Nový zákon o kybernetické bezpečnosti

Novinky a aktuální stav

NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

21. listopadu 2023
TLP: CLEAR

Vladěna Sasková
oddělení regulace soukromého sektoru

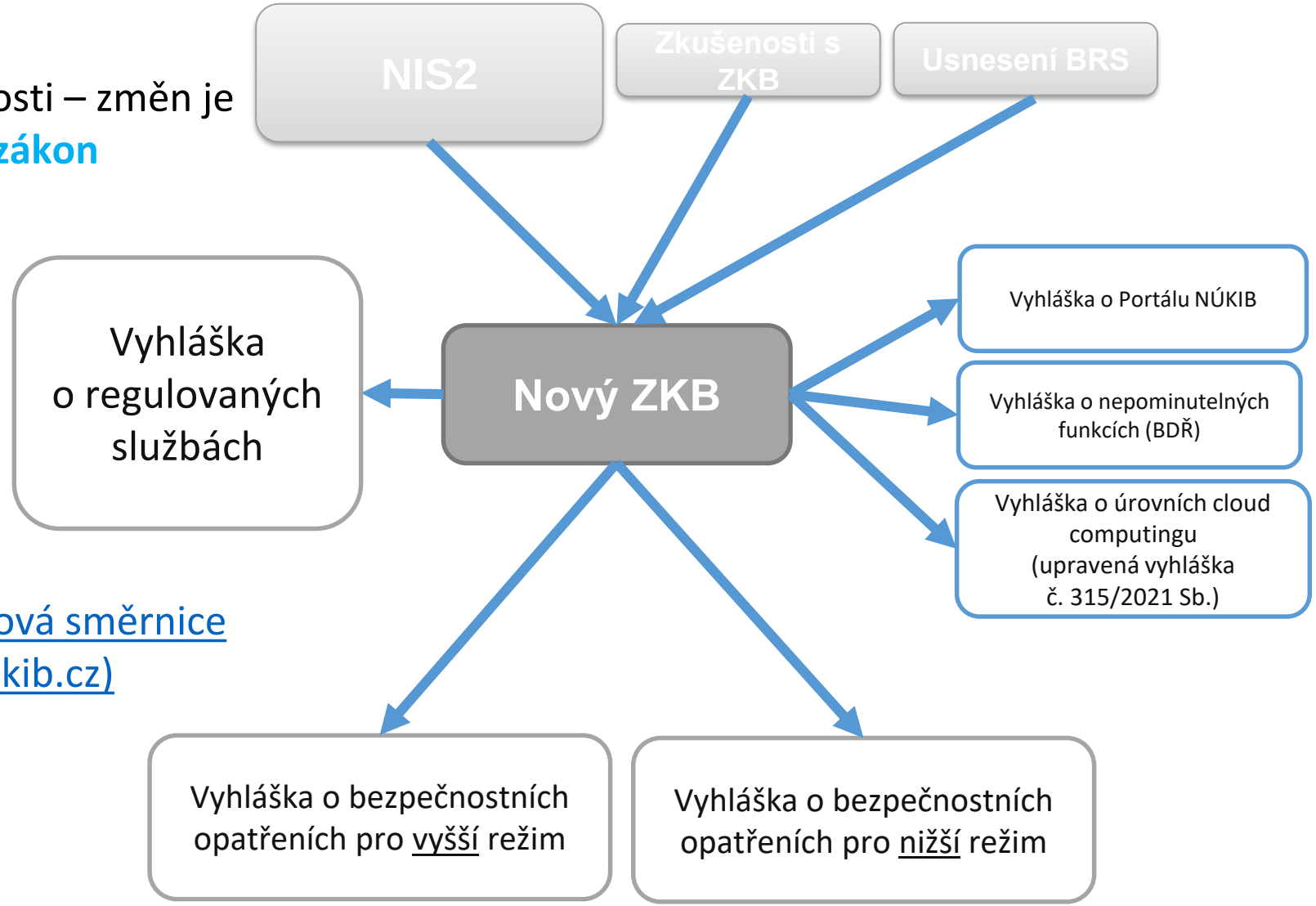
Nový zákon o kybernetické bezpečnosti (nZKB) v MPŘ

