Kybernetická bezpečnost u objektů nakládajících s vybranými nebezpečnými chemickými látkami nebo chemickými směsmi – rešerše stavu v ČR

1. Úvod

Cílem tohoto dokumentu je popsat současné legislativní, procesní a technické postupy v oblasti kybernetické bezpečnosti vztahující se na objekty nakládajících s vybranými nebezpečnými chemickými látkami, objekty spadající pod zákon č.224/2015 Sb.

Dále identifikace provozovatelů základních služeb manipulujícími s vybranými nebezpečnými chemickými látkami nebo chemickými směsmi v souvislosti s prevencí závažných havárií.

Níže jsou rozebrány jednotlivé zákony, vyhlášky a směrnice, které platí pro Českou republiku a regulují výše uvedenou oblast provozovatelů.

V souvislosti s tím jsou také definovány platné procesy, které pomáhají uvedeným provozovatelům identifikovat klíčové informační a komunikační systémy a nastavit pro jejich správnou funkci technické i metodické postupy s cílem minimalizovat, či úplně eliminovat kybernetické útoky.

2. Legislativní část

2.1. Definice objektů spadajících do regulace Zákona o prevenci závažných havárií způsobených nebezpečnými chemickými látkami a směsmi

Objekty jsou definovány zákonem č.224/2015 Sb. a příslušnými vyhláškami.

2.2. Definice provozovatelů informačních a komunikačních systémů

V oblasti kybernetické bezpečnosti v souvislosti s prevencí závažných havárií je hlavním garantem a regulátorem pro ČR Národní úřad pro kybernetickou a informační bezpečnosti (NÚKIB), Oddělení regulace veřejného sektoru (dále NÚKIB). Tento úřad definuje, identifikuje a reguluje tzv. provozovatele informačních a komunikačních systémů, kdy vychází z níže uvedeného legislativního rámce.

Současná legislativa ČR definuje základní právní předpis upravující práva a povinnosti osob, jakož i pravomoc a působnost orgánů veřejné moci v oblasti kybernetické bezpečnosti podle **Zákon o kybernetické** bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), **č.181/2014 Sb.** [10], ze dne 29. srpna 2014, platný od 1.1. 2015.
Zákon zpracovává příslušnou Směrnici Evropského parlamentu a Rady 2016/1148/EU [11] (známou jako NIS) a upravuje zajišťování bezpečnosti sítí elektronických komunikací a informačních systémů.

V roce 2017 proběhly dvě obsahově významné novely zákona o kybernetické bezpečnosti, a to prostřednictvím zákona č. 104/2017 Sb. [12] s účinností od 1.7. 2017 a zákona č.205/2017 Sb. [13] s účinností od 1. 8. 2017. K aktuálnímu datu proběhly ještě následující novelizace tohoto zákona – novelizace zákonem č. 183/2017 Sb., [14] zákonem č. 35/2018 Sb. [15], zákonem č. 111/2019 Sb. [16] a aktuálně poslední novelizace zákonem č. 12/2020 Sb. [17] Aktuální znění zákona je účinné od 1. února 2020.

Zákon o kybernetické bezpečnosti definuje oblasti provozovatelů informačních a komunikačních systémů pro specifické oblasti a to sice:

- Informační a komunikační systémy kritické informační infrastruktury.
- Významné informační a komunikační systémy.
- Informační a komunikační systémy provozovatelů základních služeb.
- Poskytovatelé digitálních služeb.

Prováděcí **nařízení komise EU 2018/151** [22], **kterým se stanoví pravidla pro uplatňování směrnice Evropského parlamentu a Rady EU 2016/1148, směrnice NIS**, je přímo aplikovatelné a pro poskytovatele digitálních služeb je tedy závazné. Toto prováděcí nařízení je účinné od 10.5. 2018
Prováděcí nařízení obsahuje bližší upřesnění bezpečnostních opatření, které musí poskytovatelé digitálních služeb (§ 3 písm. h) podle ZKB) zohledňovat při řízení bezpečnostních rizik, jimž jsou vystaveny sítě a informační systémy, a dále bližší upřesnění parametrů pro posuzování toho, zda je dopad incidentu významný.

