NÚKIB

INFORMACE O INSTITUTU ZÁKLADNÍ SLUŽBY

Shrnutí způsobu určení provozovatele základní služby a informačního systému základní služby

Verze 1.5, platná ke dni 22. 12. 2022

Obsah

Úvod

Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby, ze dne 8. prosince 2017, vstupuje v účinnost 1. února 2018. Cílem vyhlášky je stanovit kritéria pro určení provozovatele základní služby a informačního systému základní služby. Tento dokument obsahuje shrnutí informací týkajících se nových institutů, které vyhláška specifikuje.

V případě dotazů se prosím obracejte na sekretariát Národního úřadu pro kybernetickou a informační bezpečnost:

Národní úřad pro kybernetickou a informační bezpečnost
Mučednická 1125/31
616 00 Brno – Žabovřesky

E-mail: regulace@nukib.cz

Upozornění:

Tento dokument slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů. Právo změny tohoto dokumentu vyhrazeno.

1 Manažerské shrnutí

Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby (dále jen „vyhláška“), ze dne 8. prosince 2017, vstupuje v účinnost 1. února 2018.

Cílem vyhlášky je stanovit kritéria pro určení provozovatele základní služby a informačního systému základní služby. Základní služba je služba *„závislá na informačních systémech nebo sítích elektronických komunikací v odvětví energetika, doprava, bankovnictví, infrastruktura finančních trhů, zdravotnictví, vodní hospodářství, digitální infrastruktura nebo chemický průmysl“* (§ 2 písm. i) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen „zákon o kybernetické bezpečnosti“)). Kritéria pro určení provozovatele základní služby a informačního systému základní služby jsou odvětvová a dopadová (§ 28 odst. 2 písm. e) zákona o kybernetické bezpečnosti). Odvětvová kritéria se dále člení na kritéria, kterými jsou druh služby, druh subjektu a speciální kritérium druhu subjektu. Kritéria dopadová uvádějí hranice možných škod způsobených kybernetickým bezpečnostním incidentem v informačních systémech a sítích elektronických komunikací, kterých musí být pro určení dosaženo.

Při určení má být zohledněna *„významnost služeb poskytovaných v jednotlivých odvětvích“* (§ 22a odst. 1 písm. a) zákona o kybernetické bezpečnosti). Tento požadavek je reprezentován kritériem „**Speciální kritéria druhu subjektu“.** Toto kritérium naplní pouze provozovatel služeb, který je v daném odvětví významný, čímž je realizován výše uvedený požadavek zohlednění významnosti služeb v jednotlivých odvětvích.

Odvětvová kritéria jsou ve vyhlášce stanovena následovně (v závorce uveden zjednodušený příklad odpovídající prvnímu odvětví dle přílohy k vyhlášce):

- 1. Odvětví (Energetika)
- 1.1. Pododvětví (Elektřina) – pododvětví jsou stanovena pouze u odvětví Energetika a Doprava, v textu vyhlášky jsou označována souslovím „část odvětví“
- 1.1.1. Druh služby (Výroba elektřiny)
- Druh subjektu (Výrobce elektřiny podle energetického zákona)
- a) Speciální kritérium druhu subjektu – jedná se o kritérium významnosti poskytované služby v rámci daného odvětví (Výrobna s celkovým instalovaným elektrickým výkonem nejméně 500 MW)

Odvětvová kritéria na sebe navazují a postupuje se od obecného ke speciálnímu.

Tedy v každé kategorii podle vzoru: 1. – 1.1. – 1.1.1. – Druh subjektu – Speciální kritéria druhu subjektu.

Pokud jsou odvětvová kritéria subjektem naplněna, je možné přistoupit ke kritériím dopadovým a posoudit dopad kybernetického bezpečnostního incidentu v systému zajišťujícím poskytování služby. Tedy posuzuje se dopad incidentu v systému, který je využíván provozovatelem služby k zajištění služby v posuzovaném odvětví.

V rámci toho má být zvážen **dopad kybernetického bezpečnostního incidentu** na 1) rozsah a kvalitu poskytování základní služby uživatelům, 2) ekonomické a společenské činnosti a veřejnou bezpečnost a 3) vzájemnou závislost odvětví (§ 22a odst. 1 písm. b) body 1 – 3 zákona o kybernetické bezpečnosti). Tento požadavek je reprezentován **dopadovými kritérii**. Dopadová kritéria stanovují hranici škod, kterou by mohl způsobit kybernetický bezpečnostní incident. Subjekt, který naplní odvětvová kritéria, bude určen jako provozovatel základní služby, pokud by mohl případný kybernetický bezpečnostní incident v jeho informačních systémech nebo sítích elektronických komunikací, na nichž je poskytování posuzované služby závislé, naplnit některý z níže specifikovaných dopadů.

Dopadová kritéria jsou ve vyhlášce stanovena takto:

Kybernetický bezpečnostní incident v informačním systému či síti elektronických komunikací by mohl způsobit:

I. závažné omezení (či narušení[1]) (či nedostupnost[1]) druhu služby postihující více než 25 000[1], 50 000[1] nebo 500 000[1] osob,
II. závažné omezení či narušení jiné základní služby, nebo omezení či narušení provozu prvku kritické infrastruktury,
III. hospodářskou ztrátu vyšší než 0,25 % HDP,
IV. nedostupnost druhu služby pro více než 1 600 osob, která není nahraditelná jiným způsobem bez vynaložení nepřiměřených nákladů,
V. oběti na životech s mezní hodnotou více než 100[1] nebo 200[1] mrtvých nebo 1 000 zraněných osob vyžadujících lékařské ošetření,
VI. narušení veřejné bezpečnosti na významné části správního obvodu obce s rozšířenou působností, které by mohlo vyžadovat provedení záchranných a likvidačních prací složkami integrovaného záchranného systému nebo
VII. kompromitaci citlivých osobních údajů o 200 000 osobách.