Nový zákon o kybernetické bezpečnosti – změn je tolik, že bylo **potřeba vytvořit nový zákon**

= zcela nová úprava – cca 70 paragrafů

Verze v mez. připomínkovém řízení má aktuálně navíc **6 vyhlášek.**

Celý návrh zveřejněn zde: Course: Nová směrnice EU o bezpečnosti sítí a informací (nukib.cz)



nZKB – hlavní body

Nový zákon dopadne na minimálně 6 000 organizací

- jde téměř výhradně o požadavek směrnice
- reguluje **107 služeb v 22 odvětvích** (energetika, zdravotnictví, bankovnictví, doprava, veřejná správa, digitální infrastruktura,…)
- hlavním kritériem pro zahrnutí do regulace je **velikost subjektu** (daná počtem zaměstnanců nebo jeho finanční situací)
- mění se také přístup k rozsahu regulace – **nevybírají se konkrétní systémy, ale celé služby**
- do regulace se nově navrhuje **zařadit obce (ORP)**

Regulované organizace zákon nově označuje jako **tzv. poskytovatele regulované služby** a rozděluje je do **dvou režimů – nižších povinností a vyšších povinností**

- podle režimu mají stanovené povinnosti

Vznikají úplně nové instituty

- zajištění dostupnosti regulované služby nebo mechanismus prověřování bezpečnosti dodavatelského řetězce

Mění se některé stávající instituty

- stav kybernetického nebezpečí, (proti)opatření, konkrétní lhůty pro hlášení incidentů, sankce,…

Komunikace návrhů a zapojení veřejnosti

V srpnu 2022 spuštěn **informační web věnovaný směrnici NIS2 a nové regulaci**

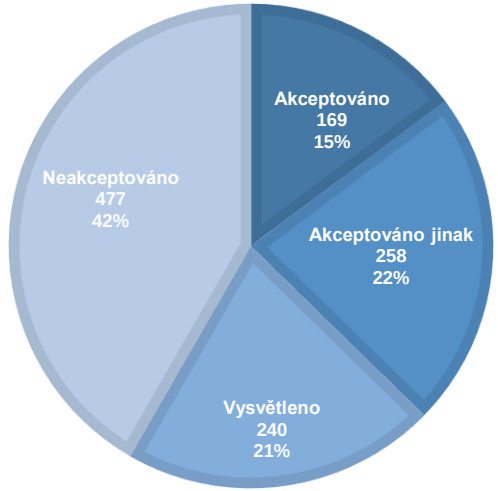
Nová směrnice EU o bezpečnosti sítí a informací (nukib.cz)*

Představení problematiky na desítkách konferencí a bilaterálních jednání se zástupci úřadů a soukromého sektoru

Osloveno a komunikováno **s více než 28 svazy, oborovými sdruženími a komorami**

Veřejná konzultace a zveřejnění prvotních návrhů ZKB pro podněty veřejnosti

- zahájeno 26. ledna 2023 a ukončeno 12. března 2023
- NÚKIB obdržel 1144 jedinečných podnětů (od 117 jednotlivých míst)
- zohledněno 58 % z nich
- 100 % autorů informováno o způsobu vypořádání



Veřejné konzultace – hlavní změny

- Formulační změny, zpřehlednění a zpřesnění textu
- Nastavení inspektorů → **zrušení institutu inspektorů**
- Obsah vyhlášky o bezpečnostních opatřeních pro režim nižších povinností