Jednotlivé oblasti jsou poté regulovány ještě níže uvedenými vyhláškami a nařízeními vlády:

Vyhláška o kybernetické bezpečnosti č. 82/2018 Sb. [18] o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), která upravuje:

- obsah a strukturu bezpečnostní dokumentace,
- obsah a rozsah bezpečnostních opatření,
- typy, kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů,
- náležitosti a způsob hlášení kybernetického bezpečnostního incidentu,
- náležitosti oznámení o provedení reaktivního opatření a jeho výsledku,
- vzor oznámení kontaktních údajů a jeho formu,
- způsob likvidace dat, provozních údajů, informací a jejich kopií.

Nařízení vlády č. 432/2010 Sb. [19], o kritériích pro určení prvku kritické infrastruktury definuje a identifikuje informační a komunikační systémy kritické informační infrastruktury. Je platné od 30.12.2010 a definuje průřezová a odvětvová kritéria pro určení prvku kritické infrastruktury. V příloze k tomuto nařízení je definováno 9 odvětví, včetně jednotlivých odvětvových kritérií pro určení prvku kritické infrastruktury. Nařízení nabylo účinnosti

1.1. 2011. V souvislosti se zahrnutím oblasti kybernetické bezpečnosti do odvětvových kritérií proběhla novela nařízením vlády č. 315/2014 Sb., s účinnosti od 1.1. 2015.

Vyhláška č. 317/2014 Sb., [20] **o významných informačních systémech a jejich určujících kritériích** upravuje definici a identifikaci významných informačních a komunikačních systémů a stanoví kritéria pro jejich určení. Vstoupila v platnost 19.12. 2014.
V roce 2020 byla přijata novela vyhlášky, která má za cíl zpřesnit kritéria pro určení toho, zda je daný informační systém významný. Nabytí účinnosti celého znění vyhlášky je rozloženo do tří období (měnit se bude znění § 2, první období nastává 1.1. 2021). Kompletní znění nabude účinnosti dne 1.1. 2023.

Vyhláška č. 437/2017 Sb., [21] **o kritériích pro určení provozovatele základní služby** upravuje definici a identifikaci informačních a komunikačních systémů provozovatelů základních služeb. Vstoupila v platnost 1.2. 2018. Vyhlášku zpracoval Národní úřad pro kybernetickou a informační bezpečnost ve spolupráci s odbornou veřejností. Vyhláška zpracovává požadavky Směrnice Evropského parlamentu a Rady EU 2016/1148, NIS. Vyhláška upravuje odvětvová a dopadová kritéria pro určení provozovatele základní služby a vymezení významnosti dopadu narušení základní služby na zabezpečení společenských nebo ekonomických činností podle § 22a odst. 1 zákona o kybernetické bezpečnosti.
Od 1.1. 2021 je účinné nové znění vyhlášky, kterým se v odvětví zdravotnictví mění dvě stávající kritéria a doplňují dvě nová kritéria.

3. Procesní část

3.1. Metodické pokyny a dokumenty k zařazení objektu a provozovatele

Otázkou je identifikací a zařazením těchto objektů, jako provozovatelů informačních a komunikačních systémů základních služeb, které spadají pod regulaci zákona **č. 181/2014 Sb**., o kybernetické bezpečnosti.

V tomto kroku by měly pomoci dokumenty vydané NÚKIB, a to sice: [23] **- Minimální bezpečnostní standard** a [24] – **Provozovatel informačního nebo komunikačního systému podle zákona o kybernetické bezpečnosti**, které shrnují nejdůležitější body týkajících se definice a identifikace institutu, jako provozovatele informačního a komunikačního systému spadajícího/nespadajícího pod regulaci zákona o kybernetické bezpečnosti.

Vodítka pro hodnocení důležitosti informačních a komunikačních systémů, hodnocení důležitost aktiv a s tím související řízení rizik, odvození požadavků na bezpečnost zpracovávaných informací a informačních systémů lze poté nalézt v dokumentu [25] – **Metodika k vodítkům pro hodnocení dopadů**.

