SS02030008

CENTRUM ENVIRONMENTÁLNÍHO VÝZKUMU ODPADOVÉ A OBĚHOVÉ HOSPODÁŘSTVÍ A ENVIRONMENTÁLNÍ BEZPEČNOST

Odborná zpráva o řešení projektu 2021 – 2022
Výstup 3.A.1.6 Kybernetická bezpečnost

Reportovací období: 01.01. – 31.12.2022
Kontaktní osoba: prof. Dr. Ing. Aleš Bernatík, ales.bernatik@vsb.cz, +420 597 322 833
Vypracovali: Ing. Filip Řezáč, Ph.D., prof. Ing. Miroslav Vozňák, Ph.D.
Datum vypracování: 5. 1. 2023

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

Obsah

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

WP 3.A Hodnocení rizik závažných havárií 2021-2022

KYBERNETICKÁ BEZPEČNOST A PREVENCE ZÁVAŽNÝCH HAVÁRIÍ U OBJEKTŮ NAKLÁDAJÍCÍCH S VYBRANÝMI NEBEZPEČNÝMI CHEMICKÝMI LÁTKAMI

Cíl WP 3.A.6: dílčí metodické doporučení k problematice kybernetické bezpečnosti

1. Úvod

Cílem projektu CEVOOH je vybudování dlouhodobě pracující, odborné, interdisciplinární, výzkumné základny tvořené klíčovými výzkumnými organizacemi disponujícími expertízou a odbornou kapacitou pro provádění výzkumu v oblasti odpadového a oběhového hospodářství v širších souvislostech. Centrum bude poskytovat Ministerstvu životního prostředí, dalším resortům, odborným platformám a dalším subjektům výsledky výzkumu, rozšiřování vědeckých poznatků a expertní podporu při tvorbě politik, strategií a regulací. Centrum tvořené konsorciem osmi výzkumných organizací a univerzit je zaměřeno na provádění výzkumu v tematických oblastech souvisejících s přechodem České republiky z lineárního na cirkulární hospodářský model. Tento přechod vyžaduje výzkum v nových, dosud neřešených oblastech, jakými jsou například materiálové toky surovin, inovativní technologie zaměřené na minimalizaci použití primárních surovin ve výrobě, maximální materiálovou využitelnost a využívání odpadů, vedlejších produktů a meziproduktů, ekodesign produktů, sledování a vyhodnocování nejen environmentálních, ale také sociálně–ekonomických procesů. Hlavními tematickými oblastmi, na které se Centrum v rámci své činnosti zaměří, jsou odpadové a oběhové hospodářství, monitoring a rozvoj nových monitorovacích nástrojů sledování přechodu k oběhovému hospodářství, včetně vývoje nových indikátorů, analýza životního cyklu výrobků, ekodesign, problematika kontaminace prostředí z hlediska technologií, nově se vyskytujících polutantů, využití nových metod a přístupů k identifikaci a odstranění znečištění, např. prostřednictvím dálkového průzkumu Země. Neopomenutelným tématem je také oblast environmentální bezpečnosti, prevence závažných havárií, a tím související témata kybernetické bezpečnosti a společenské přijatelnosti environmentálně a technologicky podmíněných.

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

Právě oblast prevence závažných havárií v souvislosti s tématem kybernetické bezpečnosti je zásadním bodem, na kterém se budou v období 2021-2026 podílet VŠB-TUO a CENIA. Tato část bude zaměřena na všechny technické aspekty oblasti prevence závažných havárií, a to od koncepčních a strategických dokumentů až k dílčím metodickým doporučením pro vybrané části systému prevence závažných havárií způsobených nebezpečnými chemickými látkami. Hlavním výstupem bude celková koncepce prevence závažných havárií pro ČR, která bude obsahovat i zkušenosti a politiky ze zahraničí. Koncepce bude zahrnovat všechny návaznosti kombinovaných rizik na stávající systém prevence závažných havárií, včetně souvislostí u takzvaných nezařazených podniků.

Tento dokument si klade za cíl popsat současné legislativní, procesní a technické postupy v oblasti definice a identifikace provozovatelů základních služeb nakládajících s vybranými nebezpečnými chemickými látkami nebo chemickými směsmi s ohledem na kybernetickou bezpečnost v souvislosti s prevencí závažných havárií.

Níže jsou rozebrány jednotlivé zákony, vyhlášky a EU směrnice, které jsou v platnosti nejen pro Českou republiku a regulují výše uvedenou oblast provozovatelů základních služeb a objektů s vybranými nebezpečnými chemickými látkami nebo chemickými směsmi. 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. Součástí textu je také náhled na budoucí možný vývoj v oblasti evropské legislativy z pohledu kybernetické bezpečnosti a její působnosti v jednotlivých členských zemích.

Dokument je rozdělen na kapitoly, které reflektují nejprve legislativní oblast problematiky, dále pak procesní postupy pro definici a identifikaci subjektu provozovatele a informačního systému, kdy následují technická a metodická doporučení, vycházející právě z legislativního rámce platného v ČR. Přílohy dokumentu obsahují jednak seznam objektů nakládajících s vybranými nebezpečnými chemickými látkami nebo chemickými směsmi dle zákona **č. 224/2015 Sb.**, a poté také stručný procesní postup s diagramem pro zařazení, určení, kontrolu a hlášení kybernetických incidentů v souvislosti s prevencí závažných havárií. Součástí této přílohy je i případová studie. Závěrečná příloha poté představuje metodický pokyn v podobě zásad tvorby bezpečnostní dokumentace pro informační a komunikační systémy základní služby dle platných zákonů a vyhlášek.

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

2. Legislativní část

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

Současná legislativa ČR definuje základní právní předpis upravující oblast prevence závažných havárií a to dle zákona **č. 224/2015 Sb.** [1]**,** ze dne 12. srpna 2015. Jedná se o Zákon o prevenci závažných havárií způsobených vybranými nebezpečnými chemickými látkami nebo chemickými směsmi a o změně zákona č.634/2004 Sb., o správních poplatcích ve znění pozdějších předpisů (zákon o prevenci závažných havárií).

Zákon zpracovává příslušnou Směrnici Evropského parlamentu a Rady **2012/18/EU** [2] (známou jako **SEVESO III**) a stanoví systém prevence závažných havárií pro objekty a zařízení, v nichž je umístěna vybraná nebezpečná chemická látka nebo chemická směs s cílem snížit pravděpodobnost vzniku a omezit následky případných závažných havárií na zdraví a životy lidí, hospodářská zvířata, životní prostředí a majetek. Zákon nabyl účinnosti dne 1. října 2015. Zákonem se ruší zákon č. 59/2006 Sb., o prevenci závažných havárií.

Legislativním garantem a regulátorem pro tuto oblast v rámci ČR je **Ministerstvo životního prostředí, odbor environmentálních rizik a ekologických škod,** (dále MŽP), kdy pro správné zařazení objektu podle zákona **č. 224/2015 Sb.** definovalo metodické pokyny [3, 4], které si kladou za cíl vymezit osoby a objekty, na které se zákon vztahuje a popsat principy a způsob zařazení objektu do skupiny A nebo B definovaných zákonem. Metodika pro určení těchto provozovatelů a objektů je detailně popsána v kapitole 3 tohoto dokumentu.

K provedení zákona č. 224/2015 Sb., slouží také následující právní předpisy:
Vyhlášky Ministerstva životního prostředí:

- Vyhláška **č. 227/2015 Sb.,** [5] ze dne 24. srpna 2015, o náležitostech bezpečnostní dokumentace a rozsahu informací poskytovaných zpracovateli posudku.
- Vyhláška **č. 228/2015 Sb.,** [6] ze dne 24. srpna 2015 o rozsahu zpracování informace veřejnosti, hlášení o vzniku závažné havárie a konečné zprávy o vzniku a dopadech závažné havárie.
- Vyhláška **č. 229/2015 Sb.,** [7] ze dne 24. srpna 2015, o způsobu zpracování návrhu ročního plánu kontrol a náležitostech obsahu informace o výsledku kontroly a zprávy o kontrole.

Vyhláška Ministerstva průmyslu a obchodu:

- Vyhláška **č. 225/2015 Sb.,** [8] ze dne 28. srpna 2015, o stanovení rozsahu bezpečnostních opatření fyzické ochrany objektu zařazeného do skupiny A nebo skupiny B.

Vyhláška Ministerstva vnitra:

- Vyhláška **č. 226/2015 Sb.,** [9] ze dne 12. srpna 2015, o zásadách pro vymezení zóny havarijního plánování a postupu při jejím vymezení a o náležitostech obsahu vnějšího havarijního plánu a jeho struktuře.

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

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. Mimo ČR, každý členský stát EU definuje podobně svého garanta a regulátora kybernetické bezpečnosti. Seznam garantů pro jednotlivé členské státy EU je uveden na [10].

Základním právním předpisem, upravující práva a povinnosti osob, jakož i pravomoc a působnost orgánů veřejné moci v oblasti kybernetické bezpečnosti je zákon **č. 181/2014 Sb.** [11]**,** ze dne 29. srpna 2014 (platný od 1.1. 2015). Jedná se o Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

Zákon zpracovává příslušnou Směrnici Evropského parlamentu a Rady **2016/1148/EU** [12] (The Directive on security of network and information systems, 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.** [13] s účinností od 1.7. 2017 a zákona **č. 205/2017 Sb.** [14] s účinností od 1. 8. 2017. K aktuálnímu datu proběhly ještě následující novelizace tohoto zákona – novelizace zákonem **č. 183/2017 Sb.,** [15] zákonem **č. 35/2018 Sb**. [16], zákonem **č. 111/2019 Sb.** [17] a aktuálně poslední novelizace zákonem **č. 12/2020 Sb**. [18] Aktuální znění zákona je účinné od 1. února 2020.

Kritéria pro zařazení provozovatele nebo objektu do režimu požadavků kybernetického zákona určuje zákon o kybernetické bezpečnosti, který vychází a ukotvuje níže uvedené pojmy ze směrnice NIS do české legislativy.

Směrnice NIS a aktuální novela zákona č. 181/2014 Sb. definují 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.

K výše uvedeným oblastem byla vydána Vyhláška o kybernetické bezpečnosti **č. 82/2018 Sb**. [19] 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,

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

- 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.

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

1. Nařízení vlády **č. 432/2010 Sb.** [20]**,** o kritériích pro určení prvku kritické infrastruktury. Řeší definici a identifikaci **Informačních a komunikačních systémů kritické informační infrastruktury**. Nařízení vlády je platné od 30.12. 2010. Nařízení vlády definuje průřezová a odvětvová kritéria pro určení prvku kritické infrastruktury. V příloze k nařízení vlády je definováno 9 odvětví, včetně jednotlivých odvětvových kritérií pro určení prvku kritické infrastruktury. Toto nařízení vlády 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.

2. Vyhláška **č. 317/2014 Sb.** [21], o významných informačních systémech a jejich určujících kritériích. Řeší definici a identifikaci **Významných informačních a komunikačních systémů**. Dne 19.12. 2014 vstoupila vyhláška v platnost. Vyhláška stanoví významné informační systémy a kritéria pro jejich určení. 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 rozděleno do tří období (měnit se bude znění § 2, první období nastává 1.1. 2021). Kompletní znění nabude účinnosti dne 1.1. 2023.

3. Vyhláška **č. 437/2017 Sb.** [22], o kritériích pro určení provozovatele základní služby. Řeší definici a identifikaci **Informačních a komunikačních systémů provozovatelů základních služeb.** Dne 1.2. 2018 vstoupila vyhláška v platnost. Vyhlášku zpracoval Národní úřad pro kybernetickou a informační bezpečnost ve spolupráci s odbornou veřejností. Vyhláška zapracovává požadavky Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6.6. 2016 (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 (změna se týká speciálních kritérií druhu subjektu).

4. Dne 31.1. 2018 zveřejnila Evropská komise prováděcí nařízení komise (EU) **2018/151** [23], kterým se stanoví pravidla pro uplatňování směrnice Evropského parlamentu a Rady (EU) 2016/1148 (Směrnice NIS). Toto 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. Toto prováděcí nařízení je účinné od 10.5. 2018 a je přímo aplikovatelné. Pro poskytovatele digitálních služeb je tedy závazné.

2.3.Změny v legislativní oblasti v souvislosti s přijetím směrnice NIS II

V lednu 2020 poprvé Evropská komise zveřejnila ve svém programu záměr provést revizi stávající směrnice **2016/1148/EU** [11] (The Directive on security of network and information systems, známou jako **NIS**) s cílem rapidně zvýšit ochranu a bezpečnost členských států v oblasti kyberprostoru. V dubnu 2021 došlo k prezentování záměru před Evropským parlamentem, dále proběhla v průběhu roku 2022 interinstitucionální třístranná jednání a koncem roku 2022 by měla být směrnice přijata a vydána ve finálním znění. Změny zákona a nové povinnosti pro ČR vyplývající ze směrnice by měly být platné od dubna 2024.

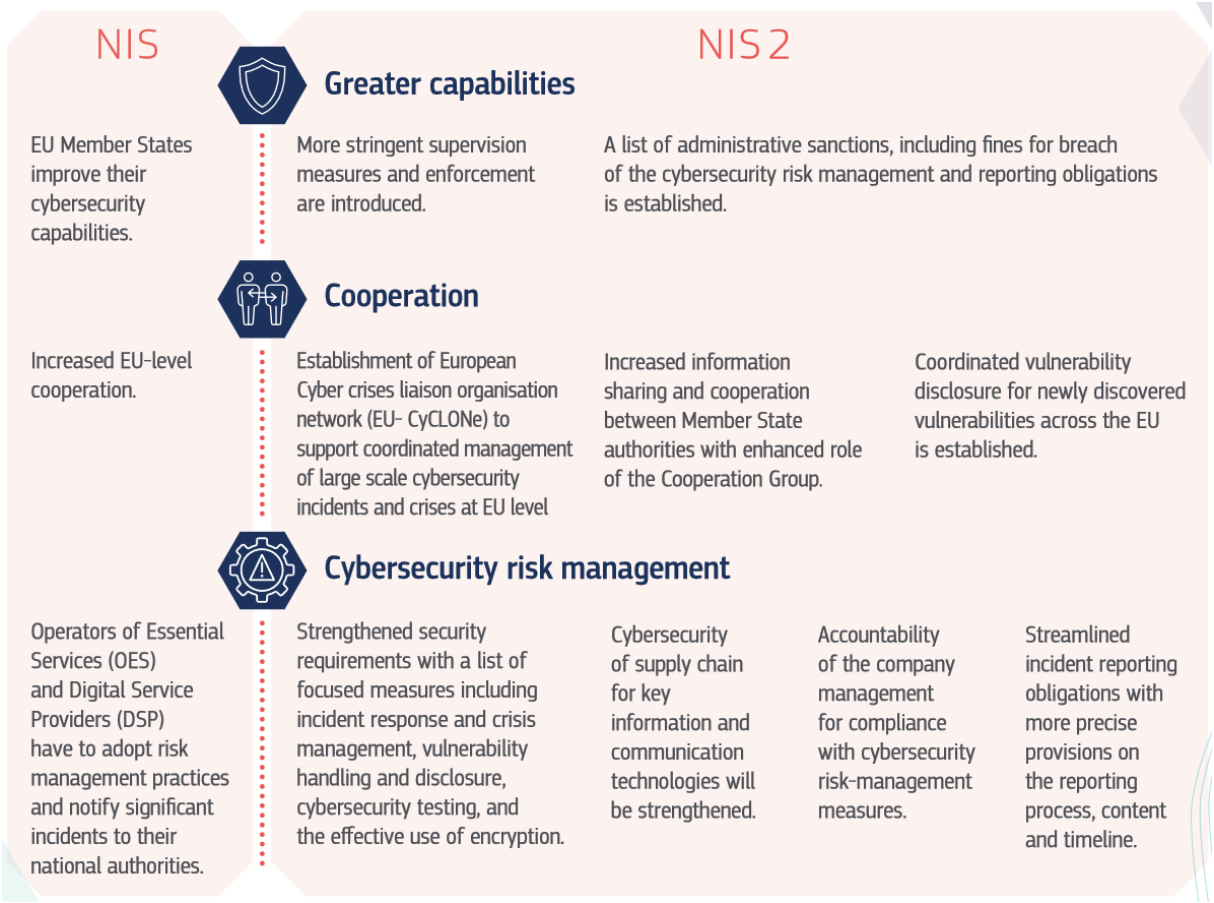
Revize stávající směrnice NIS má také vliv na soudržnost se stávajícími právními předpisy, kdy bylo nutné otevřít další tři blízké iniciativy k tomuto tématu:

- Vydání nové směrnice (The Directive on the resilience of critical entities, známé jako **CER**), která by měla řešit lepší odolnost kritických subjektů, kdy je jejich bezpečnost zahrnuta v současné směrnici NIS.
- Iniciativa týkající se zákona o digitální provozní odolnosti pro finanční sektor (**DORA**).
- Iniciativa týkající se kybernetické bezpečnosti s odvětvovými pravidly pro hraniční toky elektřiny (viz. analýza snímků v projektu **SPEAR**).

Samotná revize směrnice NIS by měla především spočívat v níže uvedených bodech, které jsou také shrnuty na obrázku 1.:

- Zvýšení úrovně kybernetické odolnosti napříč podniky v EU a to ve všech odvětvích lidské činnosti. Toho lze docílit zavedením pravidel, která budou reflektovat aktuální bezpečnostní hrozby a také rozšířením oblasti stávající působnosti směrnice do oblastí telekomunikací, platforem sociálních médií a veřejné správy. Sdružuje také postupy členských států v určitých případech - např. řešení bezpečnostních incidentů. Mizí také rozdělení ISP do několika kategorií a jsou zde také definovány pravidla pro zaručení kybernetické bezpečnosti u dodavatelů ICT.
- Snížení rozdílů mezi členskými státy a větší unifikace v procesních oblastech, jako jsou: hlášení incidentů, dohled a vymáhání při porušení bezpečnostních opatření atd. Návrh obsahuje sedm klíčových elementů, které musí všechny podniky spadající pod směrnici splňovat (odpovědnost za incident, bezpečnost dodavatelského řetězce, šifrování a odhalování zranitelností). Jsou také stanoveny přesné časové termíny pro plnění jednotlivých procesů a jsou definovány sankce v případě opakovaného porušování, či nedodržování bezpečnostních opatření.
- Zvýšení úrovně povědomí a kolektivní spolupráce na bezpečnostním incidentu. V praxi to znamená větší sdílení informací o incidentech a opatřeních mezi členskými státy, definování odpovědnostních rolí a vytvoření jasných plánů zahrnující vnitrostátní a EU orgány odpovědné za kybernetickou bezpečnost nejen na území členského státu, ale

také pro celé EU. Vznik orgánu EU-Cyber Crises Liaison Organization Network (**EU-CyCLONe)** zodpovědného za řízení a řešení incidentů celoevropského či světového rozsahu, včetně zajištění pravidelnosti výměny informací. Členské státy by nadále musely přijmout vnitrostátní strategie kybernetické bezpečnosti a určit jeden nebo více orgánů pro dohled na dodržování směrnice, určit týmy CSIRT, a zřídit kontaktní místa (**SPOC**), které budou fungovat jako styčné body pro jiné členské státy.



Obr. 1 Shrnutí plánovaných změn v rámci revize směrnice NIS (plné rozlišení: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72155).

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

3. Procesní část

3.1. Metodické pokyny a dokumenty k zařazení objektu a provozovatele

Z výše uvedeného textu plyne, že z pohledu prevence závažných havárií v souvislosti s kybernetickou bezpečností je nejdůležitější oblast **Informačních a komunikačních systémů provozovatelů základních služeb**, protože právě do této oblasti spadají i objekty nakládajících s vybranými nebezpečnými chemickými látkami nebo chemickými směsmi, na které je tato část projektu zaměřena.