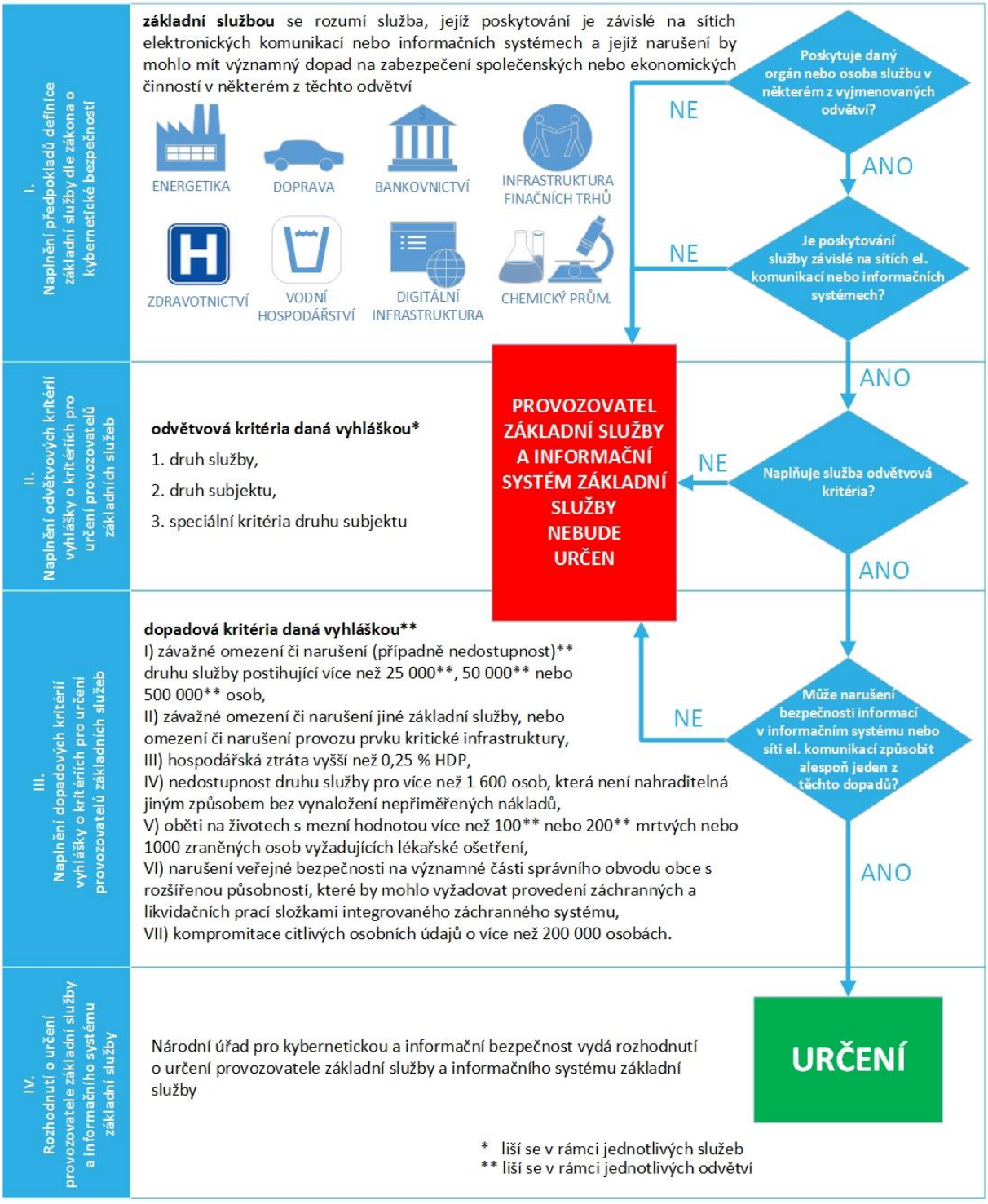
Dopad incidentu bude posuzován pouze v případech, kdy posuzovaný subjekt (ten, který službu poskytuje, a k jejímuž poskytování využívá posuzovaný systém) naplní odvětvová kritéria. Při posuzování dopadových kritérií je dopad kybernetického bezpečnostního incidentu srovnáván se stanovenými kritérii. Pokud dopad incidentu v systému naplní alespoň jedno dopadové kritérium, bude tento systém určen jako informační systém základní služby. **Pokud tedy subjekt naplní odvětvová kritéria a kybernetický bezpečnostní incident v jeho**

[1] Hodnoty se liší v rámci jednotlivých odvětví nebo pododvětví.

systému či systémech naplní dopadová kritéria, bude určen jako provozovatel základní služby a předmětný systém jako informační systém základní služby.

Proces určení a postup skrze odvětvová a dopadová kritéria popisuje Schéma určení provozovatele základní služby a informačního systému základní služby.