Z pohledu metodických pokynů pro provozovatele systémů základních služeb jsou stěžejní dokumenty [26] – **Informace o institutu základní služby** a [27] – **Průvodce určováním provozovatele základní služby**, které poskytují informace o institutu základní služby a jsou primárními dokumenty pro určení objektu s vybranými nebezpečnými chemickými látkami

nebo chemickými směsmi současně jako provozovatele informačních a komunikačních systémů základní služby.

Konkrétní doporučení v oblasti využití kryptografických prostředků pro systémy spadající do zákona o kybernetické bezpečnosti poté přináší dokument [28] – **Minimální požadavky na kryptografické algoritmy**. Tato oblast je detailně rozebrána v kapitole 4 tohoto dokumentu.

Následně dle metodických dokumentů od NÚKIB dojde k popisu definice a identifikace provozovatelů systému základních služeb.

3.2. Definice a identifikace objektu dle zákona č. 224/2015 Sb. a příslušných metodik

Zařazení objektu do regulace zákonem o prevenci závažných havárií je definováno zákonem č.224/2015 Sb., případně podpořeno metodickými pokyny MŽP.

3.3. Definice a identifikace provozovatele systému základních služeb dle zákona č. 181/2014 Sb. a příslušných metodik

V případě, že objekt spadá pod regulaci zákona č. 224/2015 sb., je u něj nutné dále vyhodnotit, zda také není současně provozovatelem systémů základních služeb z pohledu plnění zákona č. 181/2014 Sb., zákon o kybernetické bezpečnosti.

V legislativní části tohoto dokumentu (podkapitola 2.1) byly definovány oblasti provozovatelů informačních a komunikačních systémů pro specifické oblasti, kdy dle **§ 2 písm. i) zákona č.181/2014 Sb.** jsou **objekty manipulující s vybranými nebezpečnými chemickými látkami nebo chemickými směsmi řazeny do oblasti provozovatelů základních služeb, pokud provozují informační nebo komunikační systém, který splňuje daná odvětvová a dopadová kritéria (dle § 28 odst. 2 písm. e) 181/2014 Sb.).**

Z pohledu plnění této definice je potřeba jí rozebrat na jednotlivé faktory, které musí daný objekt plnit:

- Objekt provozuje činnost v odvětví s vybranými nebezpečnými chemickými látkami nebo chemickými směsmi – určuje zákon č. 224/2015 Sb. viz podkapitola 3.2
- Provozuje informační nebo komunikační systém – objekt musí identifikovat, zda provozuje informační a komunikační systémy, které jsou pro instituci klíčové a v případě havárie by mohly naplňovat níže uvedená dopadová kritéria. K této identifikaci a zhodnocení případných dopadů nejlépe poslouží již výše zmíněné dokumenty [24] a [25].
- Splňuje daná odvětvová a dopadová kritéria – podle vyhlášky č. 437/2017 Sb. a zákon č. 181/2014 Sb. viz níže.

Kritéria pro provozovatele systémů základní služby jsou definována ve vyhlášce č. 437/2017 Sb. a dělí se na:

- Odvětvová kritéria
  - Druhy služby
  - Druh subjektu
  - Speciální kritéria druhu subjektu

- Dopadová kritéria

Pro objekty manipulující s vybranými nebezpečnými chemickými látkami nebo chemickými směsmi jsou konkrétní kritéria uvedena v Příloze vyhlášky č. 437/2017, článku 8:

Tab. 1 Odvětvová a dopadová kritéria pro objekty manipulující s vybranými nebezpečnými chemickými látkami nebo chemickými směsmi dle vyhlášky. 437/2017 Sb.

