Nový zákon o kybernetické bezpečnosti

(po poslanecké sněmovně)

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

13. května 2025
ISSS 2025, Hradec Králové
TLP: CLEAR

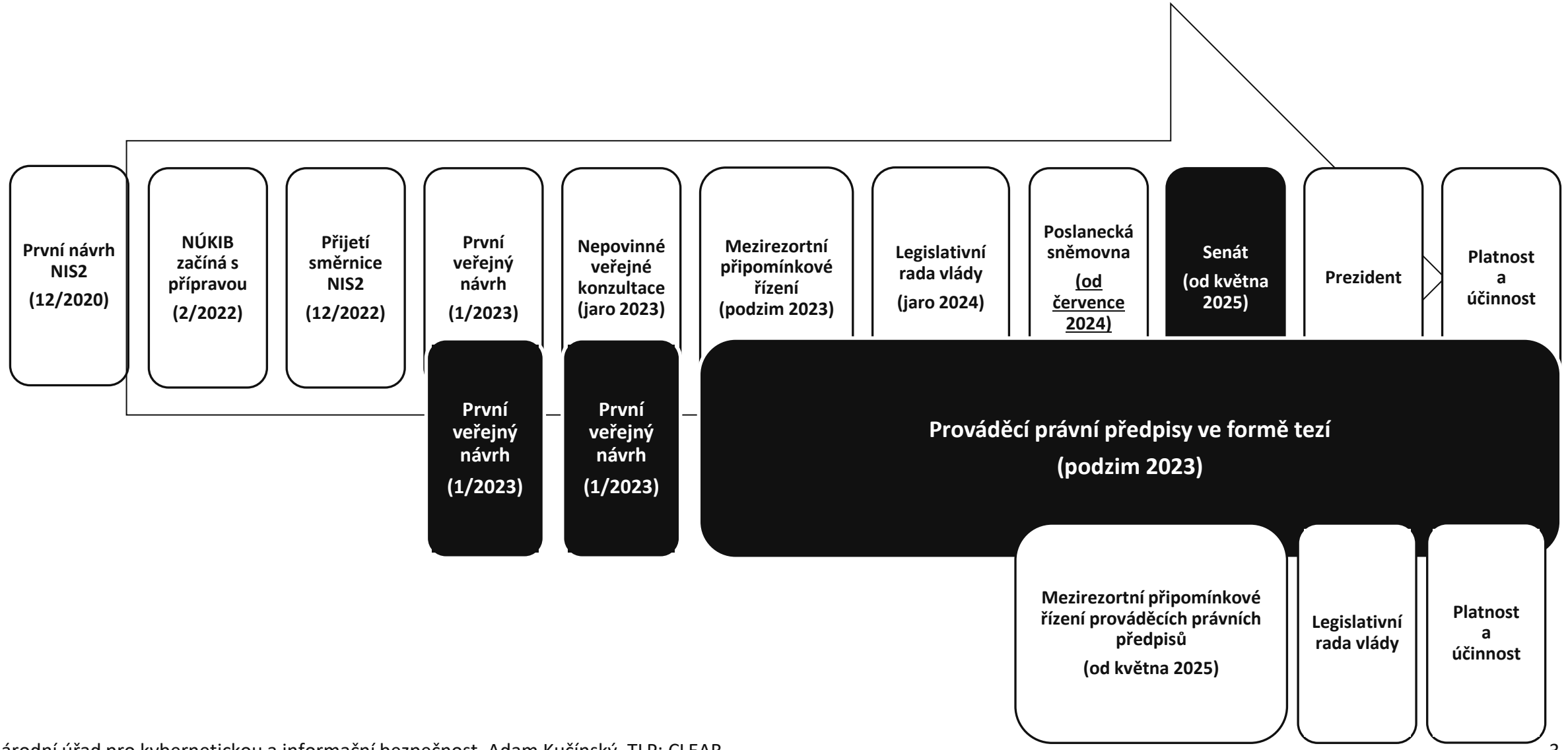
Adam Kučínský
ředitel
Odbor regulace

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.**

Harmonogram zákona o prováděcích předpisů



Pozměňovací návrhy v Poslanecké sněmovně

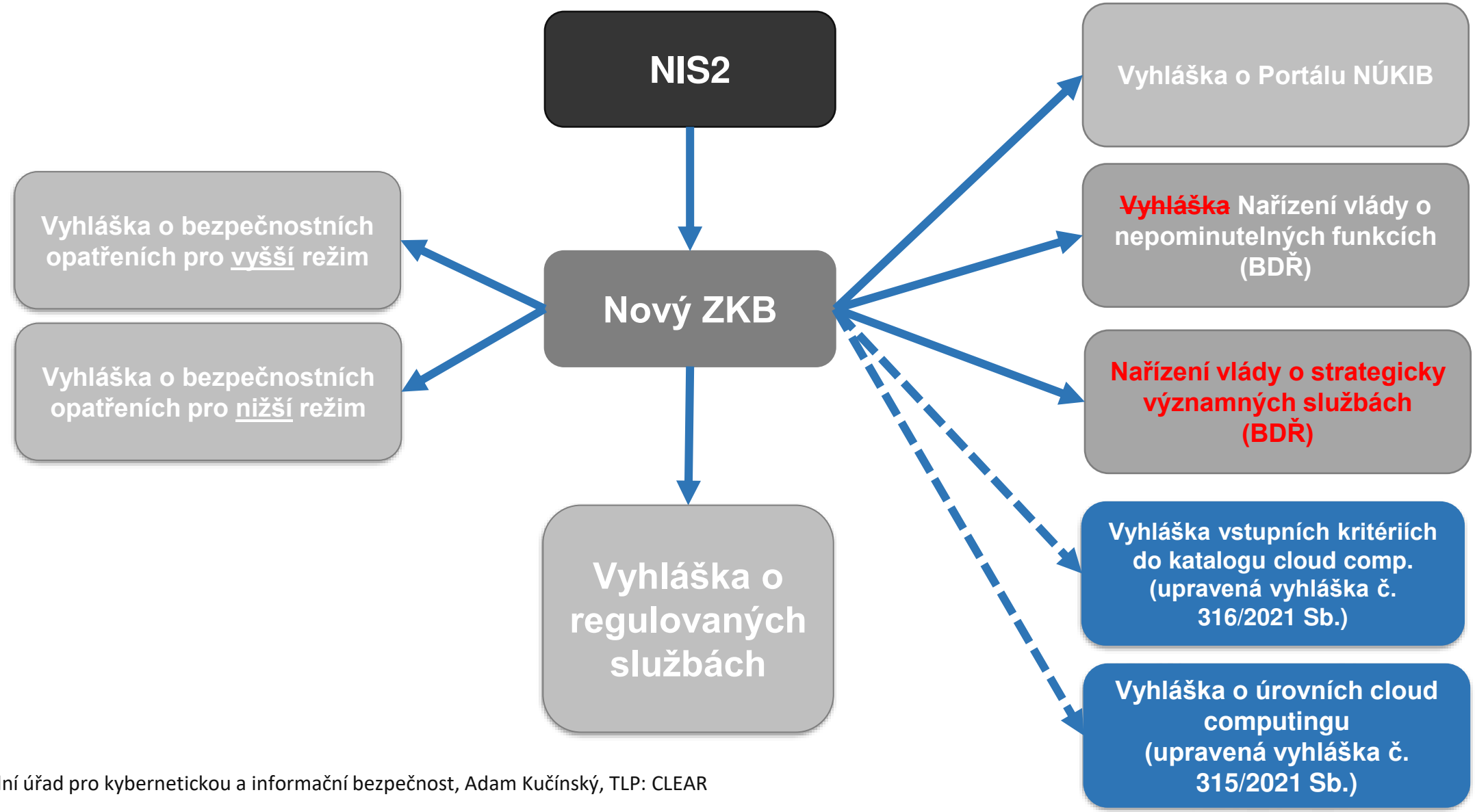
K zákonu bylo podáno několik pozměňovacích návrhů (PN) - pro přehlednost zjednodušeno:

- PN Bezpečnostního výboru – přesun rozhodování **o zákazu dodavatelů** v rámci mechanismu bezpečnosti dodavatelského řetězce na vládu - **tedy rozhoduje vláda**, NÚKIB řízení vede – **schváleno**
- PN Bezpečnostního výboru – **stanovení strategicky významných služeb a tzv. nepominutelných funkcí (**tedy subjektů a technologií na které se vztahuje mechanismus bezpečnosti dodavatelského řetězce) **nařízením vlády** (nikoli vyhláškou jak bylo navrhováno) - **schváleno**
- PN Hospodářského výboru – **zúžení mechanismu bezpečnosti dodavatelského řetězce pouze na aktiva kritická** (původně měla být zahrnuta i aktiva vysoká) - **schváleno**
- PN Hospodářského výboru – **úprava § 33** - zajištění dostupnosti strategicky významných služeb – při schválení navrhované úpravy by ustanovení nefungovalo – **neschváleno**
- PN poslankyně Lesenské – **lokalizace státních dat v ČR/EU** - **neschváleno**
- **Úprava účinnosti zákona** z pevného data na „první den třetího kalendářního měsíce následujícího po jeho vejití v platnost“ – **schváleno**

Návrh zákona schválen 25. 4. 2025 – 165 přítomno – pro 159, proti 0 (první zákon v roce 2024 – přítomno 166, pro 161, 0 proti)

Záznam jednání – projednávání návrhu nZKB začíná cca v 11:25 https://videoarchiv.psp.cz/playa.php?cast=4607