Níže jsou proto zmíněny metodické pokyny, které MŽP a NÚKIB vydávají pro lepší orientaci v legislativní oblasti, a které si kladou za cíl jednak vymezit provozovatele a objekty, na které se vztahuje zákon **č. 224/2015 Sb**. a pomoci s identifikací a zařazením objektů provozovatelů informačních a komunikačních systémů základních služeb, které spadají pod regulaci zákona **č. 181/2014 Sb**.

V souvislosti s identifikací provozovatelů a objektů spadajících do regulace Zákona o prevenci závažných havárií způsobených nebezpečnými chemickými látkami a směsmi MŽP vydalo metodické pokyny:

[3] - **Posouzení objektu s vybranými nebezpečnými chemickými látkami nebo chemickými směsmi a plnění obecných povinností právnických nebo podnikajících fyzických osob, včetně způsobu zařazení objektu do skupiny A nebo B a zpracování návrhu zařazení podle zákona č. 224/2015 Sb., o prevenci závažných havárií (dále jen zákon)** a

[4] - **Metodický postup harmonizace a optimalizace bezpečnostních přístupů při skladování zemního plynu v podzemních zásobnících**,

které si kladou za cíl vymezit podniky, na které se **zákon č. 224/2015 Sb.** vztahuje a popsat principy a způsob zařazení objektu do skupiny A nebo B definovaných zákonem.

Z pohledu určení provozovatele informačního nebo komunikačního systému základní služby, je pro objekt stěžejní informace, zda spadá pod regulaci zákona **č. 181/2014 Sb.** o kybernetické bezpečnosti, či nikoliv. V tomto kroku by měly pomoci dokumenty vydané NÚKIB, a to sice:

[24] - **Minimální bezpečnostní standard** a

[25] - **Provozovatel informačního nebo komunikačního systému podle zákona o kyb. bezpečnosti**,

které shrnují nejdůležitější body týkajících se definice a identifikace institutu, jako provozovatele informačního nebo 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

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

zpracovávaných informací a informačních systémů lze poté nalézt v dokumentu [26] – **Metodika k vodítkům pro hodnocení dopadů**.

Z pohledu metodických pokynů pro provozovatele systémů základních služeb jsou stěžejní dokumenty [27] – **Informace o institutu základní služby** a [28] – **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 [29] – **Minimální požadavky na kryptografické algoritmy**. Tato oblast je detailně rozebrána v kapitole 4 tohoto dokumentu.

Text níže zahrnuje procesní část, kdy jsou rozebrány podrobně jednotlivé metodické pokyny vydané MŽP za účelem určení objektů s vybranými nebezpečnými chemickými látkami nebo chemickými směsmi a 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

Již bylo uvedeno, že příslušný zákon definuje skupiny označené A a B, do kterých je příslušný objekt zařazen, pokud nakládá s chemickými látkami a směsmi v určitém definovaném množství. Přiřazení objektu do skupiny závisí na několika dílčích faktorech, které popisuje příslušný zákon, a jsou také uvedeny v odkazovaných metodikách.

Obecně lze říci, že pokud množství umístěných nebezpečných látek nebo směsí překračuje kvalifikační množství uvedené v tabulkách v **Příloze č. 1 zákona č. 224/2015 sb.**, konkrétně **Tabulce 1 – Kategorie nebezpečných látek** a **Tabulce 2 – Jmenovitě vybrané nebezpečné látky**, je nutné objekt zařadit do skupiny A nebo B.

U objektů, ve kterých není přítomna žádná jednotlivá látka nebo směs v množství přesahujícím nebo rovnajícím se příslušným kvalifikačním množstvím, se používá vzorec v **Příloze č. 1 zákona č. 224/2015 sb. v článku 8** pro zjištění, zda se na objekt vztahují povinnosti provozovatele podle zákona.

Metodika [3] poté prezentuje v **Příloze č. 3** příklady použití tohoto sčítacího vzorce.

Pokud objekt splňuje podmínky pro zařazení do skupiny A nebo B, je provozovatel objektu povinen zpracovat a odeslat příslušnému krajskému úřadu návrh na zařazení objektu. Vzor návrhu na zařazení objektu do skupiny A nebo B je uveden v příloze **Příloze č. 2 zákona č. 224/2015 sb**. Druhem nebezpečných látek je v tomto případě myšlen chemický název.

TA ČR
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

Obsah Návrhu na zařazení stanoví **§ 5 odst. (4)** zákona. Návrh musí být podepsán buď statutárním orgánem, nebo fyzickou osobou oprávněnou jednat za provozovatele objektu.

Jakmile je objekt zařazen do skupiny, musí v něm být nastaven bezpečnostní režim, který se snaží minimalizovat riziko závažné havárie, která by mohla vzniknout právě z důvodu přítomnosti nebezpečných látek.

Výsledkem tohoto procesu je seznam objektů (Příloha A), které spadají do jedné z uvedených skupiny A nebo B a jsou povinny se řídit zákonem **č. 224/2015 sb**. a odvozenými vyhláškami viz. kapitola 2.1.

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 nakládající 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 ji 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 [25] a [26].
- Splňuje daná odvětvová a dopadová kritéria – určuje vyhláška 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

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

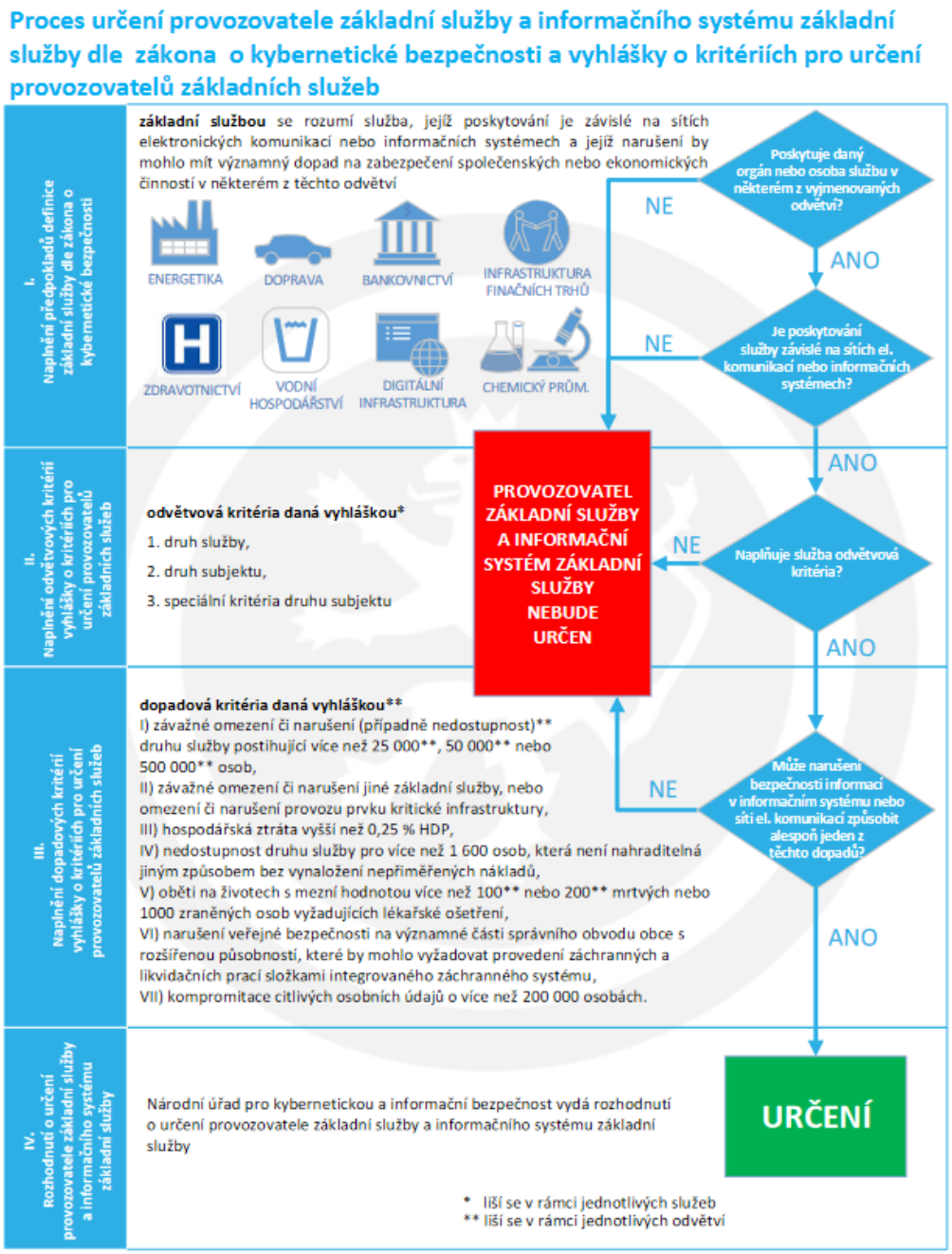
Pro objekty nakládající s vybranými nebezpečnými chemickými látkami nebo chemickými směsmi jsou konkrétní kritéria uvedena v **Příloze vyhlášky č. 437/2017, článku 8.**

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 viz. obr. 2.:

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.



Obr. 2 Proces určení provozovatele základní služby a inf. systému základní služby (plné rozlišení: https://www.nukib.cz/download/publikace/podpurne_materialy/Schema_rozhodovani_PZS_v2.1.pdf).

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

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 [30], 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.

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

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 nakládajících 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 [24] – **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. Provozovatelé systémů základních služeb tak mohou využít uvedený dokument převážně jako přehled minimálních technických a organizačních bezpečnostních opatření, které by měli splňovat.

Doporučení pro uvedenou problematiku, uvedena v tomto dokumentu, jsou rozdělena na část manažerskou a technickou:

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 Plan – 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.

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

- 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 poskytovateli 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 [24], jelikož jednotlivé paragrafy a články této části odpovídají dílčím odstavcům dokumentu a uvedená doporučení jsou v případě této části vyhlášky a dokumentu [24] ve shodě.

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

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

Posledním dokumentem, který definuje konkrétní technická doporučení v oblasti kybernetické bezpečnosti informačních a komunikačních systémů je již zmiňovaný dokument [29] - **Minimální požadavky na kryptografické algoritmy – doporučení v oblasti kryptografických prostředků**. V tomto materiálu je možné nalézt doporučené 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 hašovacích funkcí.

Na tuto kapitolu navazuje také Příloha C, která definuje metodické pokyny pro zpracování bezpečnostní dokumentace informačního a komunikačního systému základní služby tak, aby splňovala požadavky specifikované zákonem **č. 181/2014 Sb.** a vyhláškou **č. 82/2018 Sb.**

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

5. Závěr

Výše uvedený dokument reflektuje aktuální legislativní stav (k 3.11. 2022), a stav procesní a technické podpory v rámci ČR pro oblast prevence závažných havárií z pohledu kybernetické bezpečnosti u objektů nakládajících s vybranými nebezpečnými chemickými látkami nebo chemickými směsmi, které jsou zároveň také provozovateli systémů základních služeb.

Byl prezentován legislativní základ v podobě zákonů a vyhlášek, které definují, jaké podmínky a pravidla musí splňovat objekt v odvětví s vybranými nebezpečnými chemickými látkami nebo chemickými směsmi z pohledu prevence závažných havárií a následně byl také zmíněn legislativní rámec pro určení, zda taková instituce provozuje informační a komunikační systém a tím pádem se stává provozovatelem systému základní služby.

Z tohoto titulu je objekt nebo provozovatel povinen realizovat procesní postupy, které jednak jednoznačně určují, které systémy a části objektu spadají pod regulaci, a které nikoliv, a dále také dávají představiteli objektu 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 instituce zařazená dle výše uvedených legislativních a procesních postupů, měla splňovat.

Tento dokument by měl sloužit jako základní dokument k orientaci v problematice kybernetické bezpečnosti pro uvedenou problematiku, a zároveň by měl pomoci s orientací provozovatelům z daného oboru při určení povinností a závazků vůči orgánům veřejné moci.

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

Literatura

[1] Zákon č. 224/2015 Sb. Zákon o prevenci závažných havárií způsobených vybranými nebezpečnými chemickými látkami nebo chemickými směsmi a o změně zákona č. 634/2004 Sb., o správních poplatcích, ve znění pozdějších předpisů, (zákon o prevenci závažných havárií). Dostupný online: https://www.zakonyprolidi.cz/cs/2015-224 .

[2] Směrnice Evropského parlamentu a Rady 2012/18/EU ze dne 4. července 2012 o kontrole nebezpečí závažných havárií s přítomností nebezpečných látek a o změně a následném zrušení směrnice Rady 96/82/ES Text s významem pro EHP. Dostupná online: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32012L0018&from=HU .

[3] Metodický pokyn - pro zařazení objektu podle zákona č. 224/2015 Sb. Posouzení objektu s vybranými nebezpečnými chemickými látkami nebo chemickými směsmi a plnění obecných povinností právnických nebo podnikajících fyzických osob, včetně způsobu zařazení objektu do skupiny A nebo B a zpracování návrhu zařazení podle zákona č. 224/2015 Sb., o prevenci závažných havárií (dále jen zákon). Dostupný online: https://www.mzp.cz/C1257458002F0DC7/cz/metodicke_pokyny_odboru_enviro_rizik/$FILE/OERES-met_pokyn_zarazeni-20160510.pdf .

[4] Certifikovaná metodika - Metodický postup harmonizace a optimalizace bezpečnostních přístupů při skladování zemního plynu v podzemních zásobnících: postup při zpracování a struktura vnitřního havarijního plánu pro provozy podzemních zásobníků plynu. Dostupná online: https://www.mzp.cz/C1257458002F0DC7/cz/metodicke_pokyny_odboru_enviro_rizik/$FILE/oeres-met_pzp-20160310.pdf .

[5] Vyhláška č. 227/2015 Sb. Vyhláška o náležitostech bezpečnostní dokumentace a rozsahu informací poskytovaných zpracovateli posudku. Dostupná online: https://www.zakonyprolidi.cz/cs/2015-227 .

[6] Vyhláška č. 228/2015 Sb. Vyhláška o rozsahu zpracování informace veřejnosti, hlášení o vzniku závažné havárie a konečné zprávy o vzniku a dopadech závažné havárie. Dostupná online: https://www.zakonyprolidi.cz/cs/2015-228 .

[7] Vyhláška č. 229/2015 Sb. Vyhláška o způsobu zpracování návrhu ročního plánu kontrol a náležitostech obsahu informace o výsledku kontroly a zprávy o kontrole. Dostupná online: https://www.zakonyprolidi.cz/cs/2015-229 .

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

[8] Vyhláška č. 225/2015 Sb. Vyhláška o stanovení rozsahu bezpečnostních opatření fyzické ochrany objektu zařazeného do skupiny A nebo skupiny B. Dostupná online: https://www.zakonyprolidi.cz/cs/2015-225 .

[9] Vyhláška č. 226/2015 Sb. Vyhláška o zásadách pro vymezení zóny havarijního plánování a postupu při jejím vymezení a o náležitostech obsahu vnějšího havarijního plánu a jeho struktuře. Dostupná online: https://www.zakonyprolidi.cz/cs/2015-226 .

[10] State-of-play of the transposition of the NIS Directive. Dostupný online: https://digital-strategy.ec.europa.eu/en/policies/nis-transposition .

[11] Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Dostupný online: https://www.zakonyprolidi.cz/cs/2014-181 .

[12] European Union Agency for Cybersecurity, NIS Directive Tool. Dostupný online: https://www.enisa.europa.eu/topics/nis-directive/nis-visualtool .

[13] Zákon č. 104/2017 Sb. Zákon, kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějšíchpředpisů, zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a některé další zákony. Dostupný online: https://www.zakonyprolidi.cz/cs/2017-104 .

[14] Zákon č. 205/2017 Sb. Zákon, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony. Dostupný online: https://www.zakonyprolidi.cz/cs/2017-205 .

[15] Zákon č. 183/2017 Sb. Zákon, kterým se mění některé zákony v souvislosti s přijetím zákona o odpovědnosti za přestupky a řízení o nich a zákona o některých přestupcích. Dostupný online: https://www.zakonyprolidi.cz/cs/2017-183 .

[16] Zákon č. 35/2018 Sb. Zákon o změně některých zákonů upravujících počet členů zvláštních kontrolních orgánů Poslanecké sněmovny. Dostupný online: https://www.zakonyprolidi.cz/cs/2018-35 .

[17] Zákon č. 111/2019 Sb. Zákon, kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů. Dostupný online: https://www.zakonyprolidi.cz/cs/2019-111 .

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

[18] Zákon č. 12/2020 Sb. Zákon o právu na digitální služby a o změně některých zákonů. Dostupný online: https://www.zakonyprolidi.cz/cs/2020-12 .

[19] Vyhláška č. 82/2018 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). Dostupná online: https://www.zakonyprolidi.cz/cs/2018-82 .

[20] Nařízení vlády č. 432/2010 Sb. Nařízení vlády o kritériích pro určení prvku kritické infrastruktury. Dostupné online: https://www.zakonyprolidi.cz/cs/2010-432 .

[21] Vyhláška č. 317/2014 Sb. Vyhláška o významných informačních systémech a jejich určujících kritériích. Dostupná online: https://www.zakonyprolidi.cz/cs/2014-317 .

[22] Vyhláška č. 437/2017 Sb. Vyhláška o kritériích pro určení provozovatele základní služby. Dostupná online: https://www.zakonyprolidi.cz/cs/2017-437 .

[23] Prováděcí nařízení Komise (EU) 2018/151 ze dne 30. ledna 2018, kterým se stanoví pravidla pro uplatňování směrnice Evropského parlamentu a Rady (EU) 2016/1148, pokud jde o bližší upřesnění prvků, které musí poskytovatelé digitálních služeb zohledňovat při řízení bezpečnostních rizik, jimiž jsou vystaveny sítě a informační systémy, a parametrů pro posuzování toho, zda je dopad incidentu významný. Dostupný online: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32018R0151&from=ES .

[24] Minimální bezpečnostní standard – podpůrný materiál pro subjekty, které nespadají pod zákon o kybernetické bezpečnosti. Dostupný online: https://www.nukib.cz/download/publikace/podpurne_materialy/2020-07-17_Minimalni-bezpecnostni-standard_v1.0.pdf .

[25] Provozovatel informačního nebo komunikačního systému podle § 2 písm. G) zákona o kybernetické bezpečnosti. Dostupný online: https://www.nukib.cz/download/publikace/podpurne_materialy/Provozovatel-informacniho-nebo-komunikacniho-systemu_v3.1.pdf .

[26] Metodika k vodítkům pro hodnocení dopadů. Dostupná online: https://www.nukib.cz/download/publikace/podpurne_materialy/Metodika_k_voditkum_pro_hodnoceni_dopadu_NUKIB_v.1.2_s_prilohou.pdf .

[27] Informace o institutu základní služby – Shrnutí způsobu určení provozovatele základní služby a informačního systému základního služby. Dostupné online: https://nukib.cz/download/publikace/podpurne_materialy/Informace-o-institutu-zakladni-sluzby_v1.4.pdf .

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

[28] Průvodce určováním provozovatele základní služby, verze 5.5, platná ke dni 30.3. 2021, NÚKIB, Oddělení regulace veřejného sektoru.

[29] Minimální požadavky na kryptografické algoritmy – doporučení v oblasti kryptografických prostředků. Dostupné online: https://www.nukib.cz/download/publikace/doporuceni/Doporuceni_krypto_prostredky_1.0.pdf .