Pokud tedy budeme chtít celý proces určení shrnout, je možné říci, že pro to, aby byl subjekt určen jako provozovatel základní služby, musí provozovat službu v některém ze zákonem definovaných a vyhlášce konkretizovaných odvětví a poskytování této služby musí být závislé na informačním systému nebo síti elektronických komunikací (v obrázku č. 1 znázorněno blokem I.). Poté může být přistoupeno k detailnímu posouzení naplnění kritérií. Kritéria jsou odvětvová (ty musí naplnit subjekt – v obrázku č. 1 reprezentováno blokem II.) a dopadová (ty musí naplnit incident v systému posuzovaného subjektu – v obrázku č. 1 reprezentováno blokem III.). Pokud jsou kritéria naplněna, dojde k určení (v obrázku č. 1 reprezentováno blokem IV.).



Obrázek č. 1: Schéma určení provozovatele základní služby a informačního systému základní služby

2 Popis určujících odvětvových kritérií

2.1 Transpozice odvětví a pododvětví definovaných směrnicí

Odvětví a pododvětví základních služeb definovaná přílohou II Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (dále jen „směrnice NIS“) byla vzhledem k nutnosti plné transpozice přejata kompletně. Protože směrnice NIS umožňuje odvětví základních služeb rozšiřovat, přidala Česká republika mezi odvětví základní služby chemický průmysl a v rámci odvětví Energetiky pododvětví Teplárenství. Je třeba zmínit, že rozšiřování odvětví základní služby není mezi členskými státy neobvyklé, např. Německo či Francie přidávají odvětví Potravinářství.

2.2 Stanovení odvětvových kritérií

Směrnice NIS stanovuje odvětvová a pododvětvová kritéria poměrně obecně. Pro přesnou definici druhu služeb a druhu subjektu zahrnutých do regulace bylo využito unijních směrnic a nařízení, na které je směrnicí NIS odkazováno.

Pro stanovení speciálních kritérií druhu subjektu, která reprezentují významnost subjektu pro dané odvětví, byla svolána pracovní skupina z řad odborné veřejnosti i státní správy. Na základě výstupu z této pracovní skupiny byla tato speciální kritéria definována.

Pracovní skupina se skládala z podskupin pro jednotlivá odvětví. Celkem tak bylo vytvořeno 14 podskupin, které se scházely samostatně. Do tvorby vyhlášky se zapojilo cca 120 odborníků napříč zařazenými odvětvími. Na jednání pracovních skupin byl představen návrh kritérií pro provozovatele základní služby a pracovní skupina tento návrh připomínkovala a diskutovala možné varianty, dokud nebylo nalezeno vhodné řešení. Tento postup byl klíčový při tvorbě vyhlášky z důvodu širokého rozsahu a diverzity jednotlivých odvětví a pododvětví.

3 Popis dopadových určujících kritérií

3.1 Stanovení kritérií

Směrnice NIS ukládá členským státům při stanovování dopadových kritérií pro určení provozovatele základní služby a informačního systému základní služby zvážit následující hlediska (čl. 6 odst. 1 směrnice NIS):

a) počet uživatelů, kteří jsou závislí na službě poskytované subjektem,
b) závislost dalších odvětví podle přílohy II směrnice NIS na službě poskytované daným subjektem,
c) možný dopad incidentů, pokud jde o jejich intenzitu a délku trvání, na ekonomické a společenské činnosti nebo veřejnou bezpečnost,
d) podíl daného subjektu na trhu,
e) zeměpisný rozsah oblasti, která by mohla být incidentem dotčena a
f) důležitost subjektu, pokud jde o udržování dostatečné úrovně dané služby, s přihlédnutím k dostupnosti alternativních způsobů zajištění této služby.

Z výše popsaných hledisek vychází i § 22a odst. 1 písm. b) zákona o kybernetické bezpečnosti, který stanoví, že v rámci dopadových kritérií má být zohledněn dopad kybernetického bezpečnostního incidentu zejména na:

1) rozsah a kvalitu poskytování základní služby uživatelům, kteří jsou na ní závislí,
2) ekonomické a společenské činnosti a veřejnou bezpečnost a
3) vzájemnou závislost odvětví uvedených v § 2 písm. i).

Dopadová kritéria jsou ve vyhlášce stanovena tak, aby pokrývala výše popsané oblasti stanovené směrnicí NIS (čl. 6 odst. 1 směrnice NIS) i zákonem (§ 22a odst. 1 písm. b) zákona o kybernetické bezpečnosti), a to pro různé scénáře. Při identifikaci dopadových kritérií byla v souladu se směrnicí NIS zohledněna povaha a specifika jednotlivých odvětví (případně pododvětví) a kritéria se tak pro jednotlivá odvětví mírně liší (např. v pododvětví Letecká doprava či odvětví Bankovnictví jsou v některých dopadových kritériích stanoveny rozdílné prahové hodnoty, než např. v Energetice). Při rozhodnutí o relevanci konkrétního kritéria pro konkrétní odvětví nebo pododvětví bylo využito podkladů od účastníků pracovních skupin, konzultací s odborníky, zkušeností získaných při procesu určování kritické informační infrastruktury a otevřených zdrojů.

Tabulka č. 1 mapuje dopadová kritéria uvedená ve vyhlášce s požadavky směrnice NIS (čl. 6 odst. 1 směrnice NIS) a jejich transpozicí do zákona o kybernetické bezpečnosti (§ 22a odst. 2 zákona o kybernetické bezpečnosti).