  → **zeštíhlení, zjednodušení – do MPŘ byla následně předložena zcela přepracovaná verze**
- Lokalizace informací a dat při zpracování v zahraničí → **zcela přepracováno, nově zajištění dostupnosti strategicky významných služeb z České republiky**
- Určovací a identifikační kritéria ve vyhlášce → **přesun určovacích kritérií, určení změny režimu do zákona a výčet odvětví pro identifikaci přímo v zákoně**
- Zákon rozdělen na dva → **hlavní zákon a změnový zákon (měnící jiné předpisy)**
- Dílčí změny v mechanismu prověřování bezpečnosti dodavatelského řetězce
- Stav kybernetického nebezpečí → **koncepční změny, provázání s krizovým řízením**

Mezirezortní připomínkové řízení

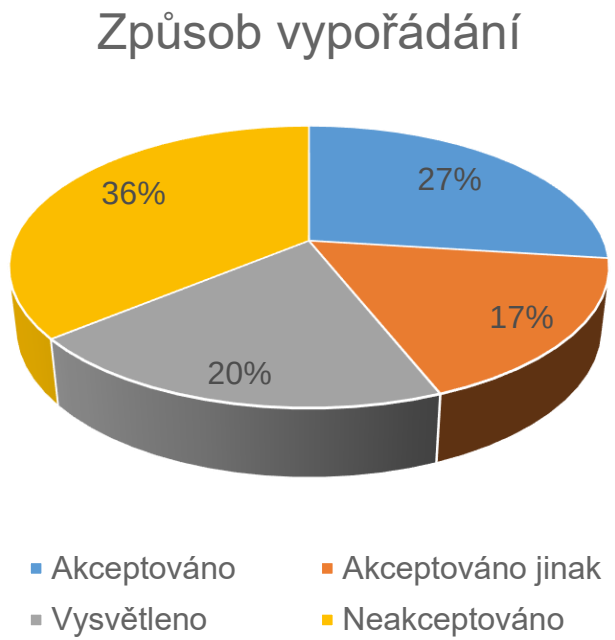
Oficiální mezirezortní připomínkové řízení bylo zahájeno 19. června 2023 a ukončeno 26. července 2023 (původní lhůta na připomínky stanovená do 19. července byla prodloužena)

NÚKIB obdržel vyšší stovky připomínek

- připomínky zaslalo **41 řádných připomínkových míst**
- dalších **11 organizací zaslalo své připomínky i bez toho, aby byli osloveni** (ale jejich připomínky byly také přijaty a řešeny)
- Připomínky vypořádány písemně + další jednání

Nejčastější připomínkované oblasti

- legislativně-technické úpravy, obsah doprovodných materiálů, definice apod.
- mechanismus bezpečnosti dodavatelského řetězce a zajištění dostupnosti strategicky významné služby
- nastavení vztahu zákon – vyhlášky
- pravomoci Úřadu a Národního CERT
- stav kybernetického nebezpečí



MPŘ – hlavní změny

- Formulační změny, zpřehlednění a zpřesnění textu
- Změna v regulaci poskytovatelů digitálních služeb (viz dále)
- Zajištění poskytování strategicky významné služby z ČR – nově jen **v nezbytném rozsahu** (stanoví vyhláška) a **ve stanoveném čase a kvalitě** (stanoví poskytovatel)
- Registrace a evidence poskytovatele → **registrace a evidence regulované služby**
- Dílčí změny v mechanismu prověřování bezpečnosti dodavatelského řetězce – **řeší se** zapojení regulátora, životní cyklus technologií, zapojení BRS
- Stav kybernetického nebezpečí – **náhrada škody** provázána s krizovým zákonem

MPŘ – hlavní změny

Zásadní změna pro poskytovatele služeb v odvětví digitální infrastruktury

Poskytovatelé

- služby systému překladu jmen domén
- služby vytvářející důvěru
- služby správy a provozu registru domén 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

→ **Bezpečnostní opatření podle prováděcího předpisu Evropské komise**

MPŘ – hlavní změny

Zásadní změna pro poskytovatele služeb v odvětví digitální infrastruktury

Poskytovatelé

- služby systému překladu jmen domén
- ~~služby vytvářející důvěru~~
- služby správy a provozu registru domén 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

