Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

# DŮVODOVÁ ZPRÁVA

## A. Obecná část

## B. Zvláštní část

Bezpečnostní opatření pro poskytovatele regulované služby v režimu vyšších povinností jsou vyjmenována v § X odst. 2 *[Seznam bezpečnostních opatření poskytovatele regulované služby]* zákona. Bezpečnostní opatření jsou organizační a technická. Pro přehlednost je níže uveden jejich výčet – tomuto výčtu v rámci návrhu vyhlášky odpovídají § 4 a následující. Ačkoliv je výčet bezpečnostních opatření pro poskytovatele regulované služby v režimu vyšším ve většině případů totožný s výčtem bezpečnostních opatření daných dosavadním zákonem č. 181/2014 Sb., o kybernetické bezpečnosti, resp. vyhláškou č. 82/2018 Sb., o kybernetické bezpečnosti, došlo v tomto návrhu vyhlášky k některým dílčím úpravám. Tyto zmíněné rozdíly jsou způsobeny především dynamickým vývojem v oblasti kybernetické bezpečnosti. Další motivací