Nová právní úprava kybernetické bezpečnosti

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

7. února 2024
TLP: CLEAR

Ondřej Polák
oddělení regulace soukromého sektoru

Na začátek

- **Směrnice NIS2** [*směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148)*] byla dne 27. prosince 2022 zveřejněna v Úředním věstníku Evropské unie.
- Publikovaná podoba směrnice NIS2 je oficiální a **nebude se již dále měnit.**
- Základem změn je jak směrnice NIS2, tak také potřeba zákon o kybernetické bezpečnosti aktualizovat mj. s ohledem na vnitrostátní požadavky.

NIS2 – regulované služby

Směrnice NIS1:

7 odvětví

Kritérium dopadu incidentu

⇒ **cca 400 povinných osob**

Směrnice NIS2:

18 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 veřejné 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

V České republice nejsou umístěny žádné subjekty pozemní infrastruktury, pro Českou republiku tedy nerelevantní.

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.

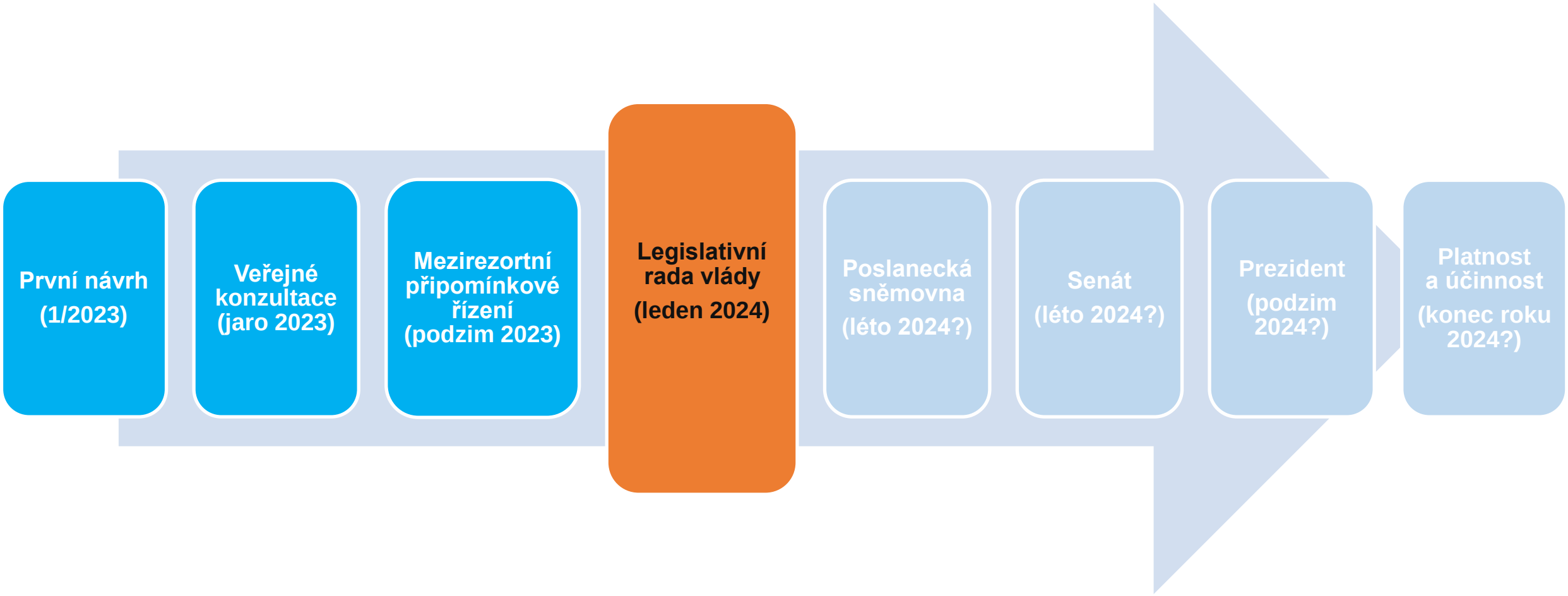
POSKYTOVATELÉ DIGI SLUŽEB

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.