[30] Dotazník pro určování provozovatele základní služby a informačního systému základní služby – Odvětví chemický průmysl. Verze 1.1., platná ke dni 8.11.2019, NÚKIB, Oddělení regulace veřejného sektoru.

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

Příloha A – Seznam objektů nakládajících s vybranými nebezpečnými chemickými látkami nebo chemickými směsmi dle zákona č. 224/2015 Sb. (k 25.6.2021)

Název	Skupina	Od	IČO provozovatele	Adresa	PSČ	Místo	Kraj
ACO Industries	A	02.05.2016	48119458	Havlíčkova 260	58222	Přibyslav	Vysočina
ADW AGRO, Kojetice na Moravě	B	31.05.2005	49969846	Kojetice na Moravě 154	67523	Kojetice na Moravě	Vysočina
AERO Vodochody Aerospace, Odolena Voda	A	06.10.2006	24194204	U Letiště 374	25070	Odolena Voda	Středočeský
AGC Flat Glass Czech, závod Barevka	A	02.01.2009	14864576	Mírová 144	417 03	Dubí	Ústecký
Agrofert, Brno	A	01.01.2005	26185610	Obilní 35	64300	Brno-Chrlice	Jihomoravský
AgroZZN, - Rakovník	A	15.08.2011	45148082	V Lubnici 2333	26926	Rakovník	Středočeský
Air Products - Brno	A	01.01.2000	41324226	Tuřanka 94	62700	Brno	Jihomoravský

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

Air Products - Děčín	A	01.01.2000	41324226	Ústecká 30	40530	Děčín	Ústecký
Air Products - Litvínov	B	01.01.2000	41324226	Záluží 1	43670	Litvínov	Ústecký
Air Products - Teplice, Teplice	A	01.01.2000	41324226	areál AGC Flat Glass	415 01	Teplice	Ústecký
ASK Chemicals Czech	A	09.02.2011	25773025	Tovární 7	643 00	Brno-Chrlice	Jihomoravský
Austin Detonator Jasenice, Vsetín	B	23.08.2006	25689916	Jasenice 712	75501	Vsetín	Zlínský
Austin Detonator Manerov	B	27.09.2012	25689916	skladový areál Manerov	683 41	Bohdalice-Pavlovice	Jihomoravský
Austin Powder Service CZ Hněvkovice, sklad Hněvkovice	B	06.03.2007	26245736	Areál skladu výbušnin	58294	Hněvkovice u Ledče nad Sázavou	Vysočina
Austin Powder Service CZ Manerov, Manerov	B	23.05.2007	26245736	skladový areál Manerov	68441	Bohdalice-Pavlovice	Jihomoravský
Austin Powder Service CZ, sklad Psáry, sklad Psáry	B	20.03.2017	26245736	Psáry 1	252 41	Psáry	Středočeský
AVE Kralupy	A	16.11.2010	27935574	O.Wichterleho 810	278 01	Kralupy nad Vltavou	Středočeský

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

BOCHEMIE	B	01.01.2000	29396824	Lidická 326	73595	Bohumín	Moravskoslezský
BorsodChem MCHZ	B	01.01.2000	26019388	Chemická 1/2039	70903	Ostrava-Mariánské Hory	Moravskoslezský
BOSCH Diesel	A	03.12.2014	46995129	Pávov 121	586 06	Jihlava	Vysočina
BRENNTAG CR	A	01.01.2000	49613464	Mezi Úvozy 1850	19300	Praha 9	Praha
Butadien Kralupy	B	19.08.2011	25053272	O.Wichterleho 810	27801	Kralupy nad Vltavou	Středočeský
Central Glass Czech, CGCZ Projekt - 1 + CGCZ Projekt - 2	B	30.04.2019	05883601	Rybitví	533 54	Rybitví	Pardubický
COLORLAK	A	20.09.2006	49444964	Tovární 1076	68602	Staré Město	Zlínský
Continental Barum/Continental Barum	B	07.08.2006	45788235	Objízdná 1628	76531	Otrokovice	Zlínský
Cray Valley Czech - Kralupy nad Vltavou	B	01.01.2012	27254984	O.Wichterleho 810	27852	Kralupy nad Vltavou	Středočeský
Crystal BOHEMIA	B	18.08.2009	28486722	Jiráskova 223	29034	Poděbrady	Středočeský

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

CS CABOT - Valašské Meziříčí	B	01.01.2000	14612411	Masarykova 753	75701	Krásno nad Bečvou, Valašské Meziříčí	Zlínský
Czech Aerosol	B	01.01.2011	49901869	Velvěty 33	41762	Rtyně nad Bílinou	Ústecký
Czech Airlines Technics	A	01.10.2011	27145573	Letiště Ruzyně	160 08	Praha 6	Praha
ČEPRO - Bělčice	B	19.09.2006	60193531		38743	Bělčice	Jihočeský
ČEPRO - Hájek	B	11.08.2006	60193531		36301	Hájek	Karlovarský
ČEPRO - Cerekvice nad Bystřicí	B	01.01.2000	60193531	Čepro 1	50777	Cerekvice nad Bystřicí	Královéhradecký
ČEPRO - Hněvice, Hněvice	B	02.11.2006	60193531	Hněvice 62	41108	Štětí	Ústecký
ČEPRO - Klobouky u Brna	B	01.01.2000	60193531		69172	Klobouky u Brna	Jihomoravský
ČEPRO - Loukov	B	01.01.2000	60193531	Loukov 166	76875	Loukov	Zlínský
ČEPRO - Mstětice	B	01.01.2000	60193531		25091	Mstětice	Středočeský

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

ČEPRO - Nové Město	B	01.01.2000	60193531		28002	Nové Město	Středočeský
ČEPRO - Potěhy, Potěhy	B	03.01.2008	60193531		28563	Potěhy	Středočeský
ČEPRO - Sedlnice	B	06.09.2006	60193531		74256	Sedlnice	Moravskoslezský
ČEPRO - Smyslov	B	26.07.2000	60193531		39156	Smyslov	Jihočeský
ČEPRO - Střelice	B	01.01.2000	60193531		66447	Střelice	Jihomoravský
ČEPRO - Šlapanov	B	01.01.2000	60193531		58251	Šlapanov	Vysočina
ČEPRO - Třemošná	B	01.01.2000	60193531		33011	Třemošná	Plzeňský
ČEPRO - Včelná	B	01.01.2000	60193531		37382	Včelná	Jihočeský
D - Technik	A	14.01.2009	25689916	Jablůnka 610	756 23	Jablůnka	Zlínský
DANSGAS	A	05.05.2021	27332128	Nádražní 188	47107	Žandov	Liberecký

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

DEZA - Organik Otrokovice, Organik Otrokovice	A	18.09.2006	00011835	Tř. T. Bati 1764	76502	Otrokovice	Zlínský
DEZA - Valašské Meziříčí	B	01.01.2000	00011835	Masarykova 753	75728	Valašské Meziříčí	Zlínský
DHL Supply Chain	A	10.05.2014	49240650	Průmyslová 1506	691 23	Pohořelice	Jihomoravský
DIAMO - Stráž pod Ralskem, Těžba a úprava uranu	B	29.10.2004	00002739	Máchova 201	47127	Stráž pod Ralskem	Liberecký
DONAUCHEM, Nymburk	B	01.01.2000	43774750	Za Žoskou 377	28802	Nymburk	Středočeský
Dormer Pramet, Šumperk	A	23.12.2006	25782983	Uničovská 2	78753	Šumperk	Olomoucký
DUKOL Ostrava	B	01.01.2000	26792893	Chemická	70903	Ostrava - Mariánské hory	Moravskoslezský
DUO CZ, Opočno	A	16.08.2007	25945114	Na Olivě 467	51773	Opočno	Královéhradecký
Elektrárna Kladno, Elektrárna Kladno	A	26.11.2014	26735865	Dubská 257	272 03	Kladno	Středočeský
Enaspol	A	01.01.2000	25006339	Velvěty 79	41501	Teplice	Ústecký

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

ENERGETIKA TŘINEC	B	01.01.2000	47675896	Průmyslová 1024	73965	Třinec	Moravskoslezský
EPISPOL	B	30.03.2016	25449842	Revoluční 86		Ústí nad Labem	Ústecký
Eurosupport Manufactoring Czechia, výroba katalyzátorů	A	20.03.2007	25417681	areál Chemopetrolu, Záluží 1	43670	Litvínov	Ústecký
EXCALIBUR ARMY - Drhovice	B	16.08.2005	64573877	Drhovice ne	39131	Dražice	Jihočeský
Explosia	B	01.01.2000	25291581	Semtín 107	53002	Pardubice	Pardubický
Explosia - Krmelín	B	01.01.2000	25291581	U Paleska 536	73924	Krmelín	Moravskoslezský
Explosia - Lužná u Rakovníka	B	01.01.2000	25291581		27051	Lužná u Rakovníka	Středočeský
FARMAK - Olomouc	A	01.01.2000	45192961	Na Vlčinci 16/3	77117	Olomouc	Olomoucký
Fehrer Bohemia	A	03.05.2021	45280479	Litoměřická 86	47001	Česká Lípa	Liberecký
FERTISTAV CZ	A	22.04.2015	25295268	T.G. Masaryka 971	289 03	Městec Králové	Středočeský

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

FK systém – povrchové úpravy, mořící kapacity ocelí,	A	22.05.2020	27736717	Karásek, areál PharmaPark 2244/1c	621 00	Brno-Řečkovice	Jihomoravský
Flaga Satalice, Plnírna PB - Praha Satalice	B	01.09.2004	47917091	Budovatelská 155/11	19015	Praha 9	Praha
Flaga, Hustopeče , Hustopeče	B	01.09.2004	47917091	Nádražní 47	693 82	Hustopeče u Brna	Jihomoravský
Flexfill, Výrobní závod Flexill Plant	A	02.01.2009	27249026	Kostelní 5	41030	Lovosice	Ústecký
Fosfa	B	01.01.2000	00152901	Hraniční 268	69141	Břeclav-Poštorná	Jihomoravský
GHC Invest, Neratovice	A	28.06.2010	60464496	areál Lach-Ner,Tovární 157	27711	Neratovice	Středočeský
Glazura	A	02.11.2006	62243462		41301	Roudnice nad Labem	Ústecký
Global Tungsten & Powders	A	15.08.2020	27808408	Zahradní 1442/46	792 01	Bruntál	Moravskoslezský
Groz-Beckert Czech	A	25.07.2006	25179811	Nádražní 607	76601	Valašské Klobouky	Zlínský

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

Huttenes-Albertus CZ	B	01.02.2011	25572806	Tovární 63	407 11	Děčín 32-Boletice nad Labem	Ústecký
Chemoprojekt, Výrobní jednotka FAME, Výrobní jednotka FAME	A	20.07.2018	45273383	Žukovova 100	400 03	Ústí nad Labem	Ústecký
CHEMOTEX Děčín	A	27.12.2019	62240471	Tovární 63	40711	Děčín XXXII - Boletice nad Labem	Ústecký
CHEPORT, CHEPORT	B	12.06.2019	13695797	Lhotsko 93	76312	Lhotsko	Zlínský
CHS Epi	B	22.09.2016	28207882	Revoluční 86	40032	Ústí nad Labem	Ústecký
Impregnace Soběslav	A	01.01.2013	25188119	Na pískách 420/II	392 13	Soběslav	Jihočeský
Ing. Josef Kořínek	B	21.12.2005	17045941	Zámeček 600	56125	Rudoltice	Pardubický
Ing. Petr Švec - PENTA	A	01.01.2000	02096013	areál AGROP	53701	Chrudim	Pardubický
JARO	B	02.04.2015	25066137	Československé armády k.ú. Zaječice	538 51	Chrast u Chrudimi	Pardubický

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

JIPOCAR Logistic Střítež, Logistický areál Střítež	B	01.08.2006	26959224	Střítež 3	58811	Střítež u Jihlavy	Vysočina
KAYAKU SYSTEMS SAFETY EUROPE	B	17.08.2010	25114638	Průmyslová zóna Jablůnka	756 23	Jablůnka	Zlínský
Kingspan	A	15.10.2007	64829201	Vážní 465	500 03	Hradec Králové	Královéhradecký
Kongresové centrum ILS, Veřejný přístav Vaňov,	A	03.11.2016	63999871	Vaňov	40002	Ústí nad Labem	Ústecký
Kovohutě Příbram nástupnická	B	24.10.2016	27118100	Příbram 530	26181	Příbram IV	Středočeský
KRALUPOL	B	20.08.2012	49679597	V Pískovně	27801	Kralupy nad Vltavou	Středočeský
Kralupol Hněvice, Hněvice	B	20.08.2012	49679597		41 108	Hněvice	Ústecký
KRALUPOL Horka na Moravě, Horka	B	20.08.2012	49679597	Olomoucká 34	783 35	Horka nad Moravou	Olomoucký
Lach-Ner, Neratovice	A	21.11.2006	26295474	Tovární 157	27711	Neratovice	Středočeský

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

Lenzing BIOCEL Paskov	B	23.05.2018	26420317	Místecká 762	73921	Paskov	Moravskoslezský
Leštírna skla Světlá n Sázavou	A	13.08.2010	27545172	Zámecká 550	582 91	Světlá nad Sázavou	Vysočina
Letiště Václava Havla Praha	A	01.02.2008	28244532	K letišti 6/1019	16008	Praha 6	Praha
Liberty Ostrava	B	01.05.2007	45193258	Vratimovská 689	707 02	Ostrava-Kunčice	Moravskoslezský
Linde Gas - Brno	B	13.02.2006	00011754	Černovické náb. 10	61700	Brno	Jihomoravský
Linde Gas - Kralupy nad Vltavou	B	13.02.2006	00011754	areál Kaučuku	27852	Kralupy nad Vltavou	Středočeský
Linde Gas - Ostrava	A	13.02.2006	00011754	Frýdecká 691	71903	Ostrava	Moravskoslezský
Linde Gas - Praha 9	B	13.02.2006	00011754	U Technoplynu 1324	19800	Praha 9	Praha
Linde Gas - Třinec	B	13.02.2006	00011754	Průmyslová 1000	73930	Třinec	Moravskoslezský
LINDE SOKOLOVSKÁ - Vřesová	B	01.01.2007	00011754	tlak.plynárna Sokolovské uhelné	35735	Vřesová	Karlovarský

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

Lovochemie	B	01.01.2000	49100262	Terezínská 57	41017	Lovosice	Ústecký
Lučební závody Draslovka - Kolín	B	01.01.2000	46357351	Havlíčkova 605	28002	Kolín	Středočeský
Lučební závody Kolín	A	20.02.2018	46357360	Pražská 54	280 02	Kolín	Středočeský
MAIER CZ	A	01.01.2015	27254500	Průmyslová 4259/14	796 01	Prostějov	Olomoucký
MERO ČR - Klobouky u Brna	B	01.01.2000	60193468		69172	Klobouky u Brna	Jihomoravský
MERO ČR - Litvínov	A	01.01.2000	60193468		43671	Litvínov	Ústecký
MERO ČR - Nelahozeves	B	01.01.2000	60193468		27751	Nelahozeves	Středočeský
MERO ČR - Nové Město	B	01.01.2000	60193468		28002	Nové Město	Středočeský
Messer Technogas	A	01.09.2009	40764788	Chemická (areál BorsodChem) 1	709 03	Ostrava	Moravskoslezský
Messer Technogas Kladno, Kladno	A	01.09.2009	40764788	areál Poldi Dříň 666	272 03	Kladno 3 - Dubí	Středočeský

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

MG Odra Gas - Acetylenka	A	01.01.2000	46577220	areál Ispat Nová Huť	70702	Ostrava	Moravskoslezský
MG Odra Gas - Vratimov	A	01.01.2000	46577220	Na Popinci 1088	73932	Vratimov	Moravskoslezský
MND Gas Storage, PZP Uhřice, PZP Uhřice	B	26.09.2016	27732894	Uhřice 1	696 34	Uhřice	Jihomoravský
MOLITAN	B	17.09.2008	27631273	Mládežnická 3062/3A	69002	Břeclav	Jihomoravský
Mölnlycke Health Care ProcedurePak	A	24.05.2018	02948231	Šachetní 439/1	73300	Havířov	Moravskoslezský
Mondi Štětí	B	01.01.2000	26161516	Litoměřická 272	41108	Štětí	Ústecký
Monroe Czechia	A	22.12.2005	61061620	Rychnovská 383	46342	Hodkovice nad Mohelkou	Liberecký
Moravia Gas Storage, PZP Dambořice, PZP Dambořice	B	22.09.2016	28506065	Dambořice	69635	Dambořice	Jihomoravský
MOTIP DUPLI, Troubsko	A	14.11.2006	60740591	Popůvky 196	66441	Troubsko	Jihomoravský
MULTIAGRO, Slatina	A	12.12.2016	15030342	Slatina 116	56601	Vysoké Mýto	Pardubický

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

NCH Distribution, Lovosice	A	29.05.2008	28374151	Průmyslová 1190	410 02	Lovosice	Ústecký
OKK Koksovny	B	01.01.2000	47675829	Koksární ulice 1112	70224	Ostrava	Moravskoslezský
ON Semiconductor Czech Republic	A	01.01.2000	45193533	1.máje 2230	75661	Rožnov pod Radhoštěm	Zlínský
OPTIMA GAZ, sklad LPG	B	08.02.2007	25776965	sklad LPG	25763	Trhový Štěpánov	Středočeský
OQEMA Slatiňany	B	03.01.2005	63988186	Vítězství 251	53821	Slatiňany	Pardubický
OQEMA Sokolov EURO - Šarm , Sokolov	A	16.05.2014	63988186	Tovární 2093	739 34	Sokolov	Karlovarský
ORLEN UNIPETROL RPA, Litvínov	B	01.01.2000	27597075	Záluží 1	43670	Litvínov	Ústecký
ORLEN UNIPETROL RPA, Rafinérie Kralupy, Rafinérie Kralupy	B	01.01.2017	27597075	O.Wichterleho 809	278 52	Kralupy nad Vltavou	Středočeský
ORLEN UNIPETROL-DOPRAVA - Kralupy nad Vltavou	B	01.01.2000	64049701	O. Wichterleho 810	27852	Kralupy nad Vltavou	Středočeský

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

ORLEN UNIPETROL-DOPRAVA - Litvínov	B	01.01.2000	64049701	Růžodol 4	43670	Litvínov	Ústecký
ORLEN UNIPETROL-DOPRAVA - Neratovice	B	01.01.2000	64049701	areál Spolana	27711	Neratovice	Středočeský
ORLEN UNIPETROL-DOPRAVA - Paramo, Paramo	B	26.11.2004	64049701	areál Paramo	53006	Pardubice	Pardubický
ORLEN UNIPETROL-DOPRAVA - Synthesia, Synthesia	B	01.01.2000	64049701	Synthesia	53006	Pardubice	Pardubický
PARAMO	B	01.01.2000	48173355	Přerovská 560	53006	Pardubice	Pardubický
PetroMax Terminal, Sklad minerálních olejů Chlumec nad Cidlinou	A	31.05.2018	05282641	Chlumec nad Cidlinou 1	503 51	Chlumec nad Cidlinou	Královéhradecký
Plnírna technických plynů Čáslav, Čáslav	A	20.01.2010	40764788	Táborská 1542	286 01	Čáslav	Středočeský
Plzeňský Prazdroj	A	01.01.2000	45357366	U Prazdroje 7	30497	Plzeň	Plzeňský