Tabulka č. 1: Srovnání navrhovaných dopadových kritérií ve vyhlášce s požadavky zákona o kybernetické bezpečnosti a směrnice NIS

Dopadové kritérium dle vyhlášky Dopad kybernetického bezpečnostního incidentu v informačním systému nebo síti el. komunikací, na jehož fungování je závislé poskytování služby, může způsobit	**Oblasti dopadu, které mají být zváženy dle § 22a odst. 2 zákona o kybernetické bezpečnosti**	**Oblasti dopadu dle článku 6 odst. 1 směrnice NIS**
I) závažné omezení (či narušení) (či nedostupnost) druhu služby postihující více než 25 000 nebo 50 000 nebo 500 000 osob	1) rozsah a kvalita poskytování základní služby uživatelům	a)
II) závažné omezení či narušení jiné základní služby, nebo omezení či narušení provozu prvku kritické infrastruktury	3) vzájemná závislost odvětví	b)
III) hospodářskou ztrátu vyšší než 0,25 % HDP	2) ekonomické a společenské činnosti a veřejná bezpečnost	c), d)
IV) nedostupnost druhu služby pro více než 1 600 osob, která není nahraditelná jiným způsobem bez vynaložení nepřiměřených nákladů	1) rozsah a kvalita poskytování základní služby uživatelům	f)
V) oběti na životech s mezní hodnotou více než 100 nebo 200 mrtvých nebo 1 000 zraněných osob vyžadujících lékařské ošetření	2) ekonomické a společenské činnosti a veřejná bezpečnost	c)
VI) narušení veřejné bezpečnosti na významné části správního obvodu obce s rozšířenou působností, které by mohly vyžadovat provedení záchranných a likvidačních prací složkami integrovaného záchranného systému	2) ekonomické a společenské činnosti a veřejná bezpečnost	a), c), e)
VII) kompromitace citlivých údajů o více než 200 000 osobách.	2) ekonomické a společenské činnosti a veřejná bezpečnost	c)

3.2 Dopadová kritéria pro určení informačního systému základní služby

Dopad kybernetického bezpečnostního incidentu v informačním systému nebo síti elektronických komunikací, na jejichž fungování je závislé poskytování služby, může způsobit (I. – VII.):

Dopady musí být naplněny kybernetickým bezpečnostním incidentem, tedy narušením dostupnosti, důvěrnosti nebo integrity v systému, na kterém je závislé poskytování služby

(první sloupec tabulky v příloze vyhlášky). Skrze informační nebo komunikační systém tedy může dojít k následujícím dopadům.

I. Závažné omezení (či narušení) (či nedostupnost) druhu služby postihující více než 25 000, 50 000 nebo 500 000 osob

Cílem kritéria je stanovit hranici dopadu kybernetického bezpečnostního incidentu na poskytování služby pro určitý hraniční počet osob.

Nedostupnost je v rámci tohoto dopadového kritéria zařazena pouze u pododvětví Elektřiny, Zemního plynu a Teplárenství, a to z důvodu jejich oborových specifik, především nenahraditelnosti těchto služeb.

Toto kritérium odpovídá požadavkům § 22a odst. 1 písm. b) bod 1 zákona o kybernetické bezpečnosti a čl. 6 odst. 1 písm. a) směrnice NIS.

50 000 osob je průměrná populace ve správním území obce s rozšířenou působností[2] (členění České republiky dle § 66 zákona č. 128/2000 Sb., o obcích a zákona č. 314/2002 Sb., o stanovení obcí s pověřeným obecním úřadem a stanovení obcí s rozšířenou působností), zaokrouhlená na desetitisíce.

V rámci některých odvětví je hranice zasažených osob stanovena odlišně – jde o odvětví Bankovnictví a Teplárenství a tyto hodnoty jsou:

- V pododvětví Teplárenství **25 000 osob** = polovina průměrné populace ve správním území obce s rozšířenou působností; důvodem nižší hranice v tomto pododvětví jsou oborová specifika teplárenství, teplárny zajišťují dodávky obecně menšímu množství osob.
- V odvětví Bankovnictví **500 000 osob** = desetinásobek průměrné populace ve správním území obce s rozšířenou působností; důvodem vyšší hranice v tomto odvětví je jeho oborové specifikum – služby v odvětví bankovnictví jsou bezprostředně poskytovány velkému množství uživatelů a hranice pro významnost subjektu v tomto odvětví byla proto navýšena.

Závažné omezení či narušení služby znamená, že dochází k závažnému narušení či omezení rozsahu nebo kvality (proti tomu nedostupnost znamená, že služba není dostupná v žádném rozsahu ani kvalitě). Může docházet k výraznému nárůstu čekací doby, nejsou uspokojeni všichni odběratelé, může docházet k ohrožení nebo omezení dostupnosti, některé podpůrné služby nejsou dostupné, nemožnost provádění složitějších úkonů, nutno řídit, případně poskytovat, službu náhradním způsobem apod.

[2] POČET OBYVATEL V OBCÍCH k 1. 1. 2017, © Český statistický úřad, Praha, 2017. s. 9-12. Dostupné z: https://www.czso.cz/csu/czso/pocet-obyvatel-v-obcich-k-112017.

Druhem služby je služba poskytovaná posuzovaným subjektem, který naplňuje odvětvová kritéria. Tato služba je definována ve sloupci označeném jako „Druh služby“. Poskytovatel služby naplňuje speciální kritérium druhu subjektu.

Osobou je každý odběratel služby. Pro určení je možné uvažovat pouze takový počet odběratelů služby, kterým by bylo zařízení schopno službu poskytnout, případně lze také zvážit geografickou polohu či spádovost.

II. Závažné omezení či narušení jiné základní služby nebo omezení či narušení provozu prvku kritické infrastruktury

Kritérium reflektuje závislost jiných, již určených, služeb na posuzovaném druhu služby.

Významnost dopadu, kterou toto kritérium zohledňuje, zde není dána rozsahem nebo závislostí určitého počtu osob na určované službě, ale samotným faktem, že omezení takové služby může omezit či narušit poskytování již určené základní služby, nebo provoz již určeného prvku kritické infrastruktury.