Harmonogram



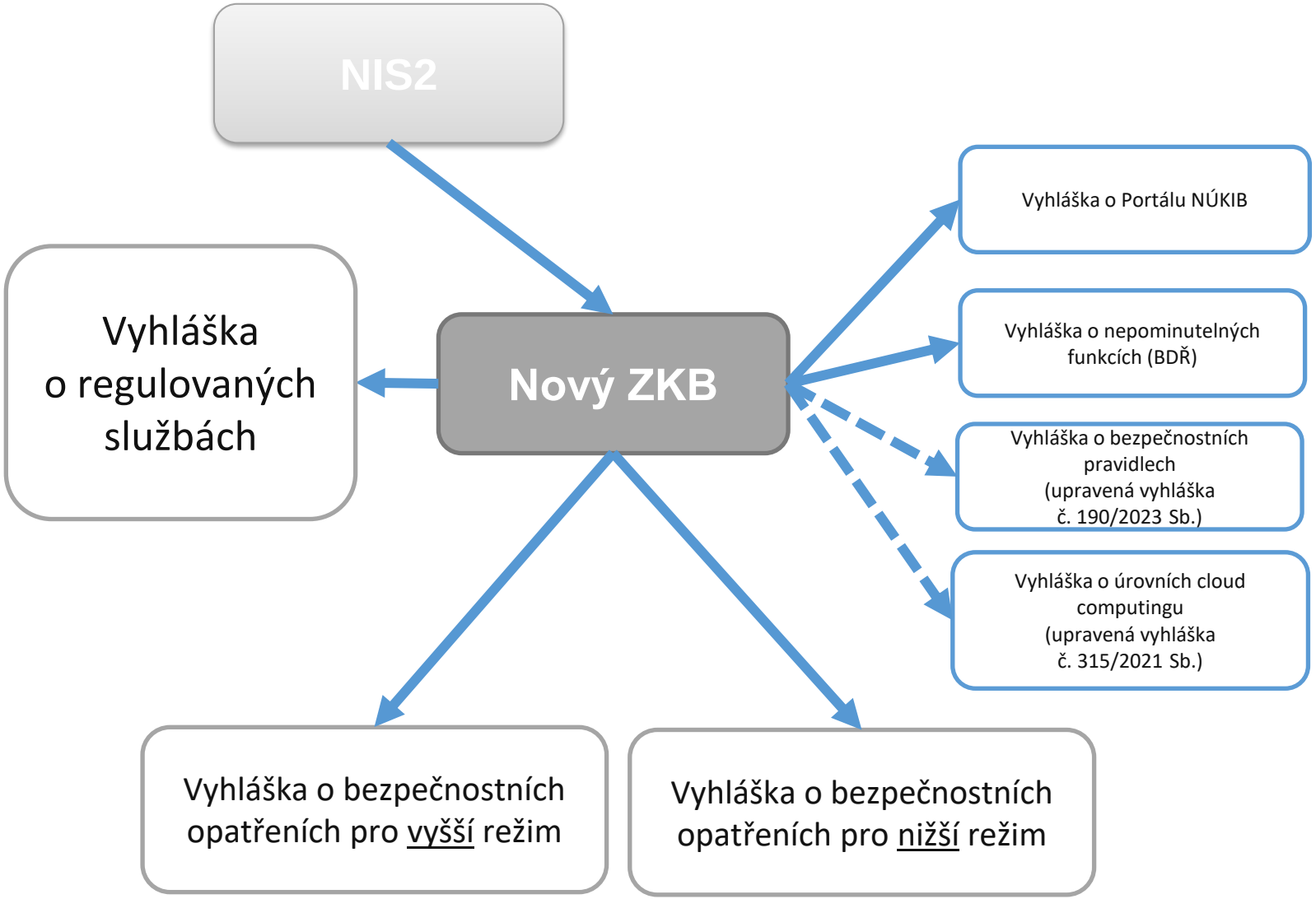
Nový zákon o kybernetické bezpečnosti (nZKB)

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

= zcela nová úprava – 74 paragrafů

Verze v mez. připomínkovém řízení má aktuálně navíc **7 vyhlášek**

Celý návrh zveřejněn na webu **nis2.nukib.cz**



Nový ZKB – 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

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.**

Režim poskytovatele regulované služby je stanoven vyhláškou o regulovaných službách, s výjimkou služeb určených NÚKIBem, pak je režim 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).

