky významnosti - velikost podniku

Doporučení Komise 2003/361/ES z 6. května 2003

Kategorie podniku	Počet zaměst-nanců: roční pracovní jednotka (RPJ)	Roční obrat nebo	Bilanční suma roční rozvahy
Střední podnik	< 250	≤ 50 milionů EUR	≤ 43 milionů EUR
Malý podnik	< 50	≤ 10 milionů EUR	≤ 10 milionů EUR
Mikropodnik	< 10	≤ 2 miliony EUR	≤ 2 miliony EUR



Zvláštní ustanovení o určování velikosti podniku

nZKB § 7 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.

Služby

Směrnice NIS1:
7 odvětví
Kritérium dopadu incidentu
- cca 400 povinných osob

Směrnice NIS2:
22 odvětví
Kritérium velikosti subjektu
- minimálně 6 000 povinných osob

SLUŽBY UVEDENÉ V PŘÍLOZE I

Subjekty poskytující služby uvedené v příloze I níže a splňující podmínku „velký podnik" dle doporučení Komise (EU) 2003/361/EC budou regulovány vždy v režimu „essential".

ENERGETIKA
Provozovatelé distribuční a přenosové soustavy, výrobci a prodejci elektrické energie, nominovaní organizátoři trhu s elektřinou, provozovatelé dobíjecích stanic spolu s poskytovateli elektromobility.
Subjekty poskytující službu dálkového vytápění nebo chlazení.
Provozovatelé ropovodů, zařízení na těžbu, rafinaci a zpracování ropy, skladovacích a přenosových zařízení, ústřední správci zásob.
Obchodníci s plynem, distributoři plynu, přepravci plynu, výrobci plynu a poskytovatelé uskladňování plynu.
Provozovatelé výroby, skladování a přepravy vodíku. Doposud však není implementováno do českého právního řádu.

DOPRAVA
Komerční letečtí dopravci, řídicí orgány letišť a subjekty provozující pomocná zařízení v rámci letišť, provozovatelé kontroly řízení provozu.
Provozovatel dráhy celostátní nebo regionální anebo veřejně přístupné vlečky a dopravce provozující na těchto drahách drážní dopravu.
Předmětné předpisy se vztahují na námořní přístavy a pro Českou republiku tedy nejsou relevantní.
Silniční orgány odpovědné za plánování, kontrolu a správu silnic spadajících do jejich územní působnosti, poskytovatelé služeb ITS.

BANKOVNICTVÍ
Sektor bankovnictví je regulován nařízením DORA.

INFRASTRUKTURA FIN. TRHŮ
Sektor infrastruktura finančních trhů je regulován nařízením DORA.

ZDRAVOTNICTVÍ
Poskytovatelé zdravotní péče (nemocnice a další), subjekty provádějící výzkum a vývoj léčivých výrobků a přípravků, výrobci základních farmaceutických přípravků.

PITNÁ VODA
Dodavatelé a distributoři vody určené k lidské spotřebě, avšak kromě těch, pro které je to vedlejší činnost k jejich hlavní činnosti zabývající se distribucí jiných komodit a zboží.

ODPADNÍ VODA
Subjekty shromažďující, vypouštějící nebo upravující městské nebo průmyslové odpadní vody nebo splašky, avšak kromě těch, pro které se jedná pouze o vedlejší činnost k jejich hlavní činnosti.

DIGITÁLNÍ INFRASTRUKTURA
Poskytovatelé: výměnných uzlů internetu (IXP), cloud computingu, datového centra, služeb vytvářejících důvěru, elektronických komunikací, CDN služeb, registrů TLD, služeb systému doménových jmen (DNS), s výjimkou poskytovatelů root name serverů .

POSKYTOVATELÉ ŘÍZENÝCH ICT SLUŽEB
Poskytovatelé řízených ICT služeb a poskytovatelé řízených ICT bezpečnostních služeb. Subjekty, pro zákazníky provozující či spravující ICT služby a nástroje, typicky na základě smlouvy o úrovni služeb (SLA).

VEŘEJNÁ SPRÁVA
Ústřední orgány státní správy, veřejná správa na regionální úrovni, soudy a státní zastupitelství a další instituce významné pro chod státu.