Významné incidenty identifikované podle pravidel prováděcího předpisu Evropské komise

nZKB – aktuální podoba

Hlavní povinnosti poskytovatelů regulovaných služeb

- hlásit kontaktní a další údaje
- stanovit rozsah řízení kybernetické bezpečnosti – definuje rozsah regulace v organizaci
- zavádět bezpečnostní opatření – podle režimu v kterém je služba určena (vyšší/nižší)
- hlásit kybernetické bezpečnostní incidenty – podle režimu v kterém je služba určena (vyšší/nižší)
- informovat zákazníky o incidentech a hrozbách
- provádět protiopatření
- plnit povinnosti z tzv. Mechanismu bezpečnosti dodavatelského řetězce u vybraných (strategicky významných) služeb
- zajistit dostupnost z České republiky u vybraných (strategicky významných) služeb

Zákon dále upravuje další oblasti nezbytné pro fungování regulatorního rámce

- specifické situace – poskytování informací, stav kybernetického nebezpečí
- úprava institucí – NÚKIB, CERT a jejich pravomoci, součinnost dalších orgánů státu
- sankce – přestupky, úprava horních limitů sankcí

nZKB – další předpokládané kroky

Legislativní rada vlády – prosinec 2023

Poslanecká sněmovna, Senát, prezident – 1Q 2024

Vydání zákona říjen 2024 (konec transpoziční lhůty)

Vyhlášky budou mít samostatný legislativní proces, který bude spuštěn v roce 2024

Regulovaná služba a její režim

Regulovanou službou je služba

- **naplňující** alespoň jedno **kritérium pro identifikaci** regulované služby **podle vyhlášky o regulovaných službách (objektivní naplnění kritérií)**

nebo

- **určená rozhodnutím NÚKIBu** na základě **kritéria pro určení** regulované služby

Režim poskytovatele regulované služby stanovuje **míru jemu uložených povinností** (tzn. dvojrychlostní kybernetická bezpečnost).

Režim poskytovatele regulované služby je stanoven vyhláškou o regulovaných službách, s výjimkou služeb určených NÚKIBem, pak je režim jejího poskytovatele vždy režimem vyšších 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 (jednotnost).

Povinné osoby – odvětví, služby

- Vše podle NIS2
- Nad rámec požadavků NIS2
  - Vybrané subjekty v odvětví letectví – po konzultaci s ÚCL
  - Vybrané subjekty v oblasti výzkumu a vývoje (nekomerční užití, veřejné financování, citlivá činnost, velké výzkumné infrastruktury; vysoké školy)
  - Vojenský průmysl – vojenský materiál, zboží a technologie dvojího užití
  - Vybrané instituce veřejné správy
- Celkem 107 služeb v 22 odvětvích (mírně odlišná taxonomie než NIS2)

Kritéria pro identifikaci regulované služby – NIS2

3. Výroba, produkce a distribuce chemických látek		podniky provádějící výrobu látek a distribuci látek nebo směsí ve smyslu čl. 3 bodů 9 a 14 nařízení Evropského parlamentu a Rady (ES) č. 1907/2006 ([2]) a podniky provádějící výrobu předmětů ve smyslu čl. 3 bodu 3 uvedeného nařízení z látek či směsí

([2]) Nařízení Evropského parlamentu a Rady (ES) č. 1907/2006 ze dne 18. prosince 2006 o registraci, hodnocení, povolování a omezování chemických látek (REACH), o zřízení Evropské agentury pro chemické látky, o změně směrnice 1999/45/ES a o zrušení nařízení Rady (EHS) č. 793/93, nařízení Komise (ES) č. 1488/94, směrnice Rady 76/769/EHS a směrnic Komise 91/155/EHS, 93/67/EHS, 93/105/ES a 2000/21/ES (Úř. věst. L 396, 30.12.2006, s. 1).