Hlavní změny za rok 2023

- 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)**
- Stav kybernetického nebezpečí → **koncepční změny, provázání s krizovým řízením** (např. náhrada škody)
- Registrace a evidence poskytovatele → **registrace a evidence regulované služby**
- Dílčí změny v mechanismu prověřování bezpečnosti dodavatelského řetězce – **zapojení regulátorů, životní cyklus technologií, zapojení BRS**

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

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
- Aktuálně 107 služeb v 22 odvětvích (mírně odlišná taxonomie než NIS2)

Kritéria pro identifikaci regulované služby – NIS2

5. Výroba	a) výroba zdravotnických prostředků a diagnostických zdravotnických prostředků in vitro	subjekty vyrábějící zdravotnické prostředky ve smyslu čl. 2 bodu 1 nařízení Evropského parlamentu a Rady (EU) 2017/745 (4) a subjekty vyrábějící diagnostické zdravotnické prostředky in vitro ve smyslu čl. 2 bodu 2 nařízení Evropského parlamentu a Rady (EU) 2017/746 (5), s výjimkou subjektů vyrábějících zdravotnické prostředky uvedených v příloze I bodu 5 páté odrážce této směrnice
	b) výroba počítačů, elektronických a optických přístrojů a zařízení	podniky vykonávající kteroukoliv z hospodářských činností ve smyslu sekce C oddílu 26 klasifikace NACE Rev. 2
	c) výroba elektrických zařízení	podniky vykonávající kteroukoliv z hospodářských činností ve smyslu sekce C oddílu 27 klasifikace NACE Rev. 2
	d) výroba strojů a zařízení j. n.	podniky vykonávající kteroukoliv z hospodářských činností ve smyslu sekce C oddílu 28 klasifikace NACE Rev. 2
	e) výroba motorových vozidel, přívěsů a návěsů	podniky vykonávající kteroukoliv z hospodářských činností ve smyslu sekce C oddílu 29 klasifikace NACE Rev. 2
	f) výroba ostatních dopravních prostředků a zařízení	podniky vykonávající kteroukoliv z hospodářských činností ve smyslu sekce C oddílu 30 klasifikace NACE Rev. 2

10. Veřejná správa		— ústřední subjekty veřejné správy vymezené členským státem v souladu s vnitrostátním právem
		— subjekty regionální veřejné správy vymezené členským státem v souladu s vnitrostátním právem

Kritéria pro identifikaci regulované služby - VRS

7. Výrobní průmysl

Regulovaná služba	
Služba	**Kritérium poskytovatele regulované služby a jeho režim pro tuto službu**
7.1. Výroba počítačů, elektronických a optických přístrojů a zařízení	Výrobce počítačů, elektronických a optických přístrojů a zařízení ve smyslu oddílu 26 klasifikace CZ-NACE, který je velkým nebo středním podnikem, je poskytovatel regulované služby v režimu nižších povinností.
7.2. Výroba elektrických zařízení	Výrobce elektrických zařízení ve smyslu oddílu 27 klasifikace CZ-NACE, který je velkým nebo středním podnikem, je poskytovatel regulované služby v režimu nižších povinností.
7.3. Výroba strojů a zařízení nezařazená pod jiné oddíly klasifikace CZ-NACE	Jinde nezařazený výrobce strojů a zařízení ve smyslu oddílu 28 klasifikace CZ-NACE, který je velkým nebo středním podnikem, je poskytovatel regulované služby v režimu nižších povinností.
7.4. Výroba motorových vozidel (kromě motocyklů), přívěsů a návěsů	Výrobce motorových vozidel, přívěsů a návěsů ve smyslu oddílu 29 klasifikace CZ-NACE je I. poskytovatel regulované služby v režimu vyšších povinností v případě, že sériově vyrábí osobní motorová vozidla, II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je velkým nebo středním podnikem.
7.5. Výroba ostatních dopravních prostředků a zařízení	Výrobce ostatních dopravních prostředků a zařízení ve smyslu oddílu 30 klasifikace CZ-NACE, který je velkým nebo středním podnikem, je poskytovatel regulované služby v režimu nižších povinností.