Odvětvová kritéria (vycházejí ze směrnice **2016/1148/EU (NIS)**, kde ČR přidala právě oblast chem. průmyslu)			**Dopadová kritéria** (vycházejí ze směrnice **NIS (čl. 6 odst. 1)** a zákona **č. 181/2014 Sb. (§ 22a odst. 1 písm. b))**
Druh služby	**Druh subjektu**	**Speciální kritéria druhu subjektu**	
8.1. Výroba technických plynů	Výrobce technických plynů	-	Dopad kybernetického bezpečnostního incidentu v informačním systému nebo síti elektronických komunikací, na jejichž fungování je závislé poskytování služby, může způsobit I. závažné omezení či narušení druhu služby postihující více než 50000 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 1600 osob, která není nahraditelná jiným způsobem bez vynaložení nepřiměřených nákladů, V. oběti na životech s mezní hodnotou více než 100 mrtvých nebo 1000 zraněných osob vyžadujících lékařské ošetření nebo, VI. narušení veřejné bezpečnosti na významné části správního
8.2. Výroba hnojiv nebo dusíkatých sloučenin	Výrobce hnojiv nebo dusíkatých sloučenin	-	
8.3. Výroba pesticidů nebo jiných agrochemických přípravků	Výrobce pesticidů nebo jiných agrochemických přípravků	-	
8.4. Výroba výbušnin	Výrobce výbušnin	-	
8.5. Zpracování jaderného paliva	Subjekt zpracovávající jaderné palivo	-	
8.6. Výroba základních farmaceutických výrobků	Výrobce základních farmaceutických výrobků	-	
8.7. Výroba farmaceutických přípravků	Výrobce farmaceutických přípravků	-	
8.8. Výroba jiných základních anorganických látek	Výrobce jiných základních anorganických látek	-	

8.9. Výroba jiných základních organických chemických látek	Výrobce jiných základních organických chemických látek	-	obvodu obce s rozšířenou působností, které by mohlo vyžadovat provedení záchranných a likvidačních prací složkami integrovaného záchranného systému.

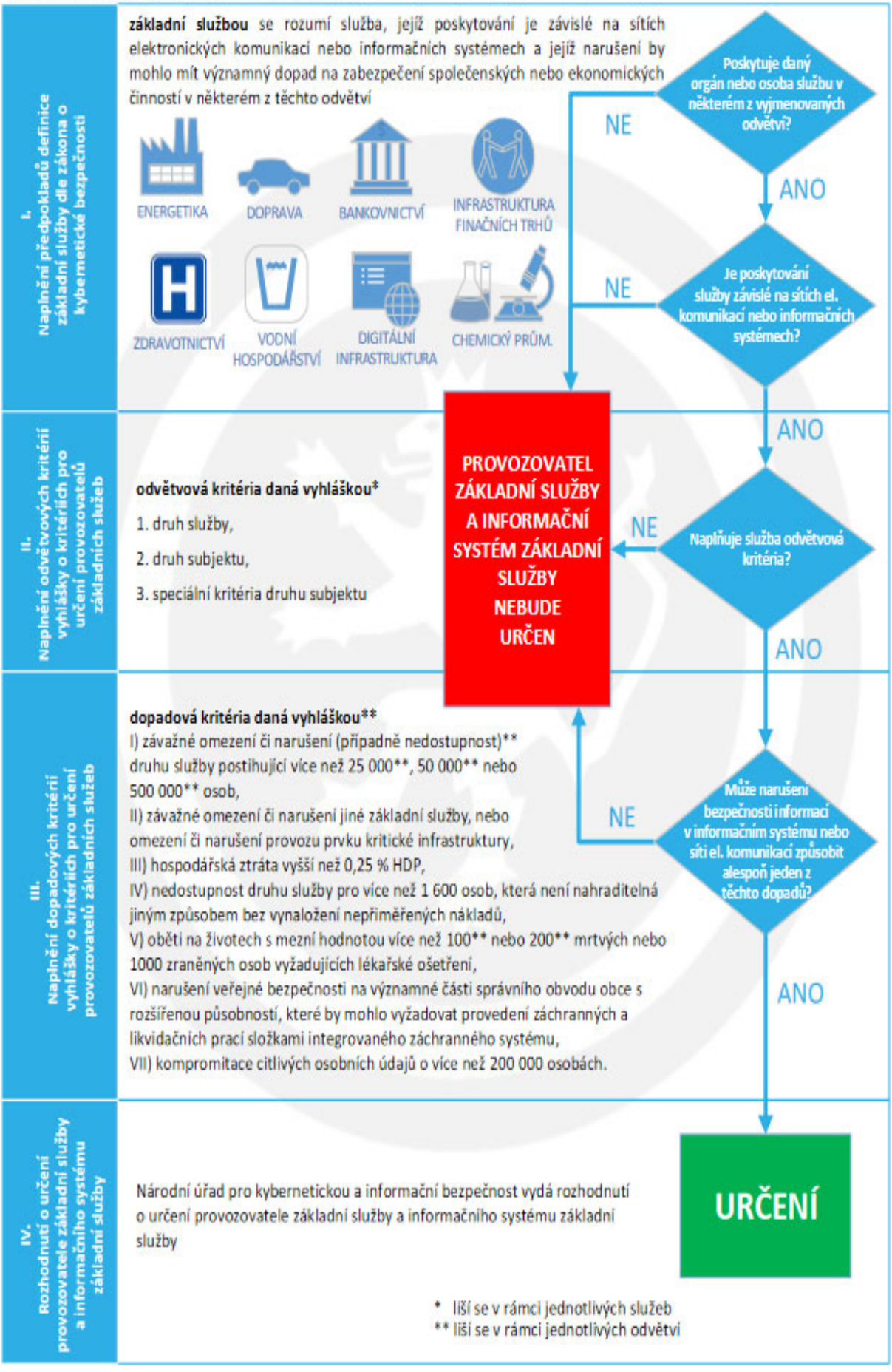
Z výše popsaných hledisek vychází i **§ 22a odst. 1 písm. b**) zákona **č. 181/2014 Sb.** o kybernetické bezpečnosti, který stanoví, že v rámci dopadových kritérií má být zohledněn dopad kybernetického bezpečnostního incidentu zejména na:

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

Pro jasné a přesné určení provozovatele systémů základní služeb dle výše uvedených definic a kritérií lze také využít dokumenty [26, 27], které shrnují uvedené poznatky a nabízí například také grafické schéma určení.

Obr. 1 Proces určení provozovatele základní služby a informačního systému základní služby (plné rozlišení: https://www.nukib.cz/download/publikace/podpurne_materialy/Schema_rozhodovani_PZS_v2.1.pdf).

Proces určení provozovatele základní služby a informačního systému základní služby dle zákona o kybernetické bezpečnosti a vyhlášky o kritériích pro určení provozovatelů základních služeb



Pokud objekt plní výše uvedenou definici a je určen jako provozovatel systémů základní služby, dochází k zahájení správního řízení mezi provozovatelem a NÚKIB.

V průběhu správního řízení NÚKIB s objektem konzultuje nutnost a účel provozovaného informačního nebo komunikačního systému, žádá popis systému a žádá o plnění požadavků dle vyhlášky **č. 82/2018 Sb.** o kybernetické bezpečnosti. Dochází také k vyplnění dotazníku [29], který NÚKIB poskytuje provozovateli.

Tato vyhláška definuje organizační a technická opatření, která jsou blíže popsána v kapitole 4. Kromě toho vyhláška definuje pojem kybernetický bezpečnostní incident, jeho formát a primárně způsoby jeho řešení a určení reaktivních opatření (hlášení incidentu národnímu CERT týmu, konzultace s NÚKIB, nezávislá kybernetická forenzní analýza).

Na aplikaci bezpečnostních požadavků má provozovatel vyhrazenou dobu 12 měsíců od zahájení správního řízení, kdy pro ověření plnění požadavků může realizovat bezpečnostní audity, jejichž výsledek je následně diskutován NÚKIB. Úřad vystupuje v roli konzultanta a v případě potřeby vyžaduje odůvodnění plnění/neplnění bezpečnostních požadavků.

4. Technická část

V této kapitole jsou rozebrány dostupné dokumenty a vyhlášky, které definují konkrétní organizační, manažerská a technická protiopatření v případě prevence havárií způsobených kybernetickým útokem u objektů manipulujících s vybranými nebezpečnými chemickými látkami nebo chemickými směsmi.