Toto kritérium nemá působnost jen v rámci České republiky, ale s ohledem na harmonizaci základních služeb z pohledu Evropské unie se může jednat také o kritérium přeshraniční. Tento případ nastane, pokud by dopad incidentu ohrozil již určenou zahraniční základní službu v jiném členském státě.

Toto kritérium odpovídá požadavkům § 22a odst. 1 písm. b) bod 3 zákona o kybernetické bezpečnosti a čl. 6 odst. 1 písm. b) směrnice NIS.

Závažné omezení či narušení služby znamená, že dochází k závažnému narušení či omezení rozsahu nebo kvality (proti tomu nedostupnost znamená, že služba není dostupná v žádném rozsahu ani kvalitě). Může docházet k výraznému nárůstu čekací doby, nejsou uspokojeni všichni odběratelé, může docházet k ohrožení nebo omezení dostupnosti, některé podpůrné služby nejsou dostupné, nemožnost provádění složitějších úkonů, nutno řídit, případně poskytovat, službu náhradním způsobem apod.

Omezení či narušení provozu znamená, že služba není poskytována ve standardní kvalitě (např. prodlužuje se doba odbavení odběratele služby oproti standardní době, tvoří se fronty, je snížen kvalitativní standard, může dojít k výpadkům).

Sousloví „**Jiné základní služby“** odkazuje na již určené základní služby v České republice nebo v jiném členském státě.

Provozem prvku kritické infrastruktury se rozumí provoz jakéhokoli již určeného prvku kritické infrastruktury.

Spojka **nebo** znamená, že pro určení je možné naplnit jen první podmínku, jen druhou podmínku nebo také obě podmínky zároveň.

III. Hospodářskou ztrátu vyšší než 0,25 % HDP

Třetím dopadovým kritériem je možnost vzniku hospodářské ztráty, a to ve výši minimálně 0,25 % HDP.

Za tuto hospodářskou ztrátu je považován široký výčet škod, zejména hospodářské ztráty vzniklé z přerušení poskytování služby, sankce nebo náklady na sanaci škod.

Na rozdíl od předchozích kritérií cílí toto kritérium především na hospodářskou situaci, která by v souvislosti s narušením služby nastala.

Toto kritérium odpovídá požadavkům § 22a odst. 1 písm. b) bod 2 zákona o kybernetické bezpečnosti a čl. 6 odst. 1 písm. c) a d) směrnice NIS.

Pro účely výpočtu **hospodářské ztráty** bude do hospodářské ztráty zahrnuto následující:

- Hospodářská ztráta z přerušení činnosti
- Předpokládaná sankce (pokuta) v případě porušení norem, předpisů, smluv, včetně pokuty za znečištění životního prostředí
- Náklady na sanaci škod na životním prostředí, škody na majetku nebo zdraví
- Případné další specifické náklady

IV. Nedostupnost druhu služby pro více než 1 600 osob, která není nahraditelná jiným způsobem bez vynaložení nepřiměřených nákladů

Cílem kritéria je stanovit hranici dopadu kybernetického bezpečnostního incidentu na poskytování služby pro určitý hraniční počet osob, pro které je služba nenahraditelná jiným způsobem.

Toto kritérium se nevyskytuje u pododvětví Elektřina, Zemní plyn a Teplárenství a odvětví Bankovnictví. Důvodem jsou jejich oborová specifika především bezprostřední poskytování služeb velkému množství uživatelů.

Toto kritérium odpovídá požadavkům § 22a odst. 1 písm. b) bod 1 zákona o kybernetické bezpečnosti a čl. 6 odst. 1 písm. f) směrnice NIS.

Kritérium reflektuje průměrný počet obyvatel obce v České republice[3].

Nedostupnost znamená, že služba není dostupná v žádném rozsahu ani kvalitě.

Druhem služby je služba poskytovaná posuzovaným subjektem, který naplňuje odvětvová kritéria. Služba je ve vyhlášce definována ve sloupci „Druh služby“.

[3] POČET OBYVATEL V OBCÍCH k 1. 1. 2017, © Český statistický úřad, Praha, 2017. s. 9-12. Dostupné z: https://www.czso.cz/csu/czso/pocet-obyvatel-v-obcich-k-112017.

Osobou se rozumí primárně každý odběratel služby; pro určení je možné podpůrně uvažovat pouze takový počet odběratelů služby, kterým by bylo zařízení schopno službu poskytnout, případně lze také zvážit geografickou polohu či spádovost.

Nahraditelnost jiným způsobem znamená, že vedle předmětného řešení existují takové způsoby, které umožňují dosáhnout stejného výsledku jiným způsobem. Pro naplnění kritéria je tedy nezbytné, aby poskytovaná služba byla unikátní a nešlo ji jednoduše nahradit. Typicky se bude jednat o síťová odvětví, kde je pouze jedna infrastruktura, která je nenahraditelná.

Při hodnocení „**vynaložení nepřiměřených nákladů**“ musí být přiměřenost zkoumána ve světle konkrétních okolností případu. Je možné se orientovat především s přihlédnutím k finančním nákladům, vynaloženému času a dalších vynaložených nákladů pro alternativní zajištění služby. Pro příklad lze uvést, že aby byla služba zajištěna, bude buď fungovat informační systém, nebo bude poskytovatel služby zajišťovat dvojnásobek personálu, udržovat redundantní technologii apod. V takovém případě lze říci, že toto by bylo nepřiměřené. Jedná se o náklady, které by při vynaložení na zajištění náhradního řešení služby byly v hrubém nepoměru vzhledem ke standardním způsobům, kterými je služba běžně zajištěna.