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 písmenu 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) Generálním ředitelstvím hasičského záchranného sboru, j) krajským ředitelstvím hasičského záchranného sboru, k) Kanceláří Veřejného ochránce práv, l) Nejvyšším kontrolním úřadem, m) Úřadem pro zastupování státu ve věcech majetkových n) orgánem soudní moci, o) státním zastupitelstvím, p) zdravotní pojišťovnou, q) krajem, r) 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[2], c) vysokou školou, d) Akademií věd České republiky, nebo e) obcí s rozšířenou působností.

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

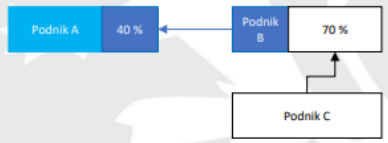
TLP: CLEAR

ŘEDNÍHO PODNIKU

PODNIKŮ

2. PARTNERSKÝ PODNIK
Každý podnik, který vlastní 25 % - 50 % základního kapitálu nebo hlasovacích práv jiného podniku. **Údaje za tento podnik se přičítají ve výši procentuálního vlastnického podílu.**

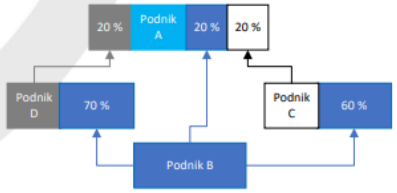
PŘÍKLAD 2
Posuzovaný podnik A je vlastněn ze 40 % podnikem B. Podnik B je navíc vlastněn podnikem C ze 70 %. Jelikož je mezi podnikem B a C spojenecký vztah, musíme k údajům za podnik A přičíst nejen 40 % zaměstnanců a 40 % ročního obratu a aktiv podniku B, ale rovněž podniku C.
Výsledek = 100 % A + 40 % B + 40 % C

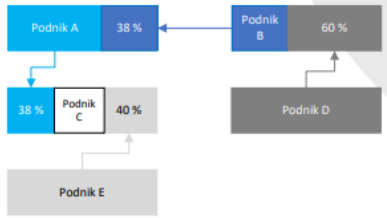


PŘÍKLAD 3
Posuzovaný podnik A vlastní z 51 % podnik B. K údajům za podnik A tedy přičítáme 100 % zaměstnanců a 100 % ročního obratu a aktiv podniku B.
Výsledek = 100 % A + 100 % B

PŘÍKLAD 5
Posuzovaný podnik A je vlastněn z 60 % podnikem B. Podnik B má dva partnery, a to podnik C, který vlastní 32 % podniku B, a podnik D, který vlastní 25 % podniku B. K údajům za podnik A tedy přičítáme 100 % zaměstnanců a 100 % ročního obratu a aktiv podniku B, dále 32 % podniku C, a 25 % podniku D.
Výsledek = 100 % A + 100 % B + 32 % C + 25 % D

PŘÍKLAD 6
Posuzovaný podnik A je vlastněn podniky B, C a D, jejichž podíl je u každého roven 20 %. Při letmém posouzení našeho vztahu k podnikům by se mohlo zdát, že se jedná o samostatný podnik, jelikož jednotlivé podíly nepřekračují hranici 25 %. Jelikož jsou ale podniky B, C a D vzájemnými spojenci, musíme jejich podíly na našem podniku A sečíst. Tím se dostáváme přes hranici 50% podílu na vlastnictví a všechny tři podniky se stávají našimi spojenci. Z toho vyplývá, že při výpočtu musíme přičíst údaje za celou skupinu.
Výsledek = 100 % A + 100 % B + 100 % C + 100 % D





Podrobnější výpočty a informace o tom, co vše započítat do velikosti zkoumaného podniku lze nalézt v uživatelské příručce k definici malých a středních podniků: **https://osveta.nukib.cz/pluginfile.php/58365/mod_page/content/311/Priloha-4_U%C5%BEivatelsk%C3%A1%20p%C5%99%C3%ADru%C4%8Dka%20k%20definici%20mal%C3%BDch%20a%20st%C5%99edn%C3%ADch%20podnik%C5%AF.pdf**

verze 1.0, platná ke dni 14.11.2022

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)]()