Za základní podpůrný materiál, který může sloužit jako vhodný dokument pro návrhy kybernetických bezpečnostních opatření, lze považovat [23] – **Minimální bezpečnostní standard**, který vydává NÚKIB spolu s Národní agenturou pro komunikační a informační technologie, s.p. (dale NAKIT). Tento dokument je však určen pro subjekty, které **nespadají pod zákon č. 181/2014 Sb. o kybernetické bezpečnosti**. Nicméně uvedený dokument se opírá o Vyhlášku **č. 82/2018 Sb.**, která je platná i pro subjekty **spadající pod regulaci zákona č.181/2014 Sb.**, což je i případ provozovatele systému základních služeb.

Tento dokument je rozdělen na manažerskou a technickou část, kdy jednotlivé sekce popisují níže uvedené oblasti a shrnují doporučení pro uvedenou problematiku:

Manažerská část:

- Vedení organizace musí projevit podporu a poskytnou a přidělit přiměřené lidské, ekonomické a časové zdroje, jasná definice bezpečnostních rolí v organizaci.
- Doporučeno vytvoření plánu bezpečnostních opatření.
- Klasifikace hodnoty informací, metodika pro identifikaci a hodnocení informací – tabulka rozdělení do 3 úrovní hodnocení informací a úrovní ochrany.
- Kontrola dodavatelů, neuzavírání smlouvy se stejnými externími bezpečnostními auditory a bezpečnostními odborníky v případě outsourcing služeb.
- Řízení lidských zdrojů – školení zaměstnanců, min. 1x ročně na základy kybernetické bezpečnosti, plány školení nových zaměstnanců, klíčový zaměstnanci – specializovaná

školení – seznam bezpečnostních profesí je uveden ve vyhlášce **č. 82/2018 Sb., příloha 6 - Výčet požadavků na bezpečnostní role**.

- Řízení změn z pohledu aktualizací a změny konfigurace informačních a komunikačních systémů, dokumentace změn, podle potřeby provést penetrační testování.
- Řízení kontinuity činností – dostupnost Business Continuity Plan a Disaster Recovery Plán – seznam bodů pro tyto plány z pohledu informační a komunikační bezpečnosti.
- Audit kybernetické bezpečnosti – pravidelně provádět bezpečnostní audit od nezávislých subjektů.

Technická část:

- Fyzická bezpečnost – definice perimetru, přístupy, ochrana majetku, kamery, bezpečnostní agentura, pohyb a vstup po autentizaci, zamykání prostor, nezávislý zdroj napájení pro klíčové systémy.
- Řízení přístupů – definice rolí, MDM pro BYOB, kontrola připojovaných periferií, AAA, pravidla pro hesla
- Ochrana před škodlivým kódem – segmentovaná síť, SW pro ochranu (firewall), pravidelná aktualizace, zálohování.
- Kybernetické události a incidenty – procesy stanovení a řešení incidentů, hlášení CERT CSIRT, logování a monitoring, definice SEC, OS a AP logů a doba jejich uchovávání.
- Aplikační bezpečnost – provádět aktualizace, testování dle procesů a pravidel pro testovací data, periodické penetrační testování, anonymizace dat při testování.
- Využití moderních kryptografických prostředků – šifrování dat, využití aktuálních šifer a cipher suit.
- Dostupnost informací – řízení úrovní dostupnost – HA, nalezení SPOF, zálohování.
- Cloudové služby – podmínky provozu dat na cloudem, smlouvy s poskytovali cloudových služeb, plnění vyhlášek a legislativy, certifikátu ČSN ISO/IEC 27001 nebo auditní zprávu SOC 2 Type II (AT101).
- Další požadavky - řízení výjimek, ochrana webových aplikací a portálů dle OWASP.
- Přílohy – Seznam doporučovaných bezpečnostních politik a dokumentace pro provozovatele, Vzorový příklad – Plán kontinuity činností (BCP) v případě prevence havárie a kybernetického útoku.