1. Pro účely této směrnice se za základní subjekty považují:

a) subjekty, jejichž druh je uveden v příloze I, které překračují stropy pro střední podniky stanovené v čl. 2 odst. 1 přílohy doporučení 2003/361/ES;

b) kvalifikovaní poskytovatelé služeb vytvářejících důvěru, registry domén nejvyšší úrovně a provozovatelé DNS bez ohledu na jejich velikost;

c) poskytovatelé veřejných sítí elektronických komunikací nebo veřejně dostupných služeb elektronických komunikací, kteří jsou považováni za střední podniky podle článku 2 přílohy doporučení 2003/361/ES;

d) subjekty veřejné správy podle čl. 2 odst. 2 písm. f) bodu i);

e) jakékoli jiné subjekty druhu, který je uveden v příloze I nebo II, jež členský stát označí za základní subjekty podle čl. 2 odst. 2 písm. b) až e);

f) subjekty určené jakožto kritické subjekty podle směrnice (EU) 2022/2557, jež jsou uvedeny v čl. 2 odst. 3 této směrnice;

g) pokud tak členský stát stanoví, subjekty, které tento členský stát označil před 16. lednem 2023 za provozovatele základních služeb v souladu se směrnicí (EU) 2016/1148 nebo s vnitrostátním právem.

2. Pro účely této směrnice se za důležité subjekty považují subjekty druhu uvedeného v příloze I nebo II, které nelze považovat za základní subjekty podle odstavce 1 tohoto článku. Patří k nim i subjekty, jež členské státy označily za důležité podle čl. 2 odst. 2 písm. b) až e).

Kritéria pro identifikaci regulované služby - nZKB

9. Chemický průmysl

Regulovaná služba	
Služba	**Kritérium poskytovatele regulované služby a jeho režim pro tuto službu**
9.1. Výroba nebezpečných chemických látek, směsí nebo přípravků nebo látky	Výrobce nebezpečných chemických látek, směsí nebo přípravků nebo látky podle přímo použitelného předpisu Evropské unie[5] je I. poskytovatel regulované služby v režimu vyšších povinností v případě, že je provozovatelem nebo uživatelem objektu zařazeného do skupiny B podle zákona o prevenci závažných havárií, II. poskytovatel regulované služby v režimu nižších povinností v případě, že a) je velkým podnikem, b) je střední podnikem, nebo c) je provozovatelem nebo uživatelem objektu zařazeného do skupiny A podle zákona o prevenci závažných havárií.
9.2. Zpracování nebezpečných chemických látek, směsí nebo přípravků nebo látky	Zpracovatel nebezpečných chemických látek, směsí nebo přípravků nebo látky podle přímo použitelného předpisu Evropské unie[6] je I. poskytovatel regulované služby v režimu vyšších povinností v případě, že je provozovatelem nebo uživatelem objektu zařazeného do skupiny B podle zákona o prevenci závažných havárií, II. poskytovatel regulované služby v režimu nižších povinností v případě, že a) je velkým podnikem, b) je střední podnikem, nebo c) je provozovatelem nebo uživatelem objektu zařazeného do skupiny A podle zákona o prevenci závažných havárií.
9.3. Skladování nebo distribuce nebezpečných chemických látek, směsí nebo přípravků nebo látky	Distributor nebo osoba skladující nebezpečné chemické látky, směsi nebo přípravky nebo látky podle přímo použitelného předpisu Evropské unie[7] je I. poskytovatel regulované služby v režimu vyšších povinností v případě, že je provozovatelem nebo uživatelem objektu zařazeného do skupiny B podle zákona o prevenci závažných havárií, II. poskytovatel regulované služby v režimu nižších povinností v případě, že a) je velkým podnikem, b) je střední podnikem, nebo c) je provozovatelem nebo uživatelem objektu zařazeného do skupiny A podle zákona o prevenci závažných havárií.
9.4. Výroba předmětů uvedených v čl. 3 bodě 3 přímo použitelného předpisu Evropské unie[8] z látek nebo směsí	Výrobce předmětů podle přímo použitelného předpisu Evropské unie[9] z látek nebo směsí je I. poskytovatel regulované služby v režimu vyšších povinností v případě, že je provozovatelem nebo uživatelem objektu zařazeného do skupiny B podle zákona o prevenci závažných havárií, II. poskytovatel regulované služby v režimu nižších povinností v případě, že a) je velkým podnikem, b) je střední podnikem, nebo c) je provozovatelem nebo uživatelem objektu zařazeného do skupiny A podle zákona o prevenci závažných havárií.