Ekosystém NZKB – prováděcí předpisy



Regulovaná služba a její poskytovatel

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**

Vyhláška o regulovaných službách - samoidentifikace

1. Veřejná správa

Regulovaná služba	
Služba	**Kritérium poskytovatele regulované služby a jeho režim pro tuto službu**
1.1. Výkon svěřených pravomocí	Orgán nebo osoba je I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že je a) ústředním orgánem státní správy, b) jiným správním úřadem s celostátní působností neuvedeným v písm. a), a to včetně ústředí a generálního ředitelství územně dekoncentrovaných (specializovaných) orgánů státní správy, c) Kanceláří prezidenta republiky, d) Kanceláří Senátu, e) Kanceláří Poslanecké sněmovny, f) Českou národní bankou, g) Policejním prezidiem, h) útvarem policie s celostátní působností, i) Generální inspekcí bezpečnostních sborů j) Generálním ředitelstvím hasičského záchranného sboru, k) krajským ředitelstvím hasičského záchranného sboru, l) Kanceláří Veřejného ochránce práv, m) Nejvyšším kontrolním úřadem, n) Úřadem pro zastupování státu ve věcech majetkových o) Správou úložišť radioaktivních odpadů, p) orgánem soudní moci, q) státním zastupitelstvím, r) zdravotní pojišťovnou, s) krajem, nebo t) hlavním městem Praha. II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je a) územně dekoncentrovaným (specializovaným) orgánem státní správy, b) profesní komorou[5], c) vysokou školou, d) Akademií věd České republiky, nebo e) obcí s rozšířenou působností, f) městským obvodem nebo městskou částí, která vykonává rozšířenou působnost.

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.

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.

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.

Specialitou vyššího režimu je „**strategicky významná služba**“

- kdo to bude stanoví nařízení vlády
- pro tyto služby platí BDŘ a zajištění dostupnosti

Povinnosti poskytovatele regulované služby

Hlavní povinnosti vyplývající z návrhu 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 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

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

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 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 aktivům = aktivum v podobě zpracovávané informace nebo poskytované služby

III. Bezpečnostní opatření - základní východiska

Základní princip – přiměřenost

- Nižší režim - ***zavede a provádí přiměřená bezpečnostní opatření***
- *Vyšší režim - na základě cílů, bezpečnostních potřeb a řízení rizik* ***zavede přiměřená bezpečnostní opatření***

Bezpečnostní opatření pro **nižší režim**

- Minimum – 8 stran, 15 paragrafů.
- Povinná osoba neprovádí hodnocení rizik ve smyslu současného znění vyhlášky o kybernetické bezpečnosti.
- Pokud některé nemůže zavést – řádně zdůvodní a přijme jiné vhodné bezpečnostní opatření.

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

Pokud významný dopad

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

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

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

V. Informační povinnost – incident a hrozba

Informační povinnost – kybernetický bezpečnostní **incident**

- Pokud to považuje **za vhodné, oznámí bez zbytečného odkladu uživatelům kybernetický bezpečnostní incident s významným dopadem,** který by mohl negativně ovlivnit poskytování této služby.
- Úřad může uložit povinnost nebo zákaz informovat uživatele regulované služby o tomto incidentu.

Informační povinnost – významná **hrozba**

- **Povinnost informovat uživatele**, 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 nebo uživatele regulované služby natolik, že způsobí značnou újmu.**

VI. Protiopatření

Výstraha

- **Informování veřejnosti** o kybernetickém bezpečnostním **incidentu či o porušování povinností** daných tímto zákonem

Varování

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

Reaktivní protiopatření

- Stanovení konkrétní povinnosti k zabezpečení
- 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 vybrané organizace – strategicky významné služby
- Organizace v rámci této povinnosti musí nahlásit dodavatele
- Budou prověřování dodavatelé do kritické části systému = aktiva s hodnotou ~~3 a~~ 4 (~~vysoká/~~kritická), kteří dodávají bezpečnostně významnou dodávku = má výpočetní kapacitu

Na základě přijatých pozm. návrhů

- Stát prověří
  - NÚKIB k tomu vyžaduje informace a součinnost řady orgánů (PČR, SLUŽBY, FAU, NSZ, MPO, MV, NBÚ, ÚOHS…)
- ~~NÚKIB/~~Vláda může vydat zákaz dodavatele použít nebo upozornění na riziko (je řešitelné bezp. opatřením)
- Hlášení dodavatelů do 1 roku od určení poskytovatele regulované služby
- Detail koho přesně se to týká – ~~vyhláška o regulovaných službách/~~nařízení vlády o strategicky významných službách

Na základě přijatých pozm. návrhů

- Jakých aktiv se to týká – ~~Vyhláška/~~Nařízení vlády o nepominutelných částech a těch s hodnocením kritická ~~a vysoká~~
- Proces hlášení dodavatelů poskytovatelem reg. služby – Vyhláška o Portálu NÚKIB

V závislosti na přijatých pozm. návrzích

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.**

V závislosti na přijatých pozm. návrzích

Nezbytný rozsah dostupnosti strategicky významné služby stanoví nařízení vlády/~~vyhláška~~

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.

VIII. Zajištění dostupnosti strategicky významných regulovaných služeb

- Východiska návrhu:
  - 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 návrhu:
  - 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 a kvalitu.

Dotazy ?

Děkuji Vám za pozornost!

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