Dalším stěžejním dokumentem, který definuje technické prostředky a opatření tentokrát již také pro provozovatele systémů základních služeb, kteří **spadají do regulace zákona č.181/2014 Sb.** je **Vyhláška č. 82/2018 Sb.**

Jak již bylo uvedeno výše, tato vyhláška je rozdělena do několika částí, kde stěžejní jsou části druhá až čtvrtá, které reflektují popis bezpečnostních opatření, definují kybernetický bezpečnostní incident a nastavují reaktivní opatření a kontaktní údaje.

Část druhá – Bezpečnostní opatření byla inspirací pro vytvoření výše zmiňovaného dokumentu [23], jelikož jednotlivé paragrafy a články této části odpovídají dílčím odstavcům dokumentu a uvedená doporučení jsou v případě této části vyhlášky a dokumentu [23] ve shodě.

Část třetí – Kybernetický bezpečnostní incident přináší kategorizaci bezpečnostních incidentů a uvádí formu a náležitosti hlášení kybernetického bezpečnostních incidentu –

zaslání elektronického formuláře na adresu NÚKIB nebo národnímu CERT, podle závažnosti a dopadu incidentu.

Část čtvrtá – Reaktivní opatření a kontaktní údaje definuje, jakým způsobem jsou řešena protiopatření na proběhnuvší kybernetický bezpečnostní incident a uvádí kontaktní údaje na úřad a národní CERT tým.

Posledním dokumentem, který definuje konkrétní technická doporučení v oblasti kybernetické bezpečnosti informačních a komunikačních systémů je již zmiňovaný dokument [28] - **Minimální požadavky na kryptografické algoritmy – doporučení v oblasti kryptografických prostředků**. V tomto materiálu je možné nalézt doporučované typy algoritmů pro Symetrické blokové a proudové šifry, dále pak doporučované módy těchto šifer pro operace šifrování, ochranu integrity a autentizaci. Dále jsou uváděny doporučované algoritmy pro Asymetrickou kryptografii, technologii digitálního podpisu a pro proces výměny a distribuci klíčů. Závěrem jsou uvedeny preferované algoritmy ohlašovacích funkcí.

5. Závěr

Tento materiál reflektuje současný stav, k 25.5.2021, legislativních požadavků z pohledu kybernetické bezpečnosti u objektů manipulujících s vybranými nebezpečnými chemickými látkami nebo chemickými směsmi, kdy pro oblast prevence havárií je určující, zda jsou objekty zároveň také provozovateli systémů základních služeb.

Uvedený legislativní rámec určuje, zda takový objekt provozuje informační a komunikační systém a tím pádem se stává provozovatelem systému základní služby podle zákona o kybernetické bezpečnosti.

Na základě tohoto určení je provozovatel povinen realizovat procesní postupy, které jednak jednoznačně určují, které systémy a části objektu spadají pod regulaci, a které nikoliv, a dále také dávají provozovateli představu o tom, jakým způsobem komunikovat s regulačním orgánem.

Závěrečná část dokumentu poté představuje veřejně dostupné materiály, které slouží jako zdroj konkrétních technických doporučení a protiopatření, které by objekt zařazený podle výše uvedených legislativních a procesních postupů, měl splňovat.

Tento dokument by měl pomoci objektům, resp. provozovatelům spadajícím do režimu zákona č.224/2015 Sb., o prevenci závažných havárií s orientací při určení povinností a závazků vyplývajících ze zákona č. 181/2014 Sb., o kybernetické bezpečnosti.

Na základě stejnojmenného materiálu:

Kybernetická bezpečnost u objektů nakládajících s vybranými nebezpečnými chemickými látkami nebo chemickými směsmi – rešerše stavu v ČR

Dokument k projektu " SS02030008 Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)" - spolufinancovaného se státní podporou Technologické agentury ČR v rámci Programu Prostředí pro život.

Zpracovaného:

Zhotovitel: Vysoká škola báňská – Technická univerzita Ostrava, 17. listopadu 2172/15, 70800 Ostrava – Poruba, IČO: 61989100

Vypracovali: Ing. Filip Řezáč, Ph.D., prof. Ing. Miroslav Vozňák, Ph.D.

Kontakt: filip.rezac@vsb.cz

Pro potřeby OEREŠ MŽP upravila:

Ing. Zuzana Machátová