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

Pragochema	A	01.01.2000	49686089	Přátelství 550	10400	Praha 10	Praha
PREOL, Výroba FAME	A	16.03.2009	26311208	Terezínská 47	410 17	Lovosice	Ústecký
PRIMAGAS - Havlíčkův Brod	B	20.09.2007	47118008	Mírovka 125	58001	Havlíčkův Brod	Vysočina
PRIMAGAS - Horní Suchá	B	01.01.2000	47118008	Dělnická	73535	Horní Suchá	Moravskoslezský
Procter & Gamble - Rakona	B	01.01.2000	14801396	Ottova 402	26932	Rakovník	Středočeský
PROFER PLUS	B	01.12.2008	25942468	Panelová	500 03	Hradec Králové	Královéhradecký
proseat Mladá Boleslav	A	25.11.2004	25064053	V.Klementa 869/11	29301	Mladá Boleslav	Středočeský
RECTICEL Interiors CZ	A	19.09.2005	26482193	Plazy 115	29301	Mladá Boleslav	Středočeský
RWE Gas Storage, PZP Dolni Dunajovice, PZP Dolni Dunajovice	B	20.10.2016	27892077	Dolní Dunajovice	69185	Dolní Dunajovice	Jihomoravský
RWE Gas Storage, PZP Háje, PZP Háje	B	20.10.2016	27892077	Jesenice 21	26101	Příbram	Středočeský

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

RWE Gas Storage, PZP Lobodice, PZP Lobodice	B	20.10.2016	27892077	Lobodice	75101	Tovačov	Olomoucký
RWE Gas Storage, PZP Štramberk, PZP Štramberk	B	19.10.2016	27892077	Štramberk,	74266	Štramberk,	Moravskoslezský
RWE Gas Storage, PZP Třanovice, PZP Třanovice	B	10.10.2016	27892077	Třanovice	73993	Třanovice	Moravskoslezský
RWE Gas Storage, PZP Tvrdonice, PZP Tvrdonice	B	20.10.2016	27892077	Tvrdonice	69153	Tvrdonice	Jihomoravský
SAINT-GOBAIN ADFORS CZ, skladovací a výrobní kapacity,	A	15.10.2019	00012661	Zahradní 256 256	671 25	Hodonice	Jihomoravský
Sellier & Bellot, výroba	A	01.01.2000	28982347	Lidická 667	25801	Vlašim	Středočeský
SCHÄFER - SUDEX	A	01.01.2000	60912278	Podolí 5	584 01	Ledeč nad Sázavou	Vysočina
SIAD CZECH - Braňany u Mostu	A	01.01.2000	48117153	Braňany u Mostu 193	43522	Braňany u Mostu	Ústecký
SIAD CZECH - Rajhradice	A	01.01.2000	48117153		66461	Rajhradice	Jihomoravský

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

Slovácké strojírny	A	04.01.2010	00008702	Komenského 193	789 69	Postřelmov	Olomoucký
Sokolovská uhelná	A	01.01.2000	26348349	Staré náměstí 69	35600	Sokolov	Karlovarský
SOUFFLET AGRO, Sklad agrochemikálií	B	21.12.2018	47115459	Zlechovská 1699	686 03	Staré Město	Zlínský
SPOLANA - Neratovice	B	01.01.2000	45147787	Ke Spolaně	27711	Neratovice	Středočeský
Spolek pro chemickou a hutní výrobu	B	01.01.2000	29200181	Revoluční 1930/86	40032	Ústí nad Labem	Ústecký
SPOLGAS, daňový sklad, daňový sklad	B	24.03.2017	25456482	Zaječice u Bečova 105	43526	Bečov	Ústecký
SPP Storage, PZP Dolní Bojanovice, PZP Dolní Bojanovice	B	12.10.2016	24822191	Dolní Bojanovice 891	69617	Dolní Bojanovice	Jihomoravský
SSE Explo Česká republika	B	01.01.2014	27262383	Tuchořice 15	43969	Tuchořice	Ústecký
STV GROUP - Hajniště	B	01.01.2000	26181134		46365	Hajniště pod Smrkem	Liberecký

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

STV GROUP - Polička, středisko Polička	B	14.06.2016	26181134	Bořiny 1145	57201	Polička	Pardubický
STV MINING, sklad Rataje, Výrobní závod Rataje	B	31.05.2017	28987250	Rataje u Kroměříže 1	76701	Kroměříž	Zlínský
Styrotrade, Čakovičky	A	16.12.2020	26152924	Zlonínská 99	25063	Čakovičky	Středočeský
SUEZ CZ	A	23.03.2017	25638955	Slovenská 2084/102	70900	Ostrava	Moravskoslezský
SYNTHESIA	B	01.04.2006	60108916	Semtín 103	53217	Pardubice	Pardubický
Synthomer / Hexion	B	10.01.2006	11771	Tovární 1	35680	Sokolov	Karlovarský
Synthos - Litvínov	B	01.01.2008	28214790	Záluží 1	43670	Litvínov	Ústecký
Synthos Kralupy	B	01.01.2008	28214790	O. Wichterleho 810	27852	Kralupy nad Vltavou	Středočeský
Synthos PBR	B	30.06.2012	28252012	O. Wichterleho 810	278 01	Kralupy nad Vltavou	Středočeský
ŠKODA AUTO	A	06.12.2016	00177041	tř. Václava Klementa 869	29360	Mladá Boleslav	Středočeský

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

TAMEH Czech	A	15.07.2016	28615425	Vratimovská 689/117	71901	Ostrava - kunčice	Moravskoslezský
TAMERO INVEST	A	22.12.2011	247814520	O. Wichterleho 810	278 01	Kralupy nad Vltavou	Středočeský
TEMPERATIOR	A	14.04.2016	27881369	Kociánova		Liberec	Liberecký
Teplárna Strakonice	A	19.12.2011	60826843	5. května mazutové hospodářství	386 43	Strakonice	Jihočeský
Teplárna Tábor	A	09.09.2011	60826827	U cihelny 2128	390 02	Tábor	Jihočeský
Tereos TTD Dobrovice, Dobrovice	A	03.05.2011	16193741	Palackého náměstí 1	29441	Dobrovice	Středočeský
Tereos TTD Kojetín	A	03.05.2011	16193741	Padlých hrdinů 927/865	75233	Kojetín	Olomoucký
Tereos TTD-lihovar Kolín	A	01.01.2000	16193741	Havlíčkova 140	28002	Kolín	Středočeský
Terminal Oil, Tlustice	A	19.11.2012	48921925	Tlustice	268 01	Hořovice	Středočeský
TEVA Czech Industries	A	01.01.2009	26785323	Ostravská 29 305	74770	Opava - Komárov	Moravskoslezský

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

TOMEGAS - Branice u Milevska	B	03.01.2005	25174363		39843	Branice u Milevska	Jihočeský
TOMEGAS - Olomouc	A	14.12.2004	25174363	areál Moravských železáren	77200	Olomouc	Olomoucký
TOPEK -Oil.cz	A	19.09.2016	28992717	S.K.Neumana 2816	530 02	Pardubice	Pardubický
TOPEK -Oil.cz, Sklad PHM – areál Elektrárny Dětmarovice, Sklad PHM – areál Elektrárny Dětmarovice	A	11.12.2017	28992717	areál elektrárny Dětmarovice 1202	73571	Dětmarovice	Moravskoslezský
TŘINECKÉ ŽELEZÁRNY	B	01.01.2000	18050646	Průmyslová 1000	73970	Třinec	Moravskoslezský
Tyco Electronics Czech, sklad	A	10.11.2016	48910791	K AMP 1293	66434	Kuřim	Jihomoravský
UNION CONSULTING	B	27.09.2004	26898985	Kostelec u Heřmanova Městce 162	53803	Heřmanův Městec	Pardubický
Veolia Energie ČR Špičková výtopna Olomouc	A	18.01.2012	45193410	Pavelkova 1081/20	772 00	Olomouc	Olomoucký
VIA-REK	A	18.07.2006	49450956	Old. Blažka 145	67902	Rájec-Jestřebí	Jihomoravský

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

Vojenský technický ústav, Provozovna Vrbětice	A	26.11.2018	24272523	Vlachovice 407	763 24	Vlachovice	Zlínský
Výzkumný ústav organických syntéz	B	01.01.2000	60108975	Rybitví 296	53218	Pardubice	Pardubický
WEIGEL CZ žárové zinkování, Velké Meziříčí	A	29.11.2016	26259125	Průmyslová 2052	59401	Velké Meziříčí	Vysočina
ZEVETA Bojkovice	B	26.07.2007	25691465	Tovární 532	68771	Bojkovice	Zlínský
ZVI	A	16.10.2015	47673621	Slavičín 1	76324	Vlachovice	Zlínský
ZZN Polabí - Bezděčín	B	31.07.2006	45148163	Bezděčín 79	29301	Mladá Boleslav	Středočeský
ZZN Polabí - Kolín	A	25.08.2006	45148210	K Vinici 1304	28066	Kolín	Středočeský
ZZN Polabí - Křinec	A	25.08.2006	45148210	Vestecká 296	28933	Křinec	Středočeský
ZZN Polabí - Nymburk	B	01.01.2009	45148210	Pražská 2214	28802	Nymburk	Středočeský
Želivská provozní - Želivka, Želivská provozní	A	01.01.2000	29131804	Hulice 106	25763	Trhový Štěpánov	Středočeský

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

Příloha B – Souhrn postupů při zařazování objektů nakládajících s vybranými nebezpečnými chemickými látkami nebo chemickými směsmi a řešení možných kybernetických incidentů

Tato příloha si klade za cíl stručným a věcným způsobem shrnout výše uvedené poznatky z dokumentu a nabídnout zájemcům ucelený konkrétní návod, jak dle legislativy postupovat při zařazování objektů chemického průmyslu, jaké činit opatření v souladu s garantem kybernetické bezpečnosti, a jaké podniknout kroky v případě vzniknuvšího bezpečnostního incidentu.

Příloha kromě textového popisu nabízí také přehledný situační diagram a případovou studii s vybraným objektem a incidentem.

B.1 Popis konkrétních kroků při zařazování objektů chemického průmyslu, opatření kybernetické bezpečnosti a řešení incidentu

V první řadě je nutné ověřit, zda vybraný objekt spadá do regulí zákona **č. 224/2015 Sb.** [1] a to pomocí metodického pokynu **Posouzení objektu s vybranými nebezpečnými chemickými látkami nebo chemickými směsmi a plnění obecných povinností právnických nebo podnikajících fyzických osob, včetně způsobu zařazení objektu do skupiny A nebo B a zpracování návrhu zařazení podle zákona č. 224/2015 Sb., o prevenci závažných havárií (dále jen zákon)** [3].

Základní pojmy, které se objevují v tomto pokynu, jsou následující:

- **Provozovatel** - uživatel či majitel objektu viz. **Vymezení osob a objektů, na které se zákon vztahuje** níže.
- **Objekt** - areál podniku, závod nebo provozovna, podzemní zásobník plynu.
- **Nebezpečná látka** - jedná se o látku nebo směs, která splňuje kritéria týkající se fyzikální nebezpečnosti, nebezpečnosti pro zdraví nebo nebezpečnosti pro životní prostředí stanovená v částech 2 až 5 přílohy I nařízení Evropského parlamentu a Rady (ES) **č. 1272/2008** o klasifikaci, označování a balení látek a směsí, o změně a zrušení směrnic 67/548/EHS a 1999/45/ES a o změně nařízení (ES) č. 1907/2006, v platném znění (dále jen nařízení **CLP**). Nebezpečné látky a směsi se klasifikují podle příslušných tříd a kategorií bezpečnosti uvedených v příloze č. 1 pokynu [3].

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

- **Umístění nebezpečné látky** - Umístění nebezpečné látky v objektu je projektované množství nebezpečné látky. Určuje se na základě údajů ve výrobní nebo stavební dokumentaci. U technologických jednotek nebo jejich částí, jako například zásobník hořlavin nebo potrubní most se množství určuje na základě projektové dokumentace dodavatele zařízení. Kapacita stavebních objektů pro skladování se posuzuje na základě údajů v kolaudačních rozhodnutích. V případě nově zřizovaného objektu se množství určí na základě projektové dokumentace použité pro podání návrhu na zahájení územního řízení o jeho umístění, popřípadě žádosti o vydání stavebního povolení. U podzemních zásobníků plynu se určuje množství nebezpečné látky na základě součtu maximálního skladovacího objemu.

Postup zařazení objektu je dle metodického pokynu následující:

- **Vymezení osob a objektů, na které se zákon vztahuje** - osobami využívající dotčený objekt mohou být **právnická osoba** dle **č. 89/2012 Sb. §20**, případné **podnikající fyzická osoba** dle **č. 89/2012 Sb. §420**. Povinnosti se nově také vztahují na **provozovatele podzemních zásobníků plynu.** Naopak se nevztahují na **vojenské objekty** a **vojenská zařízení,** nebezpečí spojená s **ionizujícím zářením**, **silniční**, **drážní**, **leteckou** a **vodní přepravu nebezpečných látek** mimo objekty, **přepravu nebezpečných látek v potrubích**, včetně souvisejících **přečerpávacích stanic postavených mimo objekt v trase potrubí**, **geologické práce**, **hornickou činnost** a **ukládání na odkaliště a skládky odpadu**, včetně **podzemního skladování odpadu.**

- **Vytvoření vstupních podkladů pro zařazení objektu do skupiny A nebo B** - **provozovatel** má povinnost zpracovat seznam umístěných **nebezpečných látek.** Určení množství nebezpečných látek vychází ze **součtu všech dílčích množství nebezpečných látek, které jsou v objektu umístěny**:
  - v technických a technologických jednotkách (projektovaná maximální kapacita);
  - ve skladovacích a provozních zásobnících (projektovaná maximální kapacita);
  - ve skladech podle jejich projektované nebo kolaudované kapacity;
  - v dopravních potrubích (projektovaná maximální kapacita);
  - v přepravních zařízeních, například vagónech a nákladních automobilech, které zastavily nebo stojí v objektu a jsou určena pro potřeby manipulace (vykládání surovin, nakládání hotových výrobků) nebo uskladnění spojené s přečerpáváním nebo překládáním látek, meziproduktů nebo výrobků do nádrží nebo skladů;
  - množství, která se mohou nahromadit v objektu v případě ztráty kontroly nad průmyslovým chemickým procesem nebo při vzniku havárie.

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

Pro sestavení seznamu je nutné provedení kompletního auditu všech nebezpečných látek a směsí v objektu. V seznamu pro zařazení objektu jsou rozhodující údaje:

- název látky definovaný podle nomenklatury IUPAC nebo ISO,
- identifikace látky číslem CAS (Chemical Abstracts Service),
- celkové množství látky v objektu v tunách,
- klasifikace nebezpečné látky podle nařízení (ES) č. 1272/2008 (CPL),
- fyzikální forma látky.

- **Principy a způsob zařazení objektu do skupiny A nebo B** -
  - Pokud **umístěné množství nebezpečné látky nebo směsi překračuje kvalifikační množství** tabulky 1 nebo tabulky 2 v příloze č. 2 pokynu [3] , je **objekt zařazen do skupiny A nebo B**.
  - Pokud umístěné množství **jedné nebezpečné látky nebo směsi nepřekračuje kvalifikační množství** uvedené v tabulce 1 nebo tabulce 2 přílohy č. 2 pokynu [3], je **nutné použít vzorec pro sčítání poměrného množství nebezpečných látek** postupem podle bodu 8. Přílohy č. 1 k zákonu **č. 224/2015 Sb.** viz. níže:

$$N = \sum_{i=1}^{n} \frac{qi}{Qi}$$

kde:
qi = množství nebezpečné látky *i* umístěné v objektu,
Qi = příslušné množství nebezpečné látky *i* uváděné v sloupci 2 (při posuzování objektu k zařazení do skupiny A) nebo sloupci 3 (při posuzování objektu k zařazení do skupiny B) tabulky 1 nebo tabulky 2 v příloze č. 2 pokynu [3],
n = počet nebezpečných látek,
N = ukazatel vyjadřující součet poměrů qi ku Qi.

Vzorec pro sčítání poměrných množství se použije **nejprve s kvalifikačním množstvím pro skupinu A**.

- Pokud je výsledek výpočtu hodnoty **N menší než 1,** objekt **nebude** zařazen do působnosti zákona - provozovatel zpracuje protokol dle přílohy č. 2 zákona **č. 224/2015 Sb.**
- Pokud je výsledek výpočtu hodnoty **N roven nebo větší než 1, bude** objekt zařazen do působnosti zákona.

Zda bude zařazen do skupiny A nebo B, rozhodne opakování výpočtu podle téhož vzorce, kdy bude pro výpočet dosazeno **kvalifikační množství pro skupinu B.**

- Pokud je výsledná hodnota **menší než 1**, **bude** objekt zařazen do **skupiny A**.

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

        - Pokud je výsledná hodnota **rovna nebo větší než 1**, **bude** objekt zařazen do **skupiny B.**
    - V relevantních případech je **nutné provést výpočet postupem až třikrát**, protože je nutno posoudit zvlášť nebezpečnost pro zdraví, fyzikální nebezpečnost a nebezpečnost pro životní prostředí.
    - Při posuzování směsi s chemickou látkou jako **volně oddělitelnou složkou** se zahrne do výpočtu **jen toto oddělitelné množství chemické látky podle jejích nebezpečných vlastností**.
    - Při posuzování směsi obsahující chemickou látku s nebezpečnými vlastnostmi jako **neoddělitelnou složku** se zahrne do výpočtu **celkové množství směsi podle nebezpečné vlastnosti směsi**.
    - Nebezpečné látky, na které se nevztahuje nařízení **(ES) č. 1272/2008 - CLP**, ale přesto jsou nebo by mohly být v objektu přítomny a mají nebo by mohly mít za podmínek existujících v objektu rovnocenné vlastnosti z hlediska potenciálu závažné havárie včetně odpadu, budou dočasně zařazeny do nejvhodnější kategorie nebo přiřazeny k nejvhodnější jmenovitě uvedené kategorii nebo nebezpečné látce spadající do oblasti působnosti zákona.

- **Zpracování návrhu na zařazení objektu do skupiny A nebo B** - Pokud objekt **splňuje podmínky pro zařazení do skupiny A nebo B**, je provozovatel povinen zpracovat a odeslat příslušnému krajskému úřadu **návrh na zařazení objektu**. Vzor návrhu na zařazení objektu do skupiny A nebo B je uveden v příloze č. 2 zákona **č. 224/2015 Sb.** Návrh musí být podepsán buď statutárním orgánem, nebo fyzickou osobou oprávněnou jednat za provozovatele objektu.

Jakmile je objekt zařazen do skupiny, musí v něm být nastaven bezpečnostní režim, který se snaží minimalizovat riziko závažné havárie, která by mohla vzniknout právě z důvodu přítomnosti nebezpečných látek.

U objektu, který spadá pod regulaci zákona **č. 224/2015 sb.** je nutné dále vyhodnotit, zda také není současně **provozovatelem základních služeb**, případně **také provozovatelem informačního nebo komunikačního systému** z pohledu plnění zákona **č. 181/2014 sb. – Zákon o kybernetické bezpečnosti**. Dle **2 písm. i) zákona č. 181/2014 Sb.** jsou **objekty nakládající 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 ji rozebrat na jednotlivé faktory, které musí daný objekt plnit:

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

- **Objekt provozuje činnost v odvětví s vybranými nebezpečnými chemickými látkami nebo chemickými směsmi** – určuje zákon **č. 224/2015 Sb.** a výše byl popsán postup určení a zařazení objektu.