V. Oběti na životech s mezní hodnotou více než 100 nebo 200 mrtvých nebo 1 000 zraněných osob vyžadujících lékařské ošetření

Počet 100 nebo 200 obětí na životech nebo počet 1 000 zraněných vyžadujících lékařské ošetření, ke kterým by došlo v souvislosti s narušením předmětné služby v důsledku kybernetického bezpečnostního incidentu v informačním systému.

Toto kritérium odpovídá požadavkům § 22a odst. 1 písm. b) bod 2 zákona o kybernetické bezpečnosti a čl. 6 odst. 1 písm. c) směrnice NIS.

Kritérium se liší v odvětví Letecká doprava, kde je hranice stanovena na 200 mrtvých. Toto kritérium se nevyskytuje u odvětví Bankovnictví, Infrastruktury finančních trhů ani Digitální infrastruktury z toho důvodu, že nelze očekávat přímou souvislost dopadu kybernetického bezpečnostního incidentu v těchto odvětvích s oběťmi na životech.

VI. Narušení veřejné bezpečnosti na významné části správního obvodu obce s rozšířenou působností, které by mohlo vyžadovat provedení záchranných a likvidačních prací složkami integrovaného záchranného systému

Narušením veřejné bezpečnosti je především stav, kdy je ohrožena bezpečnost státu, či jednotlivých státních orgánů nebo institucí, stejně jako když je ohrožena bezpečnost jednotlivce nebo veřejný či soukromý majetek.

Významnou část je možno chápat jak z pohledu rozlohy území, tak z pohledu počtu koncentrace obyvatelstva nebo významných podniků.

Toto kritérium odpovídá požadavkům § 22a odst. 1 písm. b) bod 2 zákona o kybernetické bezpečnosti a čl. 6 odst. 1 písm. a), c) a e) směrnice NIS.

Veřejnou bezpečností se rozumí ochrana jednotlivce i společnosti proti útokům, jež ohrožují např. bezpečnost státu či jednotlivých státních orgánů, institucí a funkcí, bezpečnost jednotlivce, zejména jeho čest, důstojnost, svobodu a fyzickou integritu nebo majetek státu či jednotlivce.

Významnou částí správního území obce s rozšířenou působností se rozumí území posuzované jak kvantitativním kritériem (např. rozloha zasaženého území), tak kvalitativním kritériem (co se týče koncentrace obyvatel, významných podniků, správních center apod.). Obec s rozšířenou působností je určena členěním České republiky dle § 66 zákona č. 128/2000 Sb., o obcích a zákona č. 314/2002 Sb., o stanovení obcí s pověřeným obecním úřadem a stanovení obcí s rozšířenou působností.

Záchranné práce jsou činnosti k odvrácení nebo omezení bezprostředního působení rizik vzniklých mimořádnou událostí, zejména ve vztahu k ohrožení života, zdraví, majetku nebo životního prostředí, a vedoucí k přerušení jejich příčin.

Likvidační práce jsou činnosti k odstranění následků způsobených mimořádnou událostí.

Základními složkami integrovaného záchranného systému jsou Hasičský záchranný sbor České republiky, jednotky požární ochrany zařazené do plošného pokrytí kraje jednotkami požární ochrany, poskytovatelé zdravotnické záchranné služby a Policie České republiky.

Ostatními složkami integrovaného záchranného systému jsou vyčleněné síly a prostředky ozbrojených sil, obecní policie, orgány ochrany veřejného zdraví, havarijní, pohotovostní, odborné a jiné služby, zařízení civilní ochrany a neziskové organizace a sdružení občanů, která lze využít k záchranným a likvidačním pracím.

VII. Kompromitace citlivých osobních údajů o více než 200 000 osobách

Toto kritérium je použito pouze v odvětví Zdravotnictví.

Kritérium reflektuje potřebu chránit systémy s velkým počtem citlivých osobních údajů.

Osobním údajem se rozumí jakákoliv informace týkající se určeného nebo určitelného subjektu. Subjekt se považuje za určený nebo určitelný, jestliže jej lze přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.[4]

[4] V okamžiku nabytí účinnosti vyhlášky podle § 4 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

Citlivým údajem se rozumí osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů.[5]

Toto kritérium odpovídá požadavkům § 22a odst. 1 písm. b) bod 2 zákona o kybernetické bezpečnosti a čl. 6 odst. 1 písm. c) směrnice NIS.

Přímou identifikací se rozumí, že osobu lze přímo ztotožnit, a to i jinak, než jen na základě informací, kterými sám správce údajů disponuje.

Nepřímou identifikací je proces, který povede k určení konkrétní osoby, ale až po vynaložení většího úsilí, neboť správce např. disponuje pouze jejím popisem či fotografií, ale ne identifikačními údaji.

Číslo pro identifikaci je datum narození, rodné číslo, personální číslo přidělené zaměstnavatelem, telefonní číslo, IP adresa nebo např. číslo bankovního účtu.

Kód pro identifikaci je např. identifikátor datové schránky fyzické osoby nebo hostname počítače.

Fyzická nebo fyziologická identita je vzhled dané osoby, tvar obličeje, hlavy i celého těla, výška, váha, barva vlasů nebo očí.

Psychická identita se rozumí informace o chování, reakcích dané osoby v určitých situacích nebo o motivaci takového chování.