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 (organizační x technická – IT, OT)

- 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)**

a) Odvětví 1. Veřejná správa, služba 1.1. Výkon svěřených pravomocí, bod I. písm. a) až i),
b) Odvětví 2. Energetika - Elektřina, služba 2.1. Výroba elektřiny, bod I. písm. b),
c) Odvětví 2. Energetika - Elektřina, služba 2.2. Provoz přenosové soustavy elektřiny,
d) Odvětví 2. Energetika - Elektřina, služba 2.3. Provoz distribuční soustavy elektřiny, bod I. písm. b),
e) Odvětví 3. Energetika - Ropa a ropné produkty, služba 3.4. Provoz ropovodu, bod I.,
f) Odvětví 3. Energetika - Ropa a ropné produkty, služba 3.5. Provoz produktovodu, bod I.,
g) Odvětví 4. Energetika - Plynárenství, služba 4.2. Provoz přepravní soustavy plynu,
h) Odvětví 4. Energetika - Plynárenství, služba 4.3. Provoz distribuční soustavy plynu, bod I.,
i) Odvětví 12. Letecká doprava, služba 12.4. Řízení letového provozu nad vzdušným prostorem České republiky,
j) Odvětví 12. Letecká doprava, služba 12.9. Letové navigační služby, bod I.,
k) Odvětví 13. Drážní doprava, služba 13.1. Stavění vlakových cest na celostátní úrovni,
l) Odvětví 16. Digitální infrastruktura a služby, služba 16.1. Poskytování veřejně dostupné služby elektronických komunikací, bod I. písm. c) a d),
m) Odvětví 16. Digitální infrastruktura a služby, služba 16.2. Zajišťování veřejné komunikační sítě elektronických komunikací, bod I. písm. c) a d),
n) Odvětví 16. Digitální infrastruktura a služby, služba 16.5. Správa a provoz registru internetových domén nejvyšší úrovně, nebo
o) Odvětví 16. Digitální infrastruktura a služby, služba 16.6. Poskytování služby cloud computingu, bod I. písm. b).