- **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 dokumenty **Provozovatel informačního nebo komunikačního systému podle zákona o kyb. bezpečnosti** [25] a **Metodika k vodítkům pro hodnocení dopadů** [26] oba vydané Národním úřadem pro kybernetickou a informační bezpečnost - NÚKIB.

  Provozovatelem informačního nebo komunikačního systému se podle **§ 2 písm. g) zákona č. 181/2014 sb.** rozumí **„orgán nebo osoba zajišťující funkčnost technických a programových prostředků tvořících informační nebo komunikační systém“**.

  Provozovatelem informačního nebo komunikačního systému tak z definice zpravidla **bude** orgán nebo osoba, která má na starosti:

  - nasazování nových aplikací a patchů do produkčního prostředí,
  - nasazování hardwaru do produkčního prostředí,
  - provádění konfigurace, provozu, údržby, profylaxe nebo oprav technického vybavení, komunikačních prostředků nebo programového vybavení daného systému,
  - správu privilegovaných (administrátorských) a uživatelských účtů,
  - poskytování cloudových služeb,
  - trvalou správa auditních logů.

  Provozovatelem informačního nebo komunikačního systému podle zákona naopak **nebude** orgán nebo osoba, která:

  - určitým způsobem sice ovlivňuje fungování určeného systému, nicméně její činnost nepředstavuje zajišťování funkčnosti technických a programových prostředků tvořících systém (např. provádí hodnocení rizik, zajišťuje školení pro uživatele a administrátory, apod.),
  - zajišťuje funkčnost technických a programových prostředků, které ale netvoří určený systém (provozovaná aktiva jsou např. mimo rozsah systému řízení bezpečnosti informací),
  - nezajišťuje funkčnost technických a programových prostředků, ale pouze tyto prostředky systému využívá (typicky uživatel),

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

- je dodavatelem provozovatelů (tedy poddodavatel),
- je dodavatelem programových prostředků, které mohou být v systému instalovány, ale sama je do systému nemůže implementovat, nemůže je sama v systému udržovat ani aktualizovat – tedy nezajišťuje funkčnost programových prostředků svým přímým působením v systému (např. dodavatelé operačních systémů, firmwarů i aplikačního softwaru bez možnosti přístupu k systému),
- zajišťuje provoz či testování technických a programových prostředků v testovacím nebo vývojovém prostředí, a tato prostředí jsou od produkčního prostředí určeného systému oddělena (např. testování zranitelností před nasazením do produkčního prostředí).

V obou případech (objekt **je či není provozovatelem informačního nebo komunikačního systému**) je nutné u takového objektu definovat **správce** (případně jej delegovat na straně dodavatele/provozovatele), který je zodpovědný za provozované systémy a jsou na něj vztaženy povinnosti vycházející ze zákona **č. 181/2014 sb.**.

V případě, že objekt **není** provozovatelem systému/ů, má **provozovatel objektu povinnost identifikovat a informovat dodavatele/provozovatele těchto systémů za účelem plnění povinností podle zákona č. 181/2014 sb.** Jedná se především o:

- hlásit kontaktní údaje NÚKIB (§ 16 zákona),
- zavádět bezpečnostní opatření (§ 4 zákona),
- hlásit kybernetické bezpečnostní incidenty (§ 8 zákona),
- provádět opatření (§ 11 zákona),
- stejně tak jako o další povinnosti, kterými jsou např. povinnost předat správci data, provozní údaje a informace na vyžádání (§ 6a odst. 2 zákona), povinnost předat správci data, provozní údaje a informace při ukončení spolupráce (§ 6a odst. 3 zákona), povinnost předat správci data, provozní údaje a informace na základě rozhodnutí vydaného NÚKIB (§ 15a zákona).

V tomto případě **má správce povinnost dále spolupracovat s informovaným provozovatelem** a dohlížet na plnění výše uvedených bodů.

V případě, že objekt **je** provozovatelem systému/ů, jsou výše **uvedené povinnosti přímou odpovědností správce systémů** a ten je také povinen zahájit správní řízení s NÚKIB viz. níže.

- **Splňuje daná odvětvová a dopadová kritéria** – určuje vyhláška **č. 437/2017 Sb**. a zákon **č. 181/2014 Sb.**

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

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 nakládající s vybranými nebezpečnými chemickými látkami, chemickými směsmi, ropou nebo zemním plynem jsou konkrétní kritéria uvedena v **Příloze vyhlášky č. 437/2017.**

Pokud posuzovaný objekt splňuje v rámci **odvětvových kritérií** zařazení do určitého druhu služby a druhu subjektu, je nutné následně posuzovat **dopadová kritéria** v případě bezpečnostního kybernetického incidentu v informačním systému nebo síti elektronických komunikací.

V případě že objekt **splňuje** některé z **odvětvových kritérií** a následně **splňuje** i minimálně jedno z **dopadových kritérií**, stává se **Provozovatelem základní služby**.

Pokud objekt plní výše uvedenou definici a je určen jako **Provozovatel základní služby,** dochází k **zahájení správního řízení mezi provozovatelem a NÚKIB**. Provozovatel základní služby **má také podobné povinnosti**, jako **Provozovatel informačních a komunikačních systémů** a sice:

- hlásit kontaktní údaje NÚKIB (§ 16 zákona),
- zavádět bezpečnostní opatření (§ 4 zákona),
- hlásit kybernetické bezpečnostní incidenty (§ 8 zákona),
- provádět opatření (§ 11 zákona),

V případě, že je **Provozovatel základní služby** zároveň **Provozovatelem informačního nebo komunikačního systému**, zasílá výše uvedené informace **pouze jednou** (probíhá jedno řízení s NÚKIB).

V průběhu správního řízení NÚKIB s objektem konzultuje nutnost a účel provozovaného informačního nebo komunikačního systému, žádá od **správce**, případně **provozovatele informačního nebo komunikačního systému** popis systému a žádá o plnění požadavků dle vyhlášky **č. 82/2018 Sb.** o kybernetické bezpečnosti. Dochází také k vyplnění dotazníku [30], který NÚKIB poskytuje provozovateli.

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

Vyhláška definuje organizační a technická opatření, definuje pojem kybernetický bezpečnostní incident, jeho formát a primárně způsoby jeho řešení a určení reaktivních opatření.

Níže je uvedena tabulka, která přehledně popisuje požadované aktivity od provozovatele a reflektuje rozdíl v povinnostech mezi **Provozovatelem základní služby** a **Provozovatelem informačního nebo komunikačního systému:**

Tab. 1 Povinnosti provozovatelů podle zákona č. 181/2014 Sb.

Povinnosti ze zákona	Provozovatel informačního nebo komunikačního systému [§ 3 písm. f) zákona]	Provozovatel základní služby [§ 3 písm. g) zákona]
Hlášení kontaktních údajů	Vládnímu CERT, resp. NÚKIB, prostřednictvím formuláře hlášení kontaktních údajů (uveden na internetových stránkách NÚKIB)	
Hlášení kybernetických bezpečnostních incidentů	Vládnímu CERT, resp. NÚKIB, prostřednictvím formuláře hlášení kybernetického bezpečnostního incidentu (uveden na internetových stránkách NÚKIB).	
Provádění reaktivních opatření	Musí provést reaktivní opatření, které jim ukládá NÚKIB na základě informací o probíhajícím bezpečnostním incidentu, k řešení takového incidentu, anebo k zabezpečení informačních systémů nebo sítí a služeb před kybernetickým bezpečnostním incidentem. Reaktivní opatření je vydáváno ve formě rozhodnutí nebo ve formě opatření obecné povahy.	Neprovádí.
Oznámení o provedení reaktivních opatření	O provedení reaktivního opatření jsou orgány nebo osoby povinny informovat, formou hlášení, Vládní CERT, resp. NÚKIB.	Neoznamuje.
Provádění ochranných opatření	Musí provést ochranné opatření, účelem ochranných opatření je dodatečně reagovat na zkušenosti z řešení nastalých kybernetických bezpečnostních incidentů. Ochranné opatření je vydáváno ve formě opatření obecné povahy.	Neprovádí.
Detekce kybernetických bezpečnostních událostí	Správce systému je povinen provádět detekci kybernetických bezpečnostních událostí.	Správce systému je povinen provádět detekci kybernetických bezpečnostních událostí.
Implementace a provádění bezpečnostních opatření	Správce systému musí provádět bezpečnostní opatření podle vyhlášky o kybernetické bezpečnosti.	Správce systému musí provádět bezpečnostní opatření podle vyhlášky o kybernetické bezpečnosti.

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

Níže je také uveden souhrn bezpečnostních opatření, která vycházejí z vyhlášky a jsou rozdělena na část manažerskou a technickou:

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 Plan – 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 poskytovateli cloudových služeb, plnění vyhlášek a legislativy, certifikátu ČSN ISO/IEC 27001 nebo auditní zprávu SOC 2 Type II (AT101).

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

- 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.

Pro konkrétní technická doporučení v oblasti kybernetické bezpečnosti informačních a komunikačních systémů je možné využít dokumenty **Minimální bezpečnostní standard** [24] a **Minimální požadavky na kryptografické algoritmy** [29]. V těchto materiálech je možné nalézt doporučené 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 hašovacích funkcí.

Proces správního řízení s NÚKIB a zmiňované zákony a vyhlášky také od p**rovozovatele informačního a komunikačního systému základní služby vyžadují tvorbu bezpečnostní dokumentace,** kdy je možné využít vytvořený metodický pokyn v **příloze C** tohoto dokumentu. Pokyn rozebírá jednotlivé potřebné bezpečnostní dokumenty a požadavky vyplývající především ze zákona **č. 181/2014 Sb.** a vyhlášky **č. 82/2018 Sb.**

Závěrem této části je ještě vhodné zmínit lhůty pro plnění povinností u provozovatelů. Lhůty pro plnění povinností se řídí podle zákona **č. 181/2014 Sb.**

- **Provozovatel základní služby, který není zároveň správcem nebo provozovatelem informačního nebo komunikačního systému** základní služby, plní po vydání rozhodnutí o určení provozovatelem základní služby povinnosti **neprodleně**.
- **Provozovatel základní služby, který je zároveň správcem nebo provozovatelem informačního nebo komunikačního systému** základní služby, plní povinnosti **neprodleně**.
- **Správci a provozovatelé informačního nebo komunikačního systému, v případech, kdy Provozovatel základní služby je rozdílný od správce nebo provozovatele informačního nebo komunikačního systému** základní služby, mají počítány lhůty ode dne, kdy byl správce informován provozovatelem základní služby:
    - Lhůta pro nahlášení kontaktních údajů NÚKIB - 30 dní.
    - Lhůta pro implementaci ostatních povinností daných zákonem - hlášení kybernetických bezpečnostních incidentů, zavedení bezpečnostních opatření, reaktivní opatření - 12 měsíců.
    - Plnění zákonných povinností a jejich možná kontrola ze strany NÚKIB - po uplynutí lhůty v předchozím bodě.

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

B.2 Případová studie

V této části přílohy je uveden konkrétní příklad objektu, jehož provozovatel podniká v oblasti chemického a petrochemického průmyslu a tento objekt k podnikání využívá. Je tedy nutné zjistit, zda objekt spadá pod regulaci zákona **č. 224/2015 Sb.** a následně, zda je dle zákona **č. 181/2014 Sb.** provozovatelem základní služby, případně provozovatelem informačního nebo komunikačního systému. Pokud ano, následuje proces řízení s NÚKIB a ukázkový případ řešení možného kybernetického bezpečnostního incidentu.

Postupujeme podle souhrnu pokynů v podkapitole B.1, tzn. nejprve jasně identifikujeme **provozovatele, objekt,** množství a povahu **nebezpečných látek** včetně jejich **umístění.**

Provozovatelem je firma s ručením omezeným, tzn. **právnická osoba** dle **č. 89/2012 Sb. §20** a na provozovatele se nevztahuje žádná s výjimek (vojenský objekt, přeprava nebezpečných látek, skládka odpadu apod…).

Objektem je budova v průmyslovém areálu, kde majitelem areálu je jiná osoba, než-li provozovatel. I v tomto případě je veškerá odpovědnost na provozovateli.

Množství nebezpečných látek a jejich **umístění** je nejlépe zjistitelné tak, že je vytvořen seznam, který zároveň tvoří **vstupní podklad pro zařazení objektu do skupiny A nebo B.** Je nutné tedy provést **součet všech dílčích množství nebezpečných látek, které jsou v objektu umístěny,** dle výše uvedených definic.

Níže v tabulce 2 je uveden příklad seznamu pro vybraného provozovatele:

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

Tab. 2 Seznam nebezpečných látek včetně umístěného množství ve vybraném objektu [3]

Název látky	CAS	Klasifikace/ H-věty	Kategorie nebezpečnosti - tabulka 1 / tabulka 2	Objem / kapacita dle projektu	Identifikace umístění	Fyzikální forma látky	Množství v tunách	Kvalifikační množství v tunách	
								A	B
Aceton	67-64-1	Flam. Lig. 2: H225 Eye Irrit. 2 : H319 STOT SE 3: H336	P5c hořlavé kapaliny	20 000 x 1l	malé obaly (sklad)	kapalná	114,55	5 000	50 000
				2 500 x 10l	kanystry (sklad)				
				4 x 25 000l	zásobníky				
Dimethylsulfát	77-78-1	Carc. 1B: H350 Muta. 2: H341 Acute tox. 2, imhalation: H330 Acute tox. 3: H301 Skin Corr. 1B: H314 Skin Sens. 1: H317	Jmenovitě vybraná látka	225 l	zásobník	kapalná	0,3	0,5	200
Dusitan sodný	7632-00-0	Ox. Sol. 3: H272 Acute Tox. 3: H301 Aquatic Acute 1: H400	P8 oxidující kapaliny a tuhé látky	5 000 kg	zásobník	pevná	5	50	200
			E1 Nebezpečnost pro vodní prostředí v kategorii akutní 1 nebo chronická 1					100	200
Kyslík	7782-44-7	Ox. Gas 1: H270 Press. Gas: H281 Press. Gas, H280	Jmenovitě vybraná látka	1 x 20 000 kg	zásobník	kapalná	28,52	200	2 000
				600 x 50l	tlaková láhev	plynná (200 bar)			
Acetylen	74-86-2	Flam. Gas 1; H220, EUH006 Press. Gas, H280	Jmenovitě vybraná látka	332 x10 kg 100 x 6 kg	tlaková láhev	rozpuštěný	3,920	5	50

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

Benzín	-	Flam. liq. 1: H224 Asp. Tox. 1: H304 Skin irit. 2: H315 Repr. 2: H361 Muta. 1B: H340 Carc. 1B: H350 STOT Single Exp. 3: H336 Aquatic Chronic 2: H411	Jmenovitě vybraná látka	10 x 50 000 l	vlakové cisterny	kapalná	385	2 500	25 000
1-Naftylamin	134-32-7	Acute Tox. 4: H302 Aquatic Chronic 2: H411 Carc. 1A: H350	E2 Nebezpečnost pro vodní prostředí v kategorii chronická 2	4 x 5 000 kg	zásobník	pevná	20	200	500
Oxid dusný	10024-97-2	Ox. Gas 1: H270 Press. Gas: H280	P8 oxidující kapaliny a tuhé látky	20 000 kg	zásobník	kapalná	20	50	200
Oxid siřičitý	231-195-2	Acute Tox. 3: H 331 Skin Corr. 1A: H 314 EUH071 Press. Gas: H280	H2 AKUTNÍ TOXICITA kategorie 3, inhalační cesta expozice	4 x 990 Kg 2 x 550 Kg	sud	kapalná	5,06	50	200

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

Z tabulky je patrné, že umístěné **množství žádné z nebezpečných látek nepřekračuje** kvalifikační množství pro zařazení do skupiny A nebo B.

Z tohoto důvodu je **nutné použít sčítací vzorec** viz. příklad níže:

- Pro látky, které spadají do třídy akutní toxicita, kategorii 1, 2 nebo 3 (inhalační cesta expozice) nebo toxicita pro specifické cílové orgány – jednorázová expozice kategorie 1, s nebezpečnými látkami spadajícími do oddílu H tříd H1 až H3.
  N = dimethylsulfát/0,5 + oxid siřičitý/50
  N = 0,3/0,5 + 5,06/50 = **0,712 což je < 1**

- Pro látky, které jsou výbušniny, hořlavé plyny, hořlavé aerosoly, oxidující plyny, hořlavé kapaliny, samovolně reagující látky a směsi, organické peroxidy, samozápalné kapaliny a tuhé látky, oxidující kapaliny a tuhé látky, s nebezpečnými látkami spadajícími do oddílu P tříd P1 až P8.
  N = aceton/5 000 + dusitan sodný/50 + kyslík/200 + acetylen/5 + benzín/2 500 + oxid dusný/50
  N = 114,55/5 000 + 5/50 + 28,52/200 + 3,92/5 + 385/2 500 + 20/50 = **1,604 což je > 1**

- Pro látky, které spadají mezi nebezpečné pro vodní prostředí, akutně kategorie 1, chronicky kategorie 1 nebo chronicky kategorie 2, s nebezpečnými látkami spadajícími do oddílu E tříd E1 a E2.
  N = Dusitan sodný/100 + Benzín/2 500 + 1-Naftylamin/200
  N = 5/100 + 385/2 500 + 20/200 = **0,304 což je < 1**

- Pro druhý případ, ve kterém vychází ukazatel N >1, se provede součet rovněž s kvalifikačním množstvím pro zařazení do skupiny B.
  N = aceton/50 000 + dusitan sodný/200 + kyslík/2 000 + acetylen/50 + benzín/25 000 + oxid dusný/200
  N = 114,55/50 000 + 5/200 + 28,52/2 000 + 3,92/50 + 385/25 000 + 20/200 = **0,235 což je < 1**

Výsledkem použití sčítacího vzorce pro příkladový objekt je **zařazení objektu do skupiny A.** Provozovatel zasílá na příslušný krajský úřad **návrh na zařazení objektu.** Vzor návrhu na zařazení objektu do skupiny A nebo B je uveden v příloze č. 2 zákona **č. 224/2015 Sb.** Návrh musí být podepsán buď statutárním orgánem, nebo fyzickou osobou oprávněnou jednat za provozovatele objektu.

Provozovatel má nyní za úkol zjistit, zda není také **provozovatelem základních služeb**, případně **také provozovatelem informačního nebo komunikačního systému** z pohledu plnění zákona **č. 181/2014 sb. – Zákon o kybernetické bezpečnosti**.

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

Provozovatel v objektu **užívá informační systém**, který slouží pro dávkování nebezpečných látek za účelem chemické výroby technických plynů, a dále informační systém pro dávkování a čerpání pohonných hmot. Na systému neprovádí žádné instalační, hardwarové, aktualizační, údržbové, či konfigurační kroky a ani nespravuje role v systému.

Informační systém dodává, implementuje, aktualizuje a konfiguruje externí dodavatel, který je odpovědný za veškerou správu systému včetně výměny hardwaru**.**

Nyní je jasné, že **provozovatel není provozovatelem informačního nebo komunikačního systému** a je nutné zjistit, zda **informační a komunikační systém splňuje** definovaná **odvětvová a dopadová kritéria** podle vyhlášky **č. 437/2017 Sb.** tak, aby bylo možné zjistit, zda se **provozovatel** stává **provozovatelem základní služby** a dodavatel informačního nebo komunikačního systému se stává **provozovatelem informačního nebo komunikačního systému základní služby**.

Příloha **vyhlášky č. 437/2017** definuje níže uvedené tabulky s kritérii pro provozovatele, který pracuje s petrochemickými a chemickými produkty:

Tab. 3 Odvětvová a dopadová kritéria pro objekty nakládající s ropnými produkty dle vyhl. 437/2017 Sb.