Ekonomickou identitou jsou informace o majetku, pohledávkách i závazcích, o výši nebo zdroji příjmů.

Kulturní identita obsahuje zájmy, záliby a schopnosti osoby.

Sociální identita zahrnuje rodinný stav, sociální původ, vzdělání, zaměstnání či jiné aktivity.

Národnostním původem se rozumí příslušnost k určitému národu (Obecné nařízení o ochraně osobních údajů[6] toto kritérium již výslovně neuvádí).

Rasový původ znamená příslušnost k určité rase.

---

[5] V okamžiku nabytí účinnosti vyhlášky podle § 4 písm. b) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

[6] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

Etnický původ znamená příslušnost k určitému etniku.

Politické postoje nezahrnují bez dalšího informace o členství v politické straně nebo hnutí.

Členství v odborových organizacích zahrnuje informace o členství osoby v odborových organizacích.

Náboženstvím se rozumí především informace o členství osoby v registrovaných církvích.

Filozofickým přesvědčením se rozumí především vztah osoby k neregistrovaným náboženským nebo jiným společnostem.

Odsouzením za trestný čin se rozumí informace pouze o skutečném odsouzení, nikoliv o jiných fázích trestního řízení (Obecné nařízení o ochraně osobních údajů toto kritérium již výslovně neuvádí).

Zdravotním stavem se rozumí informace o konkrétní prodělané nebo aktuální nemoci, úrazu dané osoby nebo o podstoupené léčbě, informace o prodělaných vyšetřeních, údaj o hospitalizaci nebo údaj o těhotenství.

Sexuální život zahrnuje informace o sexuálních partnerech osoby nebo jí provozovaných, vyhledávaných či preferovaných sexuálních praktikách nebo aktivitách.

Genetickým údajem informace získané rozborem lidské deoxyribonukleové kyseliny (DNA).

Biometrickým údajem, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů se rozumí otisky prstů, dlaně či chodidla, obraz oční sítnice nebo duhovky, záznam dynamického projevu chůze, ale i rozbor tváře či hlasového projevu.

Osobou je v tomto případě každý, o kom je v informačním systému veden samostatný záznam.

4 Popis posouzení naplnění kritérií

Text této kapitoly uvádí příklad a přímo odkazuje na přílohu vyhlášky, konkrétně tabulku odvětví Energetika, pododvětví Elektřina. Tento proces ilustruje obrázek č. 2.

Pro to, aby byl subjekt určen jako provozovatel základní služby, musí provozovat službu v některých, zákonem o kybernetické bezpečnosti definovaných a vyhlášce konkretizovaných odvětví. Poskytování této služby musí být závislé na informačním systému nebo síti elektronických komunikací (§ 2 písm. i) a j) zákona o kybernetické bezpečnosti). Poté může být přistoupeno k detailnímu posouzení naplnění kritérií.

První sloupec tabulky v příloze vyhlášky definuje činnost (službu), na kterou regulace cílí. V tomto případě jde tedy o činnost spočívající ve výrobě elektřiny.

Druhý sloupec tabulky definuje subjekt, který službu poskytuje. Jde tedy o definici množiny subjektů – **provozovatelů služeb** – na kterou by se regulace **mohla** vztahovat. K definicím v prvním a druhém sloupci tabulky bylo využito národní legislativy, případně evropských směrnic a nařízení. V tomto případě bude druhem subjektu takový subjekt, který naplňuje definici výrobce elektřiny podle zákona č. 458/2000 Sb., energetického zákona.

Třetí sloupec tabulky zavádí omezení na nejvýznamnější provozovatele služeb v daném odvětví. Tím je v tomto příkladu podmínka, že výrobna posuzovaného subjektu musí dosahovat celkovým instalovaným elektrickým výkonem nejméně 500 MW.

Poslední sloupec tabulky stanovuje dopadová kritéria, která musí naplnit možný dopad incidentu v informačním systému nebo síti elektronických komunikací, které jsou využívány pro poskytování v předchozích sloupcích definované služby. Při posuzování, zda subjekt naplňuje kritéria, bude v tabulce postupováno od obecného ke konkrétnímu.

Zjednodušeně:

Odvětví – vychází ze směrnice NIS a jsou definována § 2 písm. j) zákona o kybernetické bezpečnosti.

Pododvětví – vychází ze směrnice NIS, konkretizují odvětví a jsou stanovena pouze v některých odvětvích.

Sloupec „**Druh služby**“ definuje službu v rámci odvětví národního hospodářství, na které regulace cílí.

Sloupec „**Druh subjektu**“ říká, které subjekty, poskytující danou službu v daném odvětví nebo pododvětví, budou posuzovány. Jedná se o množinu, z níž budou určeni provozovatelé základních služeb.