Dozor nad dodržováním zákona

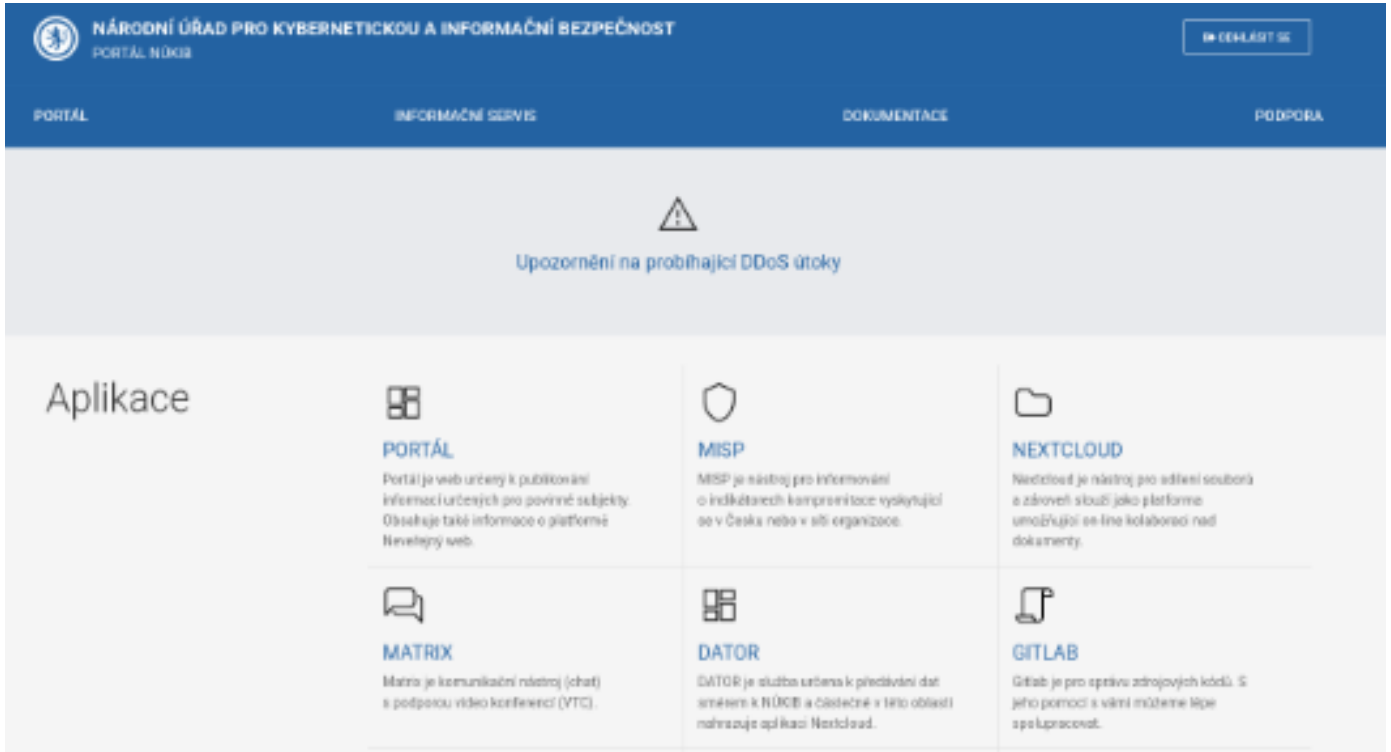
Dozorový orgán – NÚKIB

Oprávnění

- **Kontrola**
- **Nápravná opatření**
- **Zvláštní sankce**
  - Pozastavení platnosti certifikace/osvědčení souvisejících se zajištěním kybernetické bezpečnosti regulované služby (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*