VESMÍR

SLUŽBY UVEDENÉ V PŘÍLOZE II

Subjekty poskytující služby uvedené v příloze I a splňující podmínku „střední podnik" a subjekty poskytující služby uvedené v příloze II a splňující podmínku „velký podnik" a „střední podnik" dle doporučení Komise (EU) 2003/361/EC budou regulovány v režimu „important" (nižší nároky z hlediska bezpečnostních opatření), pokud nebude stanoveno speciálními kritérii jinak.

POŠTOVNÍ SLUŽBY
Subjekty, poskytující poštovní služby, tzn. výběr, třídění, přepravu a dodání poštovních zásilek, včetně provozovatelů kurýrních služeb.

ODPADNÍ HOSPODÁŘSTVÍ
Subjekty, poskytující službu nakládání s odpady, tzn. zařízení určená pro nakládání s odpady, obchodníci, zprostředkovatelé, dopravci podle zákona č. 541/2020 Sb., kromě těch, pro které nakládání s odpady není jejich hlavní ekonomickou činností.

CHEMICKÝ PRŮMYSL
Subjekty, poskytující služby v chemickém průmyslu, tzn. výrobci, distributoři, včetně maloobchodníka, který skladuje a uvádí na trh chemickou látku nebo předmět.

POTRAVINÁŘSTVÍ
Potravinářské subjekty, které se zabývají velkoobchodní distribucí a průmyslovou výrobou nebo zpracováním.

VÝROBA
Výroba: zdravotnických a diagnostických zdravotnických prostředků, počítačů, elektronických a optických přístrojů, elektrických zařízení, strojů a zařízení, motorových vozidel (kromě motocyklů), přívěsů a návěsů, ostatních dopravních prostředků a zařízení.

POSKYTOVATELÉ DIGI SLUŽEB
Poskytovatelé on-line tržišť, internetových vyhledávačů, platforem služeb sociálních sítí.

VÝZKUM
Výzkumné organizace, s výjimkou vzdělávacích institucí, jejichž hlavním cílem je provádět aplikovaný výzkum nebo experimentální vývoj s ohledem na využití výsledků tohoto výzkumu pro komerční účely.

Podmínky významnosti

18.7 Výroba zdravotnických prostředků podle přímo použitelného předpisu Evropské unie[46)]	Výrobce zdravotnických prostředků podle přímo použitelného předpisu Evropské unie[46)] je poskytovatelem regulované služby v režimu nižších povinností v případě, že je velkým podnikem, nebo středním podnikem.
18.8 Výroba diagnostických zdravotnických prostředků in vitro podle přímo použitelného předpisu Evropské unie[47)]	Výrobce diagnostických zdravotnických prostředků in vitro podle přímo použitelného předpisu Evropské unie[47)] je poskytovatelem regulované služby v režimu nižších povinností v případě, že je velkým nebo středním podnikem.
18.9 Výroba zdravotnických prostředků považovaných za kriticky důležité v případě mimořádné situace v oblasti veřejného zdraví podle přímo použitelného předpisu Evropské unie[48)]	Výrobce zdravotnických prostředků uvedených na seznamu kriticky důležitých zdravotnických prostředků při mimořádné situaci v oblasti veřejného zdraví podle přímo použitelného předpisu Evropské unie[48)] je I. poskytovatelem regulované služby v režimu vyšších povinností v případě, že je velkým podnikem, nebo II. poskytovatelem regulované služby v režimu nižších povinností v případě, že je středním podnikem.

Určení ze strany NÚKIB

§ 5 nZKB

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.

Regulovaná služba a její režim

Strategicky významná služba – specialita vyššího režimu

Vyhláška o regulovaných službách

§ 5

Regulované služby splňující podmínky strategicky významné služby

(1) Strategicky významnou službou v odvětví veřejná správa je
   a) výkon svěřených pravomocí vykonávaný orgánem nebo osobou uvedenou v příloze k této vyhlášce v odvětví 1. Veřejná správa, služby 1.1. Výkon svěřených pravomocí, bod I. písm. a) až k).

(2) Strategicky významnou službou v odvětví energetika je
   a) výroba elektřiny v rámci výrobny s celkovým instalovaným elektrickým výkonem nejméně 100 MW vykonávaná držitelem licence na výrobu elektřiny podle energetického zákona,
   b) provoz přenosové soustavy elektřiny vykonávaný držitelem licence na přenos elektřiny podle energetického zákon,
   c) provoz distribuční soustavy elektřiny v rámci celé distribuční soustavy elektřiny s přenosovou kapacitou nejméně 220 MW vykonávaný držitelem licence na distribuci elektřiny podle energetického zákona,

   - ….