Odvětvová kritéria (vycházejí ze směrnice **2016/1148/EU (NIS)**			**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**	
1.2.2. Provoz ropovodu	Provozovatel zařízení na těžbu, zpracování, rafinaci nebo úpravu ropy, skladovacího nebo přenosového zařízení na ropu	a) Zařízení na těžbu, zpracování, rafinaci nebo úpravu ropy s instalovanou roční výrobní kapacitou minimálně 3000000 tun, b) zásobník nebo komplex zásobníků s kapacitou nejméně 20000 m3, c) skladovací zařízení na LPG o kapacitě nejméně 20000 m3, d) produktovod s kapacitou přepravy produktů více než 3000000 tun ročně, e) přenosové zařízení na ropu nebo f) technický dispečink využívaný k provozu rafinérie, skladu,	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

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

		přenosového zařízení na ropu nebo k těžbě, zpracování nebo úpravě ropy.	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.
1.2.2. Provoz ropovodu	Provozovatel ropovodu	a) Vnitrostátní ropovod s kapacitou přepravy ropy více než 500000 tun ročně, b) koncové zařízení pro předání ropy nebo c) technický dispečink využívaný k provozu ropovodu.	

Tab. 4 Odvětvová a dopadová kritéria pro objekty nakládající s vybranými nebezpečnými chemickými látkami nebo chemickými směsmi dle vyhl. 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 obvodu obce s rozšířenou působností, které by mohlo vyžadovat provedení záchranných a likvidačních prací
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	-	

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

8.9. Výroba jiných základních organických chemických látek	Výrobce jiných základních organických chemických látek	-	složkami integrovaného záchranného systému.

Z pohledu **odvětvových kritérií** se nejprve provozovatele podívá na tabulku č. 3, která definuje kritéria pro ropný průmysl.

Provozovatel skladuje sice ropný produkt - benzín, ale i přesto si chce ověřit, zda splňuje uvedená kritéria. Jednotným druhem služby u ropných odvětvových kritérií je **1.2.2. Provoz ropovodu,** druhem subjektu je **Provozovatel zařízení na těžbu, zpracování, rafinaci nebo úpravu ropy, skladovacího nebo přenosového zařízení na ropu** a provozovatele vzhledem k povaze skladování nebezpečných látek zajímá nejvíce Speciální kritérium druhu subjektu - **zásobník nebo komplex zásobníků s kapacitou nejméně 20000 m3.**

Jednoduchým výpočtem zjistí, že součet zásobníků se skladovaným benzínem je pod limitem kritéria:
50 000l x 10 = 500 000 l = **500 m3 < 20 000 m3**

V případě ropných produktů tedy provozovatel **nesplňuje odvětvová kritéria**, **není** proto nutné se zabývat **dopadovými kritérii**.

Dále je potřeba zkontrolovat kritéria pro chemický průmysl - tabulka 4.

Provozovatel v objektu realizuje výrobu technických plynů a to konkrétně výrobu **oxidu dusného.** V případě **odvětvových kritérií** tedy bude zkoumat nejprve Druh služby - **8.1. Výroba technických plynů**, dále Druh subjektu - **Výrobce technických plynů** a tento druh subjektu nemá žádná speciální kritéria.

Provozovatel zjišťuje, že **splňuje odvětvová kritéria** pro objekty nakládající s vybranými nebezpečnými chemickými látkami nebo chemickými směsmi dle **vyhl. 437/2017 Sb.**

Následuje zkoumání **dopadových kritérií**, která jsou následující:

Dopad kybernetického bezpečnostního incidentu v informačním systému nebo síti elektronických komunikací, na jejichž fungování je závislé poskytování služby, může způsobit

- závažné omezení či narušení druhu služby postihující více než 50000 osob,
- závažné omezení či narušení jiné základní služby nebo omezení či narušení provozu prvku kritické infrastruktury,
- hospodářskou ztrátu vyšší než 0,25 % HDP,
- nedostupnost druhu služby pro více než 1600 osob, která není nahraditelná jiným způsobem bez vynaložení nepřiměřených nákladů,

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

- oběti na životech s mezní hodnotou více než 100 mrtvých nebo 1000 zraněných osob vyžadujících lékařské ošetření nebo,
- 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.

Jelikož **výroba oxidu dusného** probíhá tepelným rozkladem a tato reakce může být **silně exotermní**, může dojít k **explozi při výrobě**. Navíc jsou v objektu skladovány další hořlavé a explosivní látky, které by mohly případnou havárii a její dopad násobit. **Provozovatel** si je vědom, že **velká část výroby je řízena právě informačním systémem**, kde by mohlo při **kybernetickém bezpečnostním incidentu dojít právě k takovému typu havárie**.

V našem případě se objekt nachází v zastavěné průmyslové zóně, a proto **provozovatel dochází ke zjištění**, že v případě havárie může dojít k plnění **dopadového kritéria - oběti na životech s mezní hodnotou více než 100 mrtvých nebo 1000 zraněných osob vyžadujících lékařské ošetření** nebo/a n**arušení veřejné bezpečnosti na významné části správního obvodu obce s rozšířenou působností, které by mohlo vyžadovat provedení záchranných a likvidačních prací složkami integrovaného záchranného systému.**
Provozovatel tedy **plní odvětvová** i **dopadová kritéria** a stává se v tu chvíli **Provozovatelem základní služby.** Dodavatel informačního systému se v tu chvíli stává **Provozovatelem informačního systému základní služby.**

V tomto případě je **provozovatel** povinen dle zákona **č. 181/2014 sb. neprodleně** informovat **dodavatele a zároveň správce**, že se stali **provozovatelem informačního systému základní služby.** Vzor informování dodavatele/provozovatele, lze nalézt v příloze dokumentu **Provozovatel informačního nebo komunikačního systému** [25].

Následuje zahájení **správního řízení s NÚKIB**, jak ze strany **Provozovatele základní služby**, tak i ze strany **Provozovatelem informačního systému základní služby.**

Provozovatelé se řídí povinnostmi vycházejících z tabulky 1 v podkapitole B.1. Nejprve vyplní formulář s hlášením kontaktních údajů dostupný na internetových stránkách NÚKIB, kdy **Provozovatel základní služby** musí toto udělat **neprodleně, Provozovatel systému** má na nahlášení kontaktních údajů NÚKIB **30 dní.**

Provozovatel systému základní služby (externí dodavatel) musí v našem případě ve spolupráci s **Provozovatelem základní služby a NÚKIB** začít zavádět bezpečnostní opatření, která vychází z vyhlášky **č. 82/2018 Sb.** a jsou shrnuty v dokumentech **Minimální bezpečnostní standard** [24] a **Minimální požadavky na kryptografické algoritmy** [29]. Taktéž musí vypracovat **bezpečnostní dokumentaci** pro uvedený informační a komunikační systém základní služby. Metodický pokyn pro tvorbu dokumentace v rámci objektu chemického průmyslu je uveden v **příloze C** tohoto dokumentu. Na zavedení bezpečnostních opatření má **Provozovatel**

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

systému základní služby lhůtu **12 měsíců.** Po uplynutí této lhůty je NÚKIB oprávněn provádět bezpečnostní kontroly a audity za účelem ověření bezpečnostních opatření.

Předpokládejme nyní, že došlo ke **kybernetickému bezpečnostnímu incidentu**, který v **provozovaném informačním systému** změnil teploty a poměry při výrobě technického plynu a vlivem této změny došlo k **explozi v objektu a ztrátám na životech**.

Z pohledu řešení bezpečnostního incidentu je **neprodleně** nutné, aby **Provozovatel základní služby** i **Provozovatel informačního systému** hlásily incident NÚKIBu a to pomocí elektronického formuláře, který je dostupný na internetových stránkách úřadu, kdy je nutné bezpečnostní incident zařadit do jedné z níže uvedené kategorie:

- Kategorie III - velmi významný kybernetický bezpečnostní incident, při kterém je přímo a významně narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být všemi dostupnými prostředky zabráněno dalšímu šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých i potenciálních škod,

- Kategorie II - významný kybernetický bezpečnostní incident, při kterém je narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být vhodnými prostředky zabráněno dalšímu šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých škod, nebo

- Kategorie I - méně významný kybernetický bezpečnostní incident, při kterém dochází k méně významnému narušení bezpečnosti poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje zásahy obsluhy s tím, že musí být vhodnými prostředky omezeno další šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých škod

V našem případě se jedná o **bezpečnostní incident nejvyšší, tedy III kategorie** a **NÚKIB společně s národním CERT** zahajují šetření incidentu. Během šetření je zjištěno, že **nejpravděpodobnější vektor útoku** spočíval v tom, že **útočník získal přístup k administrátorskému účtu a roli vzhledem ke slabě volenému heslu** a n**apadení jednoho z aktivních síťových prvků, který využíval stejné přístupové údaje pro přístup k jeho administraci.** V roli administrátora poté **útočník mohl měnit parametry chemického procesu** výroby technického plynu a došlo tak k havárii.

V tomto případě dochází ke klasifikaci, kdy se bezpečnostní incident řadí mezi typy - **kybernetický bezpečnostní incident způsobující narušení důvěrnosti aktiv**, kde aktivy jsou v tomto případě myšleny uživatelské údaje a informace k účtům.

Dále NÚKIB, CERT a provozovatel informačního systému zjišťují, zda byla administrátorská aktiva správně klasifikována jako **kritická** tzn. nebyla veřejné přístupná, vyžadovala nadstandardní míru ochrany pomocí kryptografických prostředků, byla správně volena

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

autentizační opatření (biometrická, dvojfaktorová autentizace), bylo využito řízení a zaznamenávání přístupů, pro ochranu dostupnosti byly využívány záložní systémy.

Paralelně s šetřením incidentům dochází k **aktivaci plánů kontinuity (Business Continutiy Plan - BCP)**, případně **plánu obnovy (Disaster Recovery Plan - DRP)**, pokud byly v rámci bezpečnostní dokumentace vytvořeny.

Jakmile dojde alespoň k částečné **obnově informačních systému provozovatele** a vyšetření zásadních **nedostatků v bezpečnostních opatřeních**, jsou NÚKIBem, případně CERT **vyžadována reaktivní opatření**, která jsou vydávána ve formě rozhodnutí nebo ve formě opatření obecné povahy.

Provozovatel základní služby a **Provozovatel informačního systému základní služby** jsou **povinni** informovat vládní CERT či NÚKIB o **provedení reaktivních opatření formou hlášení.**

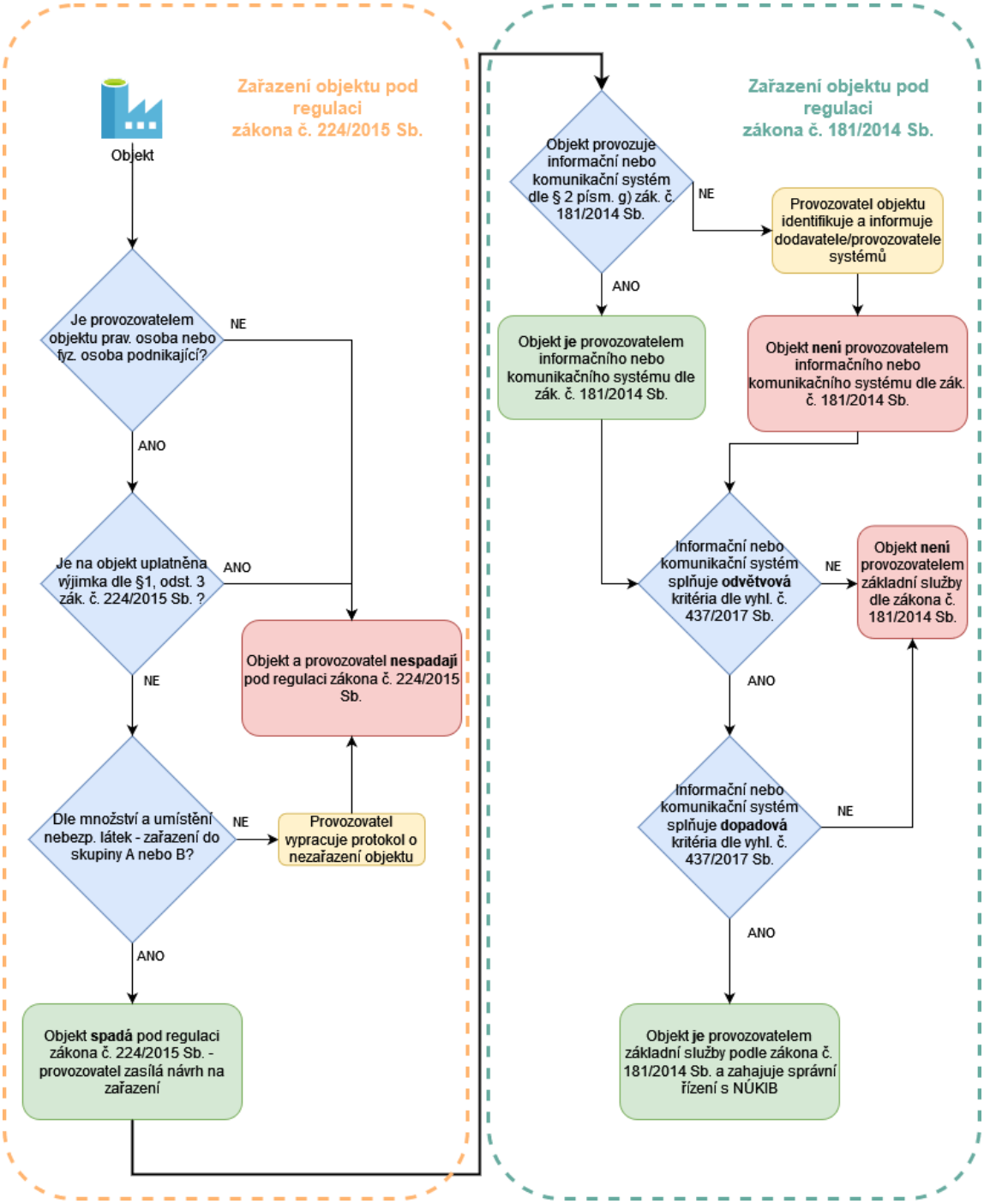
Následuje **provádění ochranných opatření**. Účelem ochranných opatření je **dodatečně reagovat na zkušenosti z řešení nastalých kybernetických bezpečnostních incidentů.** Ochranné opatření je **vydáváno ve formě opatření obecné povahy.**

NÚKIB a CERT uzavřou řešení kybernetického bezpečnostního incidentu a definují závěry, kdy prioritně **popisují vektor možného útoku, bezpečnostní opatření**, která byla aplikována a aktivována, **posoudí připravenost bezpečnostních opatření** na uvedený typ kybernetického útoku, **předávají případné důkazní materiály k dalšímu šetření složkám výkonné moci**, definují **reaktivní a ochranná opatření** a provádějí **kontrolu provozovatelů**, zda jsou tato opatření správně a včas aplikována.

B.3 Postupový diagram

Tato část prezentuje grafické znázornění zařazování objektu dle výše prezentovaných postupů popsaných v podkapitolách B.1 a B.2.

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.



Obr. 3 Postupový diagram pro zařazení objektu dle zákonů č. 223/2015 Sb. a č. 181/2014 Sb.

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

Příloha C – Metodický pokyn pro zpracování bezpečnostní dokumentace informačních a komunikačních systémů základní služby

Níže uvedený text definuje zásady pro tvorbu bezpečnostní dokumentace informačních a komunikačních systémů základní služby, kdy tyto systémy spadají pod regulaci zákona **č. 181/2014 Sb. o Kybernetické bezpečnosti** [11] a vyhlášky **č. 82/2018 Sb. o Kybernetické bezpečnosti** [19].

Cílem je definovat, jaké konkrétní dokumenty, a s jakým obsahem, by měly vzniknout v rámci prevence závažných havárií způsobených kybernetickým bezpečnostním incidentem u informačního a komunikačního systému základní služby v souladu s výše uvedeným zákonem a vyhláškou.

C.1 Dokument "Bezpečnostní politika informačního a komunikačního systému"

Dokument „Bezpečnostní politika informačního systému" je základním dokumentem bezpečnostní dokumentace informačního a komunikačního systému. Vzniká jako první v návaznosti na potřebu provozovat informační a komunikační systém základní služby.

Dokument „Bezpečnostní politika informačního systému" musí splňovat následující požadavky:

- neobsahuje konkrétní informace (typ HW nebo SW, umístění, nastavení parametrů apod.),
- je tvořen zejména deklaracemi naplnění požadavků právních norem především z oblasti kybernetických bezpečnostních opatřeních, kybernetických bezpečnostních incidentech a reaktivních opatření,
- je maximálně stručný a v rozsahu maximálně několika stran,
- je autorizován oprávněnou osobou organizace.

Struktura dokumentu "Bezpečnostní politika informačního a komunikačního systému

- 1. Úvodní ustanovení
- 2. Personální bezpečnost
- 3. Počítačová bezpečnost
- 4. Kryptografická ochrana
- 5. Fyzická bezpečnost
- 6. Průmyslové, řídicí a obdobné specifické systémy, digitální služby
- 7. Řízení a plánování kontinuity
- 8. Další bezpečnostní dokumentace

Kapitola - "1. Úvodní ustanovení"

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

Kapitola „Úvodní ustanovení“ slouží k základnímu popisu informačního a komunikačního systému a k vymezení základních bezpečnostních cílů.

Základní popis informačního systému obsahuje:

- základní definici struktury informačního systému (samostatný počítač, skupina samostatných počítačů, malá LAN, rozsáhlá LAN),
- základní určení dislokace informačního systému (neuvádí se konkrétní umístění, ale pouze rozsah umístění informačního systému jedna/několik místností, jedno/několik pater budovy, jedno/několik budov v jednom/několika areálech apod.),
- určení základních typů periferních zařízení (síťové/lokální tiskárny a skenery, aj.),
- určení hodnocení důvěrnosti aktiv dle **přílohy č. 1 k vyhlášce č. 82/2018 Sb.**,
- určení hodnocení integrity aktiv dle **přílohy č. 1 k vyhlášce č. 82/2018 Sb.**,
- určení hodnocení dostupnosti aktiv dle **přílohy č. 1 k vyhlášce č. 82/2018 Sb.**,
- základní typ a účel zpracovávaných informací (běžné dokumenty, databáze, výkresová dokumentace apod.),
- základní typ aplikačního SW (kancelářský SW, SW pro kreslení technických výkresů apod.),
- předpokládaný počet uživatelů,
- použitý operační systém/systémy (neuvádí se konkrétní verze),
- vztah k jiným počítačovým sítím (u samostatných osobních počítačů např. vyjmutí síťové karty, zákaz použití modemu, u LAN zpravidla izolace od jiných počítačových sítí),
- v případě záměru použití kryptografických prostředků uvést účel.

Mezi základní bezpečnostní cíle patří:

- zajištění důvěrnosti a integrity informace všude, kde se vyskytuje,
- zajištění dostupnosti informace a služeb informačního systému a odpovědnosti uživatele informačního systému za jeho činnost v něm,
- zajištění nepopiratelnosti a pravosti informací všude, kde je to aplikovatelné,
- zpracování informací bude probíhat v souladu s požadavky dalších právních předpisů, norem, mezinárodních smluv, nadřízené bezpečnostní politiky, interních předpisů apod. (uvést jejich případný seznam).