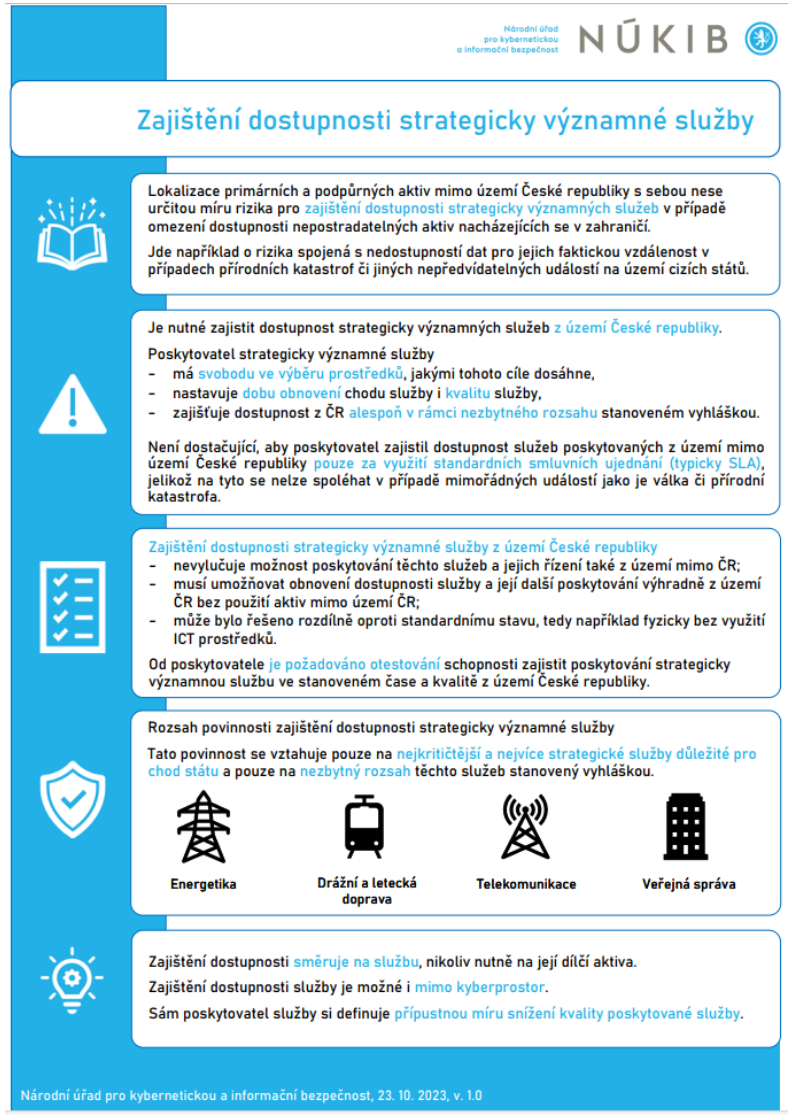
Portál NÚKIB

- 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



Factsheets

PŘEHLEDOVÉ FACTSHEETY K NOVÉMU ZÁKONU



Národní úřad pro kybernetickou a informační bezpečnost

NÚKIB

Zajištění dostupnosti strategicky významné služby

Lokalizace primárních a podpůrných aktiv mimo území České republiky s sebou nese určitou míru rizika pro zajištění dostupnosti strategicky významných služeb v případě omezení dostupnosti nepostradatelných aktiv nacházejících se v zahraničí.

Jde například o rizika spojená s nedostupností dat pro jejich faktickou vzdálenost v případech přírodních katastrof či jiných nepředvídatelných událostí na území cizích států.

Je nutné zajistit dostupnost strategicky významných služeb z území České republiky.

Poskytovatel strategicky významné služby
- má svobodu ve výběru prostředků, jakými tohoto cíle dosáhne,
- nastavuje dobu obnovení chodu služby i kvalitu služby,
- zajišťuje dostupnost z ČR alespoň v rámci nezbytného rozsahu stanoveném vyhláškou.

Není dostačující, aby poskytovatel zajistil dostupnost služeb poskytovaných z území mimo území České republiky pouze za využití standardních smluvních ujednání (typicky SLA), jelikož na tyto se nelze spoléhat v případě mimořádných událostí jako je válka či přírodní katastrofa.

Zajištění dostupnosti strategicky významné služby z území České republiky
- nevylučuje možnost poskytování těchto služeb a jejich řízení také z území mimo ČR;
- musí umožňovat obnovení dostupnosti služby a její další poskytování výhradně z území ČR bez použití aktiv mimo území ČR;
- může bylo řešeno rozdílně oproti standardnímu stavu, tedy například fyzicky bez využití ICT prostředků.

Od poskytovatele je požadováno otestování schopnosti zajistit poskytování strategicky významnou službu ve stanoveném čase a kvalitě z území České republiky.

Rozsah povinnosti zajištění dostupnosti strategicky významné služby

Tato povinnost se vztahuje pouze na nejkritičtější a nejvíce strategické služby důležité pro chod státu a pouze na nezbytný rozsah těchto služeb stanovený vyhláškou.

Energetika | Drážní a letecká doprava | Telekomunikace | Veřejná správa

Zajištění dostupnosti směruje na službu, nikoliv nutně na její dílčí aktiva.

Zajištění dostupnosti služby je možné i mimo kyberprostor.

Sám poskytovatel služby si definuje přípustnou míru snížení kvality poskytované služby.

Národní úřad pro kybernetickou a informační bezpečnost, 23. 10. 2023, v. 1.0

Co teď?

- Identifikovat všechny poskytované služby a velikost organizace
- Prostudovat návrh vyhlášky o regulovaných službách

Naplnění kritérií?

- Prostudovat návrhy vyhlášek o bezpečnostních opatřeních
- Zmapovat aktuální stav organizace (audit aktuálního stavu KB a slabých míst, gap analýza)
- Vypracovat business impact analýzu (zejm. jaké by byly dopady narušení řádného fungování jednotlivých systémů na vaši organizaci; nejde přitom jen o nedostupnost používaných informačních systémů, ale i o narušení důvěrnosti nebo integrity shromažďovaných dat)
- Začít školit relevantní osoby – management, klíčoví zaměstnanci (základní školení pro všechny uživatele, odborné školení pro osoby, které v organizaci řeší/budou řešit kybernetickou bezpečnost, nezapomínat přitom i na vrcholový management (management si musí být vědom důležitosti řízení kybernetické bezpečnosti v organizaci)
- Základní technická opatření – firewally (zejména perimetrové), antiviry (zejména sofistikovanější EDR), zálohovací řešení, provádění aktualizací

Děkuji za pozornost.

Nis2.nukib.cz

regulace@nukib.cz