Kritéria pro určení regulované služby

§ 5

Kritéria pro určení regulované služby

1) Regulovanou službou je dále služba určená orgánu nebo osobě rozhodnutím Úřadu v případě, že
   a) jde o službu uvedenou ve vyhlášce Úřadu stanovující kritéria pro identifikaci regulovaných služeb a
      1. orgán nebo osoba je jediným poskytovatelem této služby v České republice a tato služba je zásadní pro zachování nezbytných společenských nebo ekonomických činností v České republice,
      2. narušení této služby by mohlo mít významný dopad na bezpečnost České republiky, vnitřní či veřejný pořádek nebo veřejné zdraví,
      3. narušení této služby by mohlo vyvolat významná systémová rizika, zejména v odvětvích, kde by takové narušení mohlo mít přeshraniční dopad, nebo
      4. orgán nebo osoba je kvůli svému specifickému významu na regionální nebo celostátní úrovni zásadní pro konkrétní odvětví nebo typ služby nebo pro jiná vzájemně propojená odvětví v České republice,
   b) její narušení může způsobit závažný zásah do života postihující více než 125 000 osob, a to prostřednictvím ohrožení života, zdraví, majetkové hodnoty, vnitřního či veřejného pořádku, bezpečnosti nebo životního prostředí,
   c) její narušení může způsobit závažný zásah do schopnosti poskytovat jinou regulovanou službu stejného nebo jiného poskytovatele regulované služby v režimu vyšších povinností, nebo
   d) orgán nebo osoba 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.

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	nebo	≤ 43 milionů EUR
Malý podnik	< 50	≤ 10 milionů EUR	nebo	≤ 10 milionů EUR
Mikropodnik	< 10	≤ 2 miliony EUR	nebo	≤ 2 miliony EUR

TLP: CLEAR

ŘEDNÍHO PODNIKU

PODNIKŮ

2. PARTNERSKÝ PODNIK

3. SPOJENÝ

PŘÍKLAD 2

PŘÍKLAD 3

PŘÍKLAD 5

PŘÍKLAD 6

Dostupné z: [Uživatelská příručka k definici malých a středních podniků (nukib.cz)](), [2022-11-14_Pocitani-velikosti-podniku_Zjednodusene_v1.0_final.pdf (nukib.cz)]()

Hlavní povinnosti poskytovatele regulované služby

Registrovat regulovanou službu

Hlásit kontaktní a další údaje

Stanovit rozsah řízení kybernetické bezpečnosti

Zavádět bezpečnosti opatření

- Vyšší režim
- Nižší režim

Hlášení kybernetických bezpečnostních incidentů

- Vyšší režim
- Nižší režim

Protiopatření

- Výstraha, varování, reaktivní opatření

Informační povinnost poskytovatele regulované služby

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 je oprávněn poskytovateli regulované služby uložit povinnost informovat uživatele regulované služby o tomto incidentu.

Poskytovatel regulované služby je **povinen** bez zbytečného odkladu vhodným a srozumitelným způsobem **informovat uživatele regulované služby**, který může být ovlivněn významnou hrozbou, **o takových krocích, které může uživatel učinit v reakci na tuto hrozbu, aby byl případný dopad její realizace na tohoto uživatele co nejmenší**.