Kapitola - “2. Personální bezpečnost”

V kapitole „Personální bezpečnost“ jsou deklarovány základní požadavky na informační systém z hlediska personální bezpečnosti vycházející ze zákona **č. 181/2014 Sb.** a **§ 7 vyhlášky č. 82/2018 Sb.**

- definice rolí působících v informačním systému (manažer kybernetické bezpečnosti, architekt kybernetické bezpečnosti, auditor kybernetické bezpečnosti, uživatel apod.) včetně deklarace vytvoření provozních bezpečnostních směrnic pro tyto role, které budou definovat jejich povinnosti,

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

- deklarace základních požadavků na uživatele informačního systému:
  - o poučení a proškolení uživatele zastávající bezpečnostní role a určení pravidel a postupů pro řešení případů porušení bezpečnostních pravidel.
  - o pověření do role v informačním systému,
  - o používání privátních autentizačních informací,
  - o oznamování neobvyklého chování informačního a komunikačního systému a podezření na jakékoliv zranitelnosti.
- deklarace zavedení formálních postupů pro udělení oprávnění pro přístup do informačního systému, zavedení uživatele do informačního systému, pro včasné vyřazení uživatele při změně jeho pracovního zařazení, odchodu z organizace apod.,
- deklarace zásady používání jedinečného identifikátoru uživatele pro přístup k informačnímu systému.

Kapitola - "3. Počítačová bezpečnost"

V kapitole je deklarováno naplnění minimálních požadavků na bezpečnost komunikačních sítí podle **§ 18 vyhlášky č. 82/2018 Sb.**, požadavků správu a ověřování identit podle **§ 19 vyhlášky č. 82/2018 Sb.**, požadavků na řízení přístupových oprávnění podle **§ 20 vyhlášky č. 82/2018 Sb**., požadavků na ochranu před škodlivým kódem podle **§ 21 vyhlášky č. 82/2018 Sb.**, požadavků na zaznamenávání události informačního a komunikačního systému podle **§ 22 vyhlášky č. 82/2018 Sb.**, požadavků na detekci kybernetických bezpečnostních událostí podle **§ 23 vyhlášky č. 82/2018 Sb**., požadavků na sběr a vyhodnocování kybernetických bezpečnostních událostí podle **§ 24 vyhlášky č. 82/2018 Sb.**, požadavků na aplikační bezpečnost podle **§ 25 vyhlášky č. 82/2018 Sb**., požadavků na zajištění úrovně dostupnosti informací podle **§ 27 vyhlášky č. 82/2018 Sb.**

V rámci požadavků počítačové bezpečnosti je deklarováno zejména naplnění zajištění:

- zabezpečení komunikační sítě (segmentace, vzdálené přístupy),
- jednoznačné identifikace a autentizace,
- volitelného řízení k aktivům informačního systému,
- detekce a vyhodnocování kybernetických bezpečnostních událostí (ověření, kontrola, blokace),
- provádění penetračních testů a ochrany aktiv,
- nepřetržitého zaznamenávání a možnosti zpětného zkoumání auditních záznamů,
- ošetření paměťových objektů před jejich dalším použitím,
- bezpečnosti vstupně výstupních portů (zejména výměnné nosiče informací),
- ochrany před škodlivým kódem (zejména antivirová ochrana),
- požadavků na dostupnost informací a služeb informačního systému v čase a místě podle **§ 15 vyhlášky č. 82/2018 Sb**., (jak dlouho smí být služby nedostupné, jaká minimální funkčnost musí být zajištěna i v krizových situacích).

Kapitola - "4. Kryptografická ochrana"

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

V kapitole je deklarováno naplnění minimálních požadavků na kryptografické prostředky podle **§ 26 vyhlášky č. 82/2018 Sb.**. Lze také využít materiál - **Minimální požadavky na kryptografické algoritmy – doporučení v oblasti kryptografických prostředků** [29].

V rámci požadavků kryptografické ochrany je deklarováno zejména naplnění zajištění:

- používání aktuálně odolných kryptografických algoritmů a klíčů,
- používání systému správy klíčů a certifikátů (generování, distribuce, změna, zneplatnění).

Kapitola - "5. Fyzická bezpečnost"

V kapitole je deklarováno naplnění minimálních požadavků na fyzickou bezpečnost podle **§ 17 vyhlášky č. 82/2018 Sb.**.

V rámci požadavků fyzické bezpečnosti je deklarováno zejména naplnění zajištění:

- stanovení bezpečnostního perimetru,
- provádění opatření proti neoprávněnému vstupu, poškození a zásahům,
- ochrany na úrovni objektů (kamerové systémy, bezpečnostní služba, přístupy do místností v rámci objektu, ověřování vstupů do objektu).

Kapitola - "6. Průmyslové, řídicí a obdobné specifické systémy, digitální služby"

V kapitole je deklarováno naplnění minimálních požadavků na průmyslové, řídicí a obdobné specifické systémy podle **§ 28 vyhlášky č. 82/2018 Sb.**, a dále naplnění minimálních požadavků na digitální služby podle **§ 29 vyhlášky č. 82/2018 Sb..**[1]

V rámci požadavků průmyslových, řídicích a specifických systémů je deklarováno zejména naplnění zajištění:

- použití technických a programových prostředků pro specifické prostředí,
- vyčlenění komunikační sítě určené výhradně pro tyto systémy,
- řízení přístupů k těmto systémům,
- ochrana aktiv těchto systémů před využitím známých zranitelností,
- obnovení chodu systémů po kybernetickém bezpečnostním incidentu.

Kapitola - "7. Řízení a plánování kontinuity"

V kapitole je deklarováno zajištění řízení kontinuity a vypracování plánů kontinuity (havarijní plány a činnosti při krizových situacích a bezpečnostních incidentech) podle **§ 15 vyhlášky č. 82/2018 Sb.**.

Kapitola - "8. Další bezpečnostní dokumentace"

V kapitole je deklarováno, že bude provedena analýza rizik v souladu se stanovenými bezpečnostními požadavky a na základě výsledků této analýzy bude vypracován „Návrh

[1] Vzhledem k povaze zkoumaných objektů v tomto dokumentu (objekty chemického průmyslu), není dále naplnění bezpečnostních požadavků podle § 29 vyhlášky č. 82/2018 Sb. dále rozebíráno.

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

bezpečnosti informačního systému“, případně bezpečnostní směrnice pro jednotlivé role definované v informačním systému a případně další specifikované dokumenty (síťová topologie, výsledky bezpečnostního auditu, apod.).

C.2 Dokument “Analýza rizik informačního a komunikačního systému”

Dokument „Analýza rizik informačního a komunikačního systému“ je druhým dokumentem v rámci projektové bezpečnostní dokumentace. Analýza rizik vychází z dokumentu „Bezpečnostní politika informačního a komunikačního systému“ a snaží se nalézt možné hrozby a zranitelnosti působící na hodnocený informační systém a následně stanovit relevantní protiopatření pro zajištění přiměřené ochrany tak, aby byla tato protiopatření dostatečně účinná a současně finančně a organizačně přiměřená povaze chráněné věci.

Analýzu rizik je možno provádět různými metodami viz **ČSN ISO/IEC 27005 „Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací“**. Pro informační systémy malého rozsahu NÚKIB na základě normy **ČSN ISO/IEC 27005** vypracoval zjednodušenou metodiku hodnocení rizik, kterou poskytuje na základě písemného vyžádání objektům provozující informační a komunikační systém základní služby.

Zjednodušená analýza rizik je určena pro malé informační systémy (samostatná pracovní stanice).

Základní analýza rizik

Pro informační systémy malého rozsahu lze obecně konstatovat, že pokud jsou dodržena veškerá legislativní opatření a doporučení NÚKIB, pak lze předpokládat, že míry veškerých rizik jsou pod hodnotou akceptovatelné meze a informační systém lze pokládat za bezpečný.

V takovém případě postačuje, aby dokument „Analýza rizik informačního systému“ obsahoval pouze seznam identifikovaných aktiv a aplikovaných protiopatření.

Protiopatření v oblasti personální bezpečnosti a organizačních opatření

- Jsou jasně identifikována aktiva a bylo provedeno jejich hodnocení dle kritérií.(**§ 4 odst. 1 vyhlášky č. 82/2018 Sb.)**
- Je určena role garanta aktiv, který je zodpovědný za klasifikaci, evidenci, pravidla ochrany a používání aktiv (**§ 7 odst. 3 vyhlášky č. 82/2018 Sb.)**.
- Pro informační systém se zavádí systém bezpečnostní správy s rolí manažera a architekta kybernetické bezpečnosti. (**§ 7 odst. 1 a 2 vyhlášky č. 82/2018 Sb.).**
- Provozovatel informačního systému bude zajišťovat úvodní školení uživatelů, bezpečnostních správců a správců v dodržování opatření stanovených v bezpečnostní dokumentaci a správném užívání informačního systému. Další školení bude provozovatelem zajišťováno okamžitě při podstatných změnách v informačním systému a dále v pravidelných intervalech (**§ 9 vyhlášky č. 82/2018 Sb.)**.

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

- V bezpečnostní dokumentaci informačního systému budou pro řešení krizových situací stanovena opatření zaměřená na jeho uvedení do stavu odpovídající bezpečnostní dokumentaci. V bezpečnostní dokumentaci budou uvedeny základní typy krizových situací spolu se specifikovanými činnostmi zaměřenými na minimalizaci škod, likvidaci následků a zajištění informací potřebných pro zjištění příčin a mechanismu vzniku.
- Servisní činnost v informačním systému bude organizována tak, aby nebyla ohrožena jeho bezpečnost. Údržbu komponent informačního systému zajišťující bezpečnostní funkce nebo přímo ovlivňující jeho bezpečnost musí zajišťovat osoby, které mají pověření manažera nebo architekta kybernetické bezpečnosti.

Protiopatření v oblasti fyzické bezpečnosti

- Opatření fyzické bezpečnosti stanoví odpovědná osoba nebo jí pověřená osoba v projektu fyzické bezpečnosti.
- Orgán státu, právnická osoba a podnikající fyzická osoba budou zajišťovat a pravidelně ověřovat, zda použitá opatření fyzické bezpečnosti odpovídají projektu fyzické bezpečnosti a právním předpisům.
- Aktiva informačního systému budou umístěna do prostoru, ve kterém je zajištěna fyzická ochrana informačního systému před neoprávněným přístupem, poškozením a ovlivněním.
- Dle klasifikace aktiv informačního systému budou vybraná aktiva podle potřeby opatřena ochrannými prvky, tak aby je bylo možné otevřít, pouze při současném zničení těchto prvků.

Protiopatření v oblasti počítačové bezpečnosti

- Operační systémy budou nastaveny v souladu s doporučeními NÚKIB a dle příslušných zákonů a vyhlášek.
- Každý SW bude před nasazením do informačního systému testován v provozním prostředí s ohledem na požadovanou funkcionalitu a testování bude zadokumentováno.
- Řízení vstupně výstupních portů bude prováděno v souladu s doporučeními NÚKIB a dle příslušných zákonů a vyhlášek.
- Ochrana před škodlivým kódem bude prováděna v souladu s doporučeními NÚKIB a dle příslušných zákonů a vyhlášek.

Protiopatření v oblasti komunikační bezpečnosti

- Komunikační bezpečnost bude nastavena v souladu s doporučeními NÚKIB a dle příslušných zákonů a vyhlášek.
- Ochrana pasivních prvků síťové infrastruktury bude prováděna v souladu s doporučeními NÚKIB a dle příslušných zákonů a vyhlášek.
- Ochrana aktivních prvků síťové infrastruktury bude prováděna v souladu s doporučeními NÚKIB a dle příslušných zákonů a vyhlášek.

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

Protiopatření v oblasti průmyslových, řídicích a specifických systémů

- Bezpečnost takových systémů bude nastavena v souladu s doporučeními NÚKIB a dle příslušných zákonů a vyhlášek.
- Ochrana pasivních prvků síťové infrastruktury specifických systémů bude prováděna v souladu s doporučeními NÚKIB a dle příslušných zákonů a vyhlášek.
- Ochrana aktivních prvků síťové infrastruktury specifických systémů bude prováděna v souladu s doporučeními NÚKIB a dle příslušných zákonů a vyhlášek.

Doplňková analýza rizik

Pokud nelze splnit některá protiopatření definovaná v předešlých kapitolách, pak je nutné tuto skutečnosti zohlednit a odůvodnit v doplňkové analýze rizik.

Doplňková analýza rizik musí obsahovat:

- stanovení hrozeb a zranitelností na něž neaplikované protiopatření mělo působit,
- stanovení nových náhradních protiopatření,
- ohodnocení vlivu nových protiopatření na hrozby a zranitelnosti a
- odůvodnění dostatečnosti navrhovaných protiopatření.

C.3 Dokument “Návrh bezpečnostního informačního systému”

Dokument „Návrh bezpečnosti informačního systému“ je stěžejním dokumentem projektové bezpečnostní dokumentace informačního systému. Návrh bezpečnosti detailně rozpracovává aplikaci protiopatření stanovených v dokumentu „Analýza rizik informačního systému“ pro splnění požadavků definovaných v dokumentu „Bezpečnostní politika informačního systému“.

Dokument „Návrh bezpečnosti informačního systému“ musí splňovat následující požadavky:

- obsahuje konkrétní informace (typ HW nebo SW, umístění, nastavení parametrů apod.),
- je maximálně přesný,
- je autorizován oprávněnou osobou organizace.

Struktura dokumentu “Návrh bezpečnosti informačního systému”

- 1. Úvodní ustanovení
  - 1.1. Popis informačního systému
  - 1.2. HW konfigurace informačního systému
  - 1.3. SW konfigurace informačního systému
- 2. Personální bezpečnost
- 3. Počítačová bezpečnost
  - 3.1. Jednoznačná identifikace a autentizace
  - 3.2. Volitelné řízení přístupu
  - 3.3. Auditní záznamy
  - 3.4. Opakované použití objektů

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

    - 3.5. Ochrana před škodlivým kódem
    - 3.6. Instalace, používání a bezpečnostní nastavení SW
    - 3.7. Komunikační bezpečnost
    - 3.8. Servisní činnost
    - 3.9. Požadavky na dostupnost
- 4. Kryptografická ochrana
- 5. Fyzická bezpečnost
- 6. Průmyslové, řídicí a obdobné specifické systémy
- 7. Řízení a plánování kontinuity

Kapitola "1. Úvodní ustanovení"

Kapitola detailně rozpracovává základní popis informačního systému uvedený v dokumentu „Bezpečnostní politika".

Kapitola "1.1 Popis informačního a komunikačního systému"

- úplný a přesný popis informačního systému doplněný schématem,
- přesnou dislokaci informačního systému,
- určení hodnocení důvěrnosti aktiv dle **Přílohy č. 1 k vyhlášce č. 82/2018 Sb.**,
- určení hodnocení integrity aktiv dle **Přílohy č. 1 k vyhlášce č. 82/2018 Sb.**,
- určení hodnocení dostupnosti aktiv dle **Přílohy č. 1 k vyhlášce č. 82/2018 Sb.**,
- předpokládaný počet uživatelů,
- vztah k jiným počítačovým sítím (u samostatných osobních počítačů např. vyjmutí síťové karty, zákaz použití modemu, u LAN zpravidla izolace od jiných počítačových sítí),
- v případě záměru použití kryptografických prostředků uvést účel a typ.

Kapitola "1.2 HW konfigurace informačního a komunikačního systému"

Úplný a přesný seznam HW komponent včetně sériových čísel.
Informační systém samostatných počítačů (1 a více):

- typ PC s bližšími údaji o jeho komponentách včetně HDD,
- typ monitoru včetně typu připojení k PC (VGA, DVI apod.),
- human interface (klávesnice, myš) včetně typu připojení (PS2, USB apod.),
- HW kryptografické prostředky,
- periferní zařízení (např. zálohování, UPS).

Informační a komunikační systém typu LAN:

- servery – typ a bližší údaje o jejich komponentách,
- pracovní stanice – typ a bližší údaje o jejich komponentách včetně lokálních periferních zařízeních
- (např. tiskárny, UPS),
- HW kryptografické prostředky,

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

- síťové periferní zařízení (např. síťové tiskárny, disková pole, zálohovací zařízení, centrální UPS),
- pasivní prvky síťové infrastruktury (datové rozvody) – typ, způsob vedení apod.,
- aktivní prvky síťové infrastruktury (např. router, switch).

Kapitola "1.3 SW konfigurace informačního a komunikačního systému"

Úplný a přesný seznam SW komponent včetně označení jejich verzí.
Mezi SW komponenty patří zejména:

- operační systémy,
- aplikační SW (komerční i speciální),
- antivirové programy,
- SW kryptografické prostředky,
- zálohovací utility,
- administrátorské utility.

Kapitola "2. Personální bezpečnost"

- Definice rolí působících v informačním systému (podle bezpečnostní politiky),
- seznam konkrétních požadavků na osoby v jednotlivých rolích informačního systému:
  - pověření do role v informačním systému (kdo a jak),
  - proškolení ze znalostí provozních bezpečnostních směrnic (kdo a jak),
  - další konkrétní požadavky podle potřeb organizace (např. odborná způsobilost).
- popis způsobu pověřování osob vyžadovaných bezpečnostní politikou pro správu informačního systému (manažer kybernetické bezpečnosti, architekt kybernetické bezpečnosti, garant aktiv, auditor kybernetické bezpečnosti, správce, případně jejich zástupci aj.)
  - odkaz na přílohu, v níž jsou uvedeny osoby, aktuálně jmenované do těchto funkcí,
  - vzory formulářů pro jmenování uvedených osob,
  - zajištění zástupnosti,
  - případné sloučení rolí,
- popis postupu pro zařazení/vyřazení uživatele do/z informačního systému (kdo o tom rozhodne, kdo informuje manažera kybernetické bezpečnosti o zrušení oprávnění pro přístup do informačního systému před odchodem dané osoby z organizace, způsob sdělování této informace manažerovi kybernetické bezpečnosti, vzor formuláře se schválením zařazení/vyřazení uživatele do/z informačního systému),
- určení povinnosti vedení seznamu uživatelů manažerem kybernetické bezpečnosti informačního systému včetně vzoru seznamu uživatelů.
- definovat všechny evidence a formuláře vedené v informačním systému, kdo je vede, kdo je autorizuje, kde jsou ukládány během používání, kde a jak dlouho jsou uchovávány, jejich vzory, obvykle:
  - seznam uživatelů,

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

- evidence školení uživatelů,
- evidence provozních nosičů informací,
- u vyjímatelných HDD evidence výdeje/příjmu HDD z úschovného objektu,
- seznam HW (pokud není uveden v návrhu bezpečnosti),
- seznam SW (pokud není uveden v návrhu bezpečnosti),
- provozní deník systému (záznamy o opravách a údržbě, o provedení zálohy, o provedení updatu antivirového programu, o kontrole auditních záznamů a jejich zálohování, o krizových situacích a bezpečnostních incidentech, o dalších bezpečnostně relevantních událostech, charakteru administrativní pomůcky, s uvedením data, času, zúčastněných osob a jejich podpisů),
- případně další administrativní pomůcky.

Kapitola "3. Počítačová bezpečnost"

Uvést pro nasazené operační systémy původ použitého bezpečnostního nastavení (vlastní návrh, dodané třetí stranou apod.).

Bezpečnostní nastavení operačního systému může být obsaženo v jednotlivých podkapitolách kapitoly „Počítačová bezpečnost", nebo je možné shrnout veškerá nastavení bezpečnostních parametrů do samostatného dokumentu a v dokumentu „Návrhu bezpečnosti informačního systému„ se na něj pouze odkazovat.