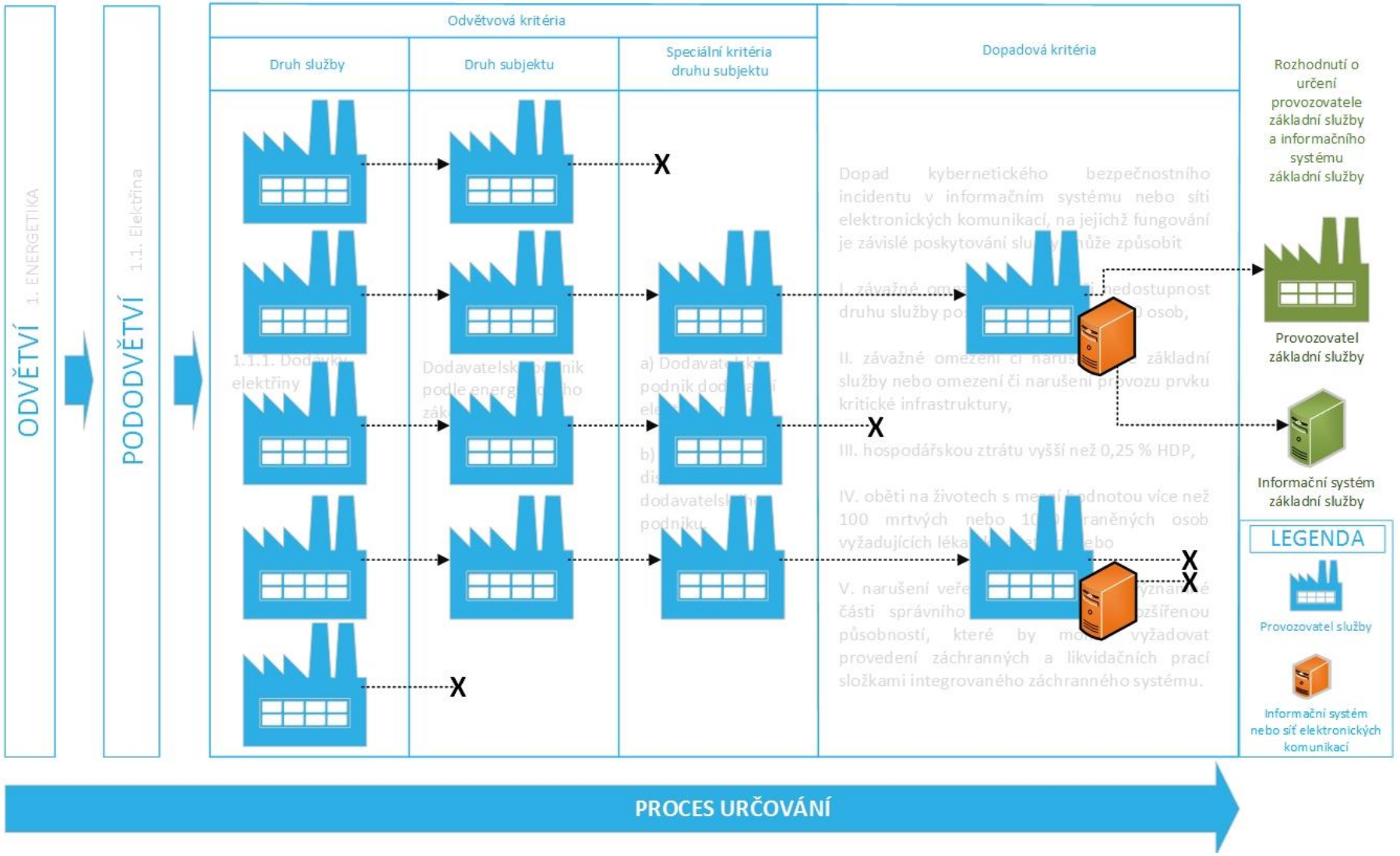
Sloupec „**Speciální kritéria druhu subjektu**“ slouží k filtraci provozovatelů dané služby na provozovatele významné, na které se regulace zaměřuje, a ostatní, kteří v objektu zájmu regulace nejsou. Je zaměřen na kvalitu nebo kvantitu poskytované služby.

Poslední sloupec „**Dopadová kritéria**“, tedy dopad kybernetického bezpečnostního incidentu v informačním systému nebo síti elektronických komunikací, na jehož fungování je závislé poskytování služby, vyjadřuje dopady na společnost, které dosahují takového významu, že je nutné jim předcházet. Systémy, jejichž narušení by takové dopady mohlo způsobit, je nutné zabezpečit a chránit.

Aby byl subjekt určen, musí **ve stejném řádku tabulky naplnit alespoň jedno kritérium z každého sloupce**. Tedy k druhu služby, druhu subjektu a speciálnímu kritériu druhu subjektu uvedeným na témž řádku přílohy k této vyhlášce se vztahují dopadová kritéria stanovená pro dané odvětví, popřípadě pododvětví.

Samotné určování ze strany NÚKIB bude probíhat následovně (příklad: 1. Energetika – 1.1. Elektřina – 1.1.1. Výroba elektřiny).

1) Bude vyžádán seznam výrobců elektřiny podle zákona č. 458/2000 Sb., energetický zákon,
2) budou vybráni pouze ti výrobci, kteří splní alespoň jedno speciální kritérium druhu subjektu,
3) se subjekty vybranými dle předchozího bodu NÚKIB provede posouzení naplnění dopadových kritérií a
4) systémy, které naplní dopadová kritéria, budou určeny jako informační systémy základní služby. Subjekt odpovědný za poskytování služby bude určen jako provozovatel základní služby.



Obrázek č. 2: Schéma určení PZS – průchod posuzovaného subjektu dopadovými a odvětvovými kritérii (příklad: 1. Energetika – 1.1. Elektřina – 1.1.1. Výroba elektřiny)

Verze dokumentu

Datum	Verze	Změněno (jméno)	Změna
4. 1. 2018	1.0	Odd. RAP	Vytvoření dokumentu
20. 3. 2018	1.1	Odd. RAP	Grafická úprava bez úprav textu
29. 3. 2018	1.2	Odd. RAP	Oprava Obrázku 1
12. 11. 2018	1.3	Odb. regulace	Grafická úprava
28. 1. 2019	1.4	Odb. regulace	Změna kontaktních údajů
22. 12. 2022	1.5	Odb. regulace	Změna kontaktních údajů