Lhůty pro plnění povinností

Registrovat regulovanou službu

→ **Do 30, resp. 90 dnů od naplnění identifikačních kritérií**

Hlásit kontaktní a další údaje

→ **Do 30 dnů (nové), resp. 15 dnů (změny)**

Stanovit rozsah řízení kybernetické bezpečnosti

→ **Kdykoli (ALE do doby stanovení je rozsahem celá organizace)**

Zavádět bezpečnosti opatření

- Vyšší režim
- Nižší režim

→ **Do 1 roku od vyrozumění od zařazení do evidence**

Hlášení kybernetických bezpečnostních incidentů

- Vyšší režim
- Nižší režim

→ **Do 1 roku od vyrozumění od zařazení do evidence**

Protiopatření

- Výstraha, varování, reaktivní opatření

→ **Ihned (lhůty v protiopatření)**

Informační povinnost poskytovatele regulované služby

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 je oprávněn poskytovateli regulované služby uložit povinnost informovat uživatele regulované služby o tomto incidentu.

Poskytovatel regulované služby je **povinen** bez zbytečného odkladu vhodným a srozumitelným způsobem **informovat uživatele regulované služby**, který může být ovlivněn významnou hrozbou, **o takových krocích, které může uživatel učinit v reakci na tuto hrozbu, aby byl případný dopad její realizace na tohoto uživatele co nejmenší**.

→ **Ihned (ALE vychází z bezpečnostních opatření a hlášení incidentů)**

Povinnosti vyplývající z národních potřeb

Mechanismus prověřování dodavatelského řetězce

- Cíl = stát musí mít mechanismus jak **řešit závislost na nedůvěryhodných dodavatelích** (projev národní suverenity)
- platí **pouze pro vybrané organizace v režimu vyšších povinností (a to nikoli všech)**
- **budou prověřováni dodavatelé do kritické části systému** = aktiva s hodnotou 3 a 4 (vysoká/kritická), kteří dodávají bezpečnostně významnou dodávku = má výpočetní kapacitu
- **stát prověří to, zda dodavatel není hrozbou pro bezpečnost ČR, zájmy ČR, vnitřní a veřejnou bezpečnost**
- **NÚKIB může vydat zákaz dodavatele použít nebo upozornění na riziko** (je řešitelné bezpečnostním opatřením) + **lze udělit výjimku** (např. pokud to nikdo jiný nevyrábí, ohrozilo by to službu apod.) + **přechodné lhůty**

→ **Do 1 roku od vyrozumění o označení služby jako strategické**

Zajištění dostupnosti strategicky významných služeb

- Cíl = kritické služby musíme být **schopni zajistit alespoň omezeně z České republiky**, abychom byli připraveni na mimořádné situace v zahraničí
- poskytovatel strategicky významné služby je **povinen zajistit dostupnost strategicky významné služby v nezbytném rozsahu ve stanoveném čase a kvalitě z území České republiky** + **pravidelné ověřování** schopnosti zajištění

→ **Do 1 roku od vyrozumění o označení služby jako strategické (+ 1x za 2 roky prověřovat)**

Dopady na dosud regulované subjekty

- Primárně v režimu vyšších povinností
- Dílčí změny v dosavadním fungování
  - Rozsah ISMS – rozšíření podle služeb, defaultní rozsah celá organizace
  - Bezpečnostní opatření – víceméně shodná
  - Hlášení incidentů – principiálně shodné
  - Způsob určení – primárně samoidentifikace
  - Sankce – významně vyšší (+ 2 nové)
  - Komunikace s NÚKIB – speciální IS

Dozor nad dodržováním zákona

Dozorový orgán – NÚKIB

Oprávnění:

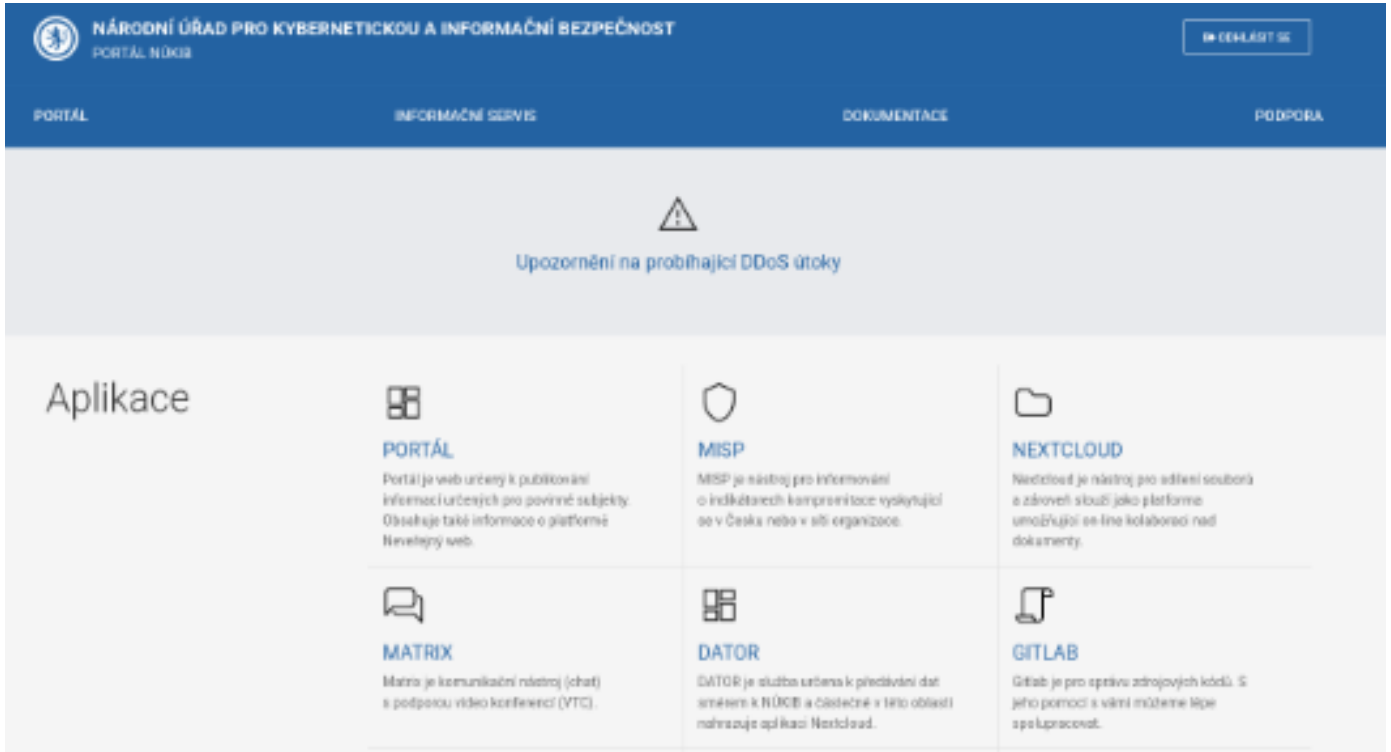
- **Kontrola**
- **Nápravná opatření**
- **Zvláštní sankce**
  - Pozastavení platnosti certifikace (NÚKIB)
  - Pozastavení výkonu řídicí funkce (soud)
- **Pokuta za přestupek**
  - Odstupňováno podle režimu a povahy pochybení
  - Až 250 mil. Kč nebo 2 % z celosvětového obratu
  - GDPR – *ne bis in idem*

~~**Doplňkový režim – inspektoři**~~

! Větší důležitost prohlášení o aplikovatelnosti (self-assessment)

Portál NÚKIB

- Připravujeme tzv. Portál NÚKIB
- Portál bude rozhraní sloužící administraci povinností, poskytování služeb a sdílení informací
  - Registrace organizace
  - Hlášení kontaktních údajů
  - Hlášení incidentů
  - Další hlášení (provádění opatření apod.)
  - Přístup k registru zranitelností
- Provázáno s vyhláškou o Portálu NÚKIB
- Vystavěn na platformě Neveřejného webu
- Tvoříme interním vývojem



Děkuji za pozornost.

Nis2.nukib.cz

regulace@nukib.cz