Pro tyto služby platí ještě **mechanismus bezpečnosti dodavatelského řetězce** a **zajištění dostupnosti**

Nebudou definovány ve vyhlášce ale v nařízení vlády

Povinnosti poskytovatele regulované služby

Hlavní povinnosti vyplývající ze zákona

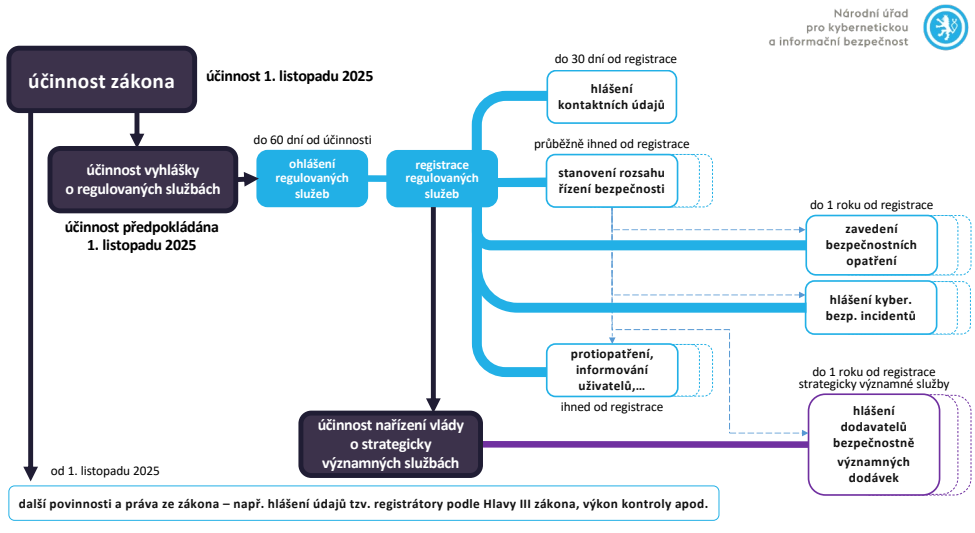
V případě **všech poskytovatelů regulované služby**

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 NÚKIB

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

VII. Mechanismus prověřování bezpečnosti dodavatelského řetězce
VIII. Zajištění dostupnosti strategicky významné služby

Do kdy co plnit?



I. 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 upraveno vyhláškou o portálu NÚKIB
  - 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)

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 jsou pak plněny povinnosti ze zákona.
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) 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 …**“*

Bezpečnostní opatření v nižším povinnostním režimu

Bezpečnostní opatření – nižší režim:
1. zajišťování kybernetické bezpečnosti,
2. požadavky na vrcholné 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.

- stanovení rozsahu řízení kybernetické bezpečnosti
- zpracování přehledu bezpečnostních opatření
- pravidla pro používání a manipulaci technických aktiv = politiky a dokumentace
- určení osoby pověřené řízením a rozvojem kybernetické bezpečnosti
- stanovení politiky bezpečného chování uživatelů
- vstupní školení v oblasti kybernetické bezpečnosti
- zajištění hlášení neobvyklého chování technických aktiv a podezření na zranitelnosti

IV. Hlášení kybernetických bezpečnostních incidentů

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

- v rámci stanoveného rozsahu
- hlásit NÚKIB
- 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

Pokud významný dopad
- no 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

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 ostatních dalších služeb takového poskytovatele se však prováděcí nařízení Komise nepoužije!

V. 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.
- NÚKIB může poskytovateli regulované služby uložit povinnost nebo zákaz informovat uživatele regulované služby o tomto incidentu.

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.**

VI. Protiopatření

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

Výstraha

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

Varování

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

VII. Bezpečnost dodavatelského řetězce

- 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

- 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

VIII. Zajištění dostupnosti strategicky významných regulovaných 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 BCM,
  - úroveň služby může být snížena – míru snížení si definuje sám poskytovatel v BCM,
  - rozsah služby může je dle připomínek subjektů nutno omezit/definovat, aby byla právní jistota.