Kapitola "3.1 Jednoznačná identifikace a autentizace"

- popis nastavení bezpečnostních parametrů operačního systému,
- popis případných použitých speciálních prostředků pro identifikaci a autentizaci včetně konkrétních údajů a nastavení (smart card, biometrické zařízení, apod.),
- pokud je používána identifikace a autentizace na aplikační úrovni, tak popsat a specifikovat potřebné nastavení,
- definice povinnosti uzamčením pracovní stanice nebo samostatného osobního počítače při krátkodobém opuštění zapnutého počítače a umožněním opětovné práce v systému až po úspěšné identifikaci a autentizaci uživatele,
- definice povinnosti bezpečného ukládání hesel pro speciální účty ve stanoveném úschovném objektu (vestavěné účty administrátorů, účty důležitých služeb, BIOS apod.).

Kapitola "3.2 Volitelné řízení přístupu"

- popis nastavení bezpečnostních parametrů operačního systému,
- pokud je používáno na aplikační úrovni, popsat a specifikovat potřebné nastavení,
- popis řízení přístupu k vstupně výstupním portům zejména k USB (zablokování přístupu všech uživatelů, umožnění přístupu pro konkrétní média konkrétním uživatelům apod.), uvést použité prostředky a příslušná nastavení,

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

- popis logické struktury pevných disků, pravidla pro řízení přístupu uživatelů k datové části pevného disku,
- matice přístupových práv pro uživatele.

Kapitola "3.3 Auditní záznamy"

- popis nastavení bezpečnostních parametrů operačního systému,
- definice povinnosti bezpečnostního správce:
  - zkoumat pravidelně auditní záznamy,
  - archivovat pravidelně auditní záznamy (kdy, jak a na jak dlouho),
- pokud je používáno vytváření auditních záznamů na aplikační úrovni, popsat a specifikovat potřebné nastavení (např. speciální SW pro řízení přístupu k USB),
- definovat omezení přístupu uživatelů k auditním záznamům,
- uvést a popsat používané nástroje pro analýzu auditních záznamů.

Kapitola "3.4 Opakované použití objektů"

- popis nastavení bezpečnostních parametrů operačního systému,
- v případě používání speciálních prostředků, např. utilit pro bezpečné vymazávání informací z pevných disků, popsat a specifikovat potřebné nastavení,
- definovat možnosti a způsob případné deklasifikace nosičů informací,
- definovat způsob zacházení s HW komponentami informačního systému, které obsahují nosiče informací (paměti typu RAM, HDD apod.), odpojování od napájecího napětí, vyjímání nosičů apod.

Kapitola "3.5 Ochrana před škodlivým kódem"

- uvést typ antivirového prostředku,
- definovat kdo bude zajišťovat jeho aktualizaci,
- definovat jak často bude prováděna jeho aktualizace.

Kapitola "3.6 Instalace, používání a bezpečnostní nastavení SW"

- uvést způsob zajištění správy konfigurace a vedení seznamu SW bezpečnostním správcem, včetně údaje o, případně používaném SW nástroji,
- uvést způsob zajištění údržby SW (aplikace opravných programových balíčků a aktualizací vydávaných výrobci SW).

Kapitola "3.7 Komunikační bezpečnost"

- typ kabeláže a použité standardy,

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

- síťové protokoly a pro ně potřebná konfigurace (např. MAC adresy, IP adresy a masky podsítí pro IP protokol),
- topografie LAN (fyzické umístění jednotlivých zařízení - servery, pracovní stanice, aktivní prvky sítě, kryptografické prostředky, kabely),
- topologie LAN (např. sběrnicová, hvězdicová, kruhová, fyzická segmentace na jednotlivých vrstvách OSI modelu a skutečná konfigurace síťových komponent, případně logická segmentace na bázi VLAN a konfigurační soubory), aj.

Kapitola "3.8 Servisní činnost"

- definovat povinnost pracovníků správy systému při provádění nebo zajišťování servisní činnost (kdo, jak a kde může servis provádět).

Kapitola "3.9 Požadavky na dostupnost"

- uvést požadavky na dostupnost definované v bezpečnostní politice,
- definovat systém zálohování SW i HW prostředků pro zajištění definované dostupnosti,
- definovat a popsat minimální funkčnost systému, která musí být zajištěna,
- definovat a popsat způsob obnovy systému,
- definovat odpovědnosti za zálohování a obnovu systému.

Kapitola "4. Kryptografická ochrana"

- uvést jaký kryptografický prostředek bude v informačním systému používán, přesný typ a počty prostředků, jak bude zajišťován klíčový materiál, kde bude umístěn a jak bude zajištěna jeho fyzická bezpečnost, vyškolený personál požadovaný pro jeho provoz, jaké dokumenty pro jeho provoz budou vytvořeny apod.

Kapitola "5. Fyzická bezpečnost"

- popsat zabezpečení všech prostor, v nichž budou umístěny komponenty informačního systému:
  - identifikace místnosti, které komponenty v ní jsou a aplikovaná opatření fyzické bezpečnosti včetně režimových opatření, pro podrobnější popis je možno provést odkaz na příslušný bezpečnostní projekt nebo směrnici,
  - zvlášť opatření pro servery a pro pracovní stanice,
  - rozmístění jednotlivých zařízení v místnosti, se zohledněním instalačních požadavků (např. formou grafického znázornění).
- definovat povinnost pracovníků správy systému v oblasti kontroly a vedení přehledu umístění všech zařízení a jejich rozmístění v stanovených prostorech,
- popsat, jak bude vedena evidence spjatá se vstupem uživatelů, pokud je vyžadována bezpečnostní politikou, evidenční pomůcky, procedury,

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

- popsat, jak bude vedena evidence spjatá se vstupem návštěv, pokud jsou povoleny v bezpečnostní politice,
- uvést umístění úschovných objektů pro ukládání výměnných nosičů informací a řešení řízení fyzického přístupu k těmto nosičům,
- definovat způsob použití a typ ochranných prvků pro pečetění krytů HW komponent,
- definovat povinnost pracovníků správy systému a uživatelů v oblasti kontroly ochranných prvků,
- definovat způsob evidence a označování HW komponent,
- definovat povinnost pracovníků správy systému v oblasti vedení seznamu HW komponent.

Kapitola "6. Průmyslové, řídicí a obdobné specifické systémy"

- v návaznosti na podkapitolu 3.7, uvést popis komunikačního systému určeného pro specifické systémy.
- definovat jakým způsobem je oddělena komunikační síť určená pro specifické systémy od standardní komunikační sítě.
- popis technických a programových prostředků, které jsou určeny do specifického prostředí,
- určení omezení a řízení přístupů a vzdáleného přístupů k těmto systémům.
- popis ochrany těchto systémů před využitím známých zranitelností a obnovení chodu těchto systémů po kybernetickém bezpečnostním incidentu.

Kapitola "7. Řízení a plánování kontinuity"

- definovat typy a modelové způsoby řešení možných krizových situací,
- definovat typy a modelové způsoby řešení bezpečnostních incidentů,
- definovat typy a modelové způsoby řešení možné kompromitace (v případě použití kryptografické ochrany),
- definovat povinnost pracovníků správy systému při řízení změn v provozovaném informačním systému (jak změny provádět a jaké změny hlásit NÚKIBu),
- definovat povinnost pracovníků správy systému při provádění testů bezpečnosti (způsob provádění a vyhodnocování testů).

C.4 Dokument "Bezpečnostní směrnice informačního a komunikačního systému"

Pro zajištění bezpečnosti během provozu informačního a komunikačního systému je na základě **§ 6 a 7 vyhlášky č. 82/2018 Sb.** vhodné vytvořit oddělené bezpečnostních směrnice pro klíčové osoby odpovědné za bezpečnostní řízení informačního a komunikačního systému, a také pro jednotlivé typy a role uživatelů informačního systému.

Obecně se i v malém informačním a komunikačním systému základní služby určuje manažer kybernetické bezpečnosti a garant aktiv (**§ 6 odst. 4 vyhlášky č. 82/2018 Sb.**), případně další role vyžadované povahou a užíváním systému.

TA ČR
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

Provozní bezpečnostní směrnice musí konkretizovat povinnosti osob při manipulaci s informacemi a informačním a komunikačním systémem. V dalším textu jsou proto uvedeny obvyklé povinnosti **manažera kybernetické bezpečnosti, garanta aktiv, architekta kybernetické bezpečnosti, auditora kybernetické bezpečnosti, správce informačního a komunikačního systému** a uživatele informačního a komunikačního systému základní služby.

Tyto seznamy nepředstavují univerzální a úplný seznam povinností uživatelů a bezpečnostních správců informačních systémů a je třeba k nim přistupovat z hlediska požadavků konkrétního informačního systému. Jednotlivé body vyžadují konkretizaci a rozvedení do potřebných podrobností. Rozdělení povinností mezi jednotlivé správce kybernetické bezpečnosti je možno modifikovat, s ohledem na úroveň bezpečnostního prověření správce informačního systému a předpokládané technické znalosti bezpečnostního správce informačního systému.

Pokud je v informačním systému zavedena další role související se zabezpečením informačního a komunikačního systému, je nutno navíc specifikovat povinnosti a procedury s ní spjaté. Dokumenty „Bezpečnostní směrnice“ musí být autorizovány oprávněnou osobou organizace.

Struktura bezpečnostních směrnic

Dokument „Bezpečnostní směrnice pro správce kybernetické bezpečnosti“ musí obsahovat minimálně kapitoly, které popisují:

- povinností dané role,
- práva dané role,
- procedury spojené s povinnostmi a právy dané role.

Dokument „Bezpečnostní směrnice uživatele“ musí navíc obsahovat kapitoly popisující:

- stručný a zjednodušený popis informačního systému včetně jeho rozsahu a umístění,
- definici a rozdělení krizových situací včetně základního popisu toho, jak se uživatel podílí na řešení,
- definici a rozdělení bezpečnostních incidentů včetně základního popisu toho, jak se uživatel podílí na řešení,
- definici kompromitace včetně základního popisu toho, jak se uživatel podílí na řešení (pouze při použití kryptografického prostředku).

V bezpečnostní směrnici bezpečnostního správce informačního systému je možno specifikovat jeho povinnosti a procedury s nimi spojené odkazem na dokument „Návrh bezpečnosti informačního systému“ (pokud jsou v něm řešeny).

V bezpečnostní směrnici uživatele je nutno uvádět úplnou a přesnou specifikaci jeho povinností a procedur s nimi spojených, neboť uživatel obvykle nemá k jiným dokumentům bezpečnostní dokumentace přístup.

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

Typické povinnosti manažera kybernetické bezpečnosti

- udržuje aktuální seznam oprávněných uživatelů,
- zajišťuje, aby fyzický přístup do prostor s HW komponentami informačního systému, k vyjímatelným pevným diskům apod. mohli získat jen oprávnění uživatelé,
- přiděluje uživateli uživatelské jméno a prvotní heslo, vytváří uživatelské účty a spravuje je ve shodě s bezpečnostní dokumentací, v případě potřeby mu v této činnosti poskytuje technickou podporu správce,
- ručí za trvalé dodržování schválené konfigurace HW i SW informačního systému, včetně nastavení bezpečnostních charakteristik operačního systému a aplikačního SW,
- ručí za dodržování umístění informačního systému a instalačních požadavků, ve shodě s bezpečnostní dokumentací,
- zkoumá a řeší bezpečnostní incidenty, hlásí je řediteli organizace (nebo jinému příslušnému funkcionáři),
- zajišťuje školení uživatelů v oblasti bezpečnosti informačního systému,
- kontroluje dodržování bezpečnostních směrnic,
- vede potřebné evidence (podle bezpečnostní dokumentace, uvést seznam evidencí),
- provádí správu dokumentace bezpečnosti informačního systému (kde je uložena apod.),
- vydává uživatelům výměnné pevné disky, přenosný počítač (popsat jak, pokud je ovšem tento postup použit),
- spolupracuje s ostatními správci při uvedení informačního systému do stavu odpovídajícího schválené bezpečnostní dokumentaci informačního systému po ostatních bezpečnostních incidentech nebo mimořádných událostech,
- hraje klíčovou úlohu při řešení základních krizových situací,
- je-li oblastí působnosti bezpečnostního správce LAN, musí být veškeré povinnosti rozšířeny do síťového prostředí, musí být zahrnuta kontrola neporušenosti kabeláže, aktivních prvků sítě, konfigurace VLAN apod.
- nesmí být pověřen výkonem rolí odpovědných za provoz informačního a komunikačního systému.

Typické povinnosti garanta aktiv

- určení a evidence jednotlivých primárních a podpůrných aktiv,
- hodnocení důležitosti primárních a podpůrných aktiv z hlediska důvěrnosti, integrity a dostupnosti,
- definuje pravidla ochrany jednotlivých úrovní aktiv,
- určuje způsoby rozlišování jednotlivých úrovní aktiv a pravidla pro manipulaci a evidenci aktiv podle těchto úrovní,
- zajišťuje v předepsaném rozsahu bezpečnost nosičů informací, zejména jejich vyřazování a ničení,
- disponuje dobrou znalostí spravovaných aktiv.

Typické povinnosti architekta kybernetické bezpečnosti

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

- zajištění návrhu implementace bezpečnostních opatření tak, aby byla zajištěna bezpečná architektura informačního a komunikačního systému,
- rozvoj architektury bezpečnosti,
- navrhuje hardwarové komponenty, nástroje a síťové architektury,
- navrhuje vhodné operační systémy a software,
- navrhuje podnikové procesy a jejich integraci a závislost na ICT,
- odpovídá za řízení bezpečnosti a rizik,
- provádí hodnocení a testování bezpečnosti,
- kontroluje integraci a závislosti ICT a obchodních procesů,
- je odpovědný za řízení dodavatelů a bezpečnostní opatření pro smluvní vztahy.

Typické povinnosti auditora kybernetické bezpečnosti

- provádí a dokumentuje bezpečnostní audit při prvotním nasazení informačního a komunikačního systému do provozního prostředí a poté při významných změnách, nejpozději však každé 2 roky,
- kontroluje dodržování bezpečnostní politiky, včetně přezkoumání technické shody, a výsledky auditu zohlední v plánu rozvoje bezpečnostního povědomí a plánu zvládání rizik,
- posuzuje soulad bezpečnostních opatření s nejlepší praxí, právními předpisy, vnitřními předpisy, jinými předpisy a smluvními závazky vztahujícími se k informačnímu a komunikačnímu systému a určí případná nápravná opatření pro zajištění souladu,
- zkoumá pravidelně auditní záznamy a vytváří jejich archivní kopie takovým způsobem, aby bylo umožněno jejich zpětné zkoumání, obvykle 3 roky nazpět,
- zajišťuje ochranu záložních kopií auditních záznamů před modifikací nebo zničením,
- zkoumá auditní záznamy po bezpečnostním incidentu,
- nesmí být pověřen výkonem jiných bezpečnostních rolí.

Typické povinnosti správce informačního a komunikačního systému

- provádí činnost administrátora operačního systému (správce sítě LAN), stanoveným způsobem zabezpečuje denní provoz informační systém po technické stránce,
- instaluje operační systém, aplikační SW, zajišťuje aktualizaci antivirového SW,
- provádí zálohování systémového programového vybavení, zajišťuje ochranu záložních dat (konkretizovat systém zálohování, kde jsou zálohy ukládány apod.),
- spolupracuje s manažerem a architektem kybernetické bezpečnosti informačního a komunikačního systému při nastavení bezpečnostních charakteristik operačního systému a aplikačního SW podle schválené bezpečnostní dokumentace informačního a komunikačního systému,
- spravuje uživatelské účty ve spolupráci s manažerem kybernetické bezpečnosti informačního a komunikačního systému,
- spolupracuje s manažerem kybernetické bezpečnosti informačního a komunikačního systému při vyčištění a zotavení systému po napadení viry,

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

- spolupracuje s manažerem kybernetické bezpečnosti informačního a komunikačního systému při uvedení informačního systému do stavu odpovídajícího schválené bezpečnostní dokumentaci informačního systému po ostatních bezpečnostních incidentech nebo mimořádných událostech.

Typické povinnosti uživatele

Bezpečnostní směrnice pro uživatele vyžaduje přehledné a srozumitelné zpracování. Nesmí obsahovat údaje, které uživatel nepotřebuje znát a které by mu umožnily zneužití informačního systému. Zejména je třeba, aby byl uživatel informován:

- o účelu informačního systému,
- jaké je standardní zahájení práce v informačním systému (přístup, přihlašovací procedura a postup identifikace a autentizace uživatele, jaká jsou omezení v počtu chybných přihlášení, délce hesla a době jeho platnosti, délce PINu čipové karty apod.),
- jakou kontrolu HW (případně kabeláže), prostředí nebo podle okolností i jiných prvků informačního systému má provést před započetím práce,
- jak má zacházet s vyjímatelnými pevnými disky a dalšími nosiči informací používanými v daném informačním systému,
- do jakého úschovného objektu má ukládat klasifikované nosiče informací nebo od koho je před započetím práce v informačním systému získá a komu je po skončení práce vrací k uložení,
- jakým způsobem získá vyjímatelný pevný disk nebo přenosný počítač nebo jiný HW systému před započetím práce, jakým způsobem ho opět vrací, s tím spjaté povinnosti a evidence,
- v jaké oblasti pevného disku může/má ukládat uživatelské soubory, případně že je na lokální pevný disk ukládat nesmí/nemůže apod.,
- jak musí/může zálohovat uživatelská data a na jaký nosič informací, jak musí chránit záložní nosiče informací,
- jak se chovat k návštěvě, jak k pracovníkům úklidu (aby to vyhovovalo bezpečnostní dokumentaci),
- o své povinnosti dodržovat schválenou konfiguraci HW a SW,
- o své povinnosti hlásit poruchy HW i SW, výskyt bezpečnostního incidentu nebo podezření na možnost kompromitace aktiv,
- o tom, jaké základní bezpečnostní incidenty se mohou vyskytnout a jak má bezprostředně reagovat, pokud to typ události vyžaduje, před kontaktem s manažerem kybernetické bezpečnosti,
- o zavedené ochraně vstupně výstupních portů, zejména v souvislosti s používáním USB paměťových zařízení,
- o postupu pro export informací z informačního systému na nosič informací, pokud je uživateli povolen,

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.

- o postupu pro import informací do informačního systému prostřednictvím nosiče informací, pokud je uživateli povolen,
- o postupech při ničení a skartaci nosičů informací a příslušných pravidlech administrativní bezpečnosti,
- o předepsaném postupu při nutnosti opustit počítač v běhu, povolená lhůta,
- o proceduře pro standardní bezpečné ukončení práce v informačním systému - veškeré povinnosti týkající se počítače, periférií, místnosti, klíčů, EZS atd.
- o správném používání hesla, jak ho tvořit, že ho nesmí sdílet, prozradit atd.,
- o ochraně, kterou musí poskytovat magnetické nebo čipové kartě (případně jiným pomůckám) využívané pro identifikaci a autentizaci uživatele v informačním systému,
- o způsobu používání klíčů od místnosti, systému elektrické zabezpečovací signalizace, systému elektronické kontroly vstupu, podle konkrétní situace, je možno řešit i odkazem na příslušný bezpečnostní projekt objektové a technické bezpečnosti,
- o tom, jaké základní mimořádné (krizové) situace mohou nastat a jaké jsou jeho povinnosti při jejich řešení,
- o všech svých dalších povinnostech vyplývajících z bezpečnostní dokumentace informačního a komunikačního systému, v potřebné míře o okolnostech umožňujících mu pochopení jeho povinností.

T A
Č R
Projekt SS02030008 **Centrum environmentálního výzkumu: Odpadové a oběhové hospodářství a environmentální bezpečnost (CEVOOH)** je spolufinancován se státní podporou Technologické agentury ČR v rámci **Programu Prostředí pro život**.