- 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,
  - zajištění služby může být i mimo ICT, např. náhradním postupem fyzicky - pokud to splní stanovený rozsah a kvalitu.

Jak se na zákon připravit?

Přehled v organizaci
- Mé agendy/služby, co poskytuji
- Co pro to potřebuji?
- Z toho vyplývá rozsah, ve kterém KB řeším.

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

Určení priorit
- Jaké mám kapacity?
- Co je má prioritní služba?
- Provedu analýzy, stanovím plán se zohledněním kapacit a priorit.

Zavádění opatření
- Určím odpovědné osoby.
- Priorita je vzdělávání zaměstnanců včetně vedení.
- Pokračuji dle plánu.

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

Národní úřad pro kybernetickou a informační bezpečnost, TLP:CLEAR

Bezpečnostní opatření: nižší režim povinností

Národní úřad pro kybernetickou a informační bezpečnost

Stanovení rozsahu řízení kybernetické bezpečnosti

Povinná základní bezpečnostní opatření
§ 3, § 4, §, 5, § 6 a § 10

např. dokumentace, odpovědná osoba a vrcholné vedení, lidské zdroje, smlouvy s dodavateli, kontinuita činností, incidenty

Přiměřeně zaváděná bezpečnostní opatření
§ 7, § 8, § 9, § 11, § 12 a § 13

např. vícefaktorová autentizace, přístupová práva, fyzická bezpečnost, aktualizace, skenování zranitelností, segmentace sítě, firewall, VPN, kryptografie

Národní úřad pro kybernetickou a informační bezpečnost, TLP: CLEAR

Kde najít další informace?

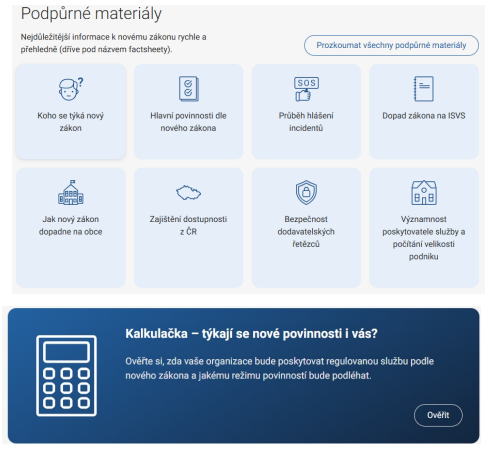
Portál NÚKIB

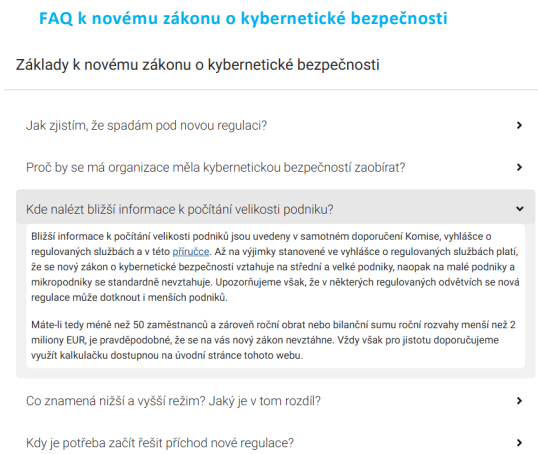
https://portal.nukib.gov.cz/

Hlavní komunikační platforma týkající se nového ZKB

- Podpůrné materiály
- Aktuality
- Otázky & odpovědi

Portál NÚKIB





NCC-CZ CZECHIA CYBERSECURITY COORDINATION CENTRE

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Financováno Evropskou unií

Projekt TEST-CERT-CZ

CyberCertification Boost:
Podpora rozvoje certifikačních kapacit v oblasti kybernetické bezpečnosti

V pondělí 15. září byla spuštěna Třetí výzva NKC na podporu aktivit pod Cyber Resilience Act, přihlášky přijímáme do 18. listopadu 2025. Alokováno je 8 miliónů Kč a získat můžete kofinancování do výše 50 %.

Kontakt: ncc@nukib.gov.cz
Odborný garant: simona.vysatova@nukib.gov.cz

Supported by the Digital Europe Programme within the **Building Testing and Certification Capabilities in the Czech Republic** (TEST-CERT-CZ, no. 101127940).

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

Děkuji za pozornost

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

regulace@nukib.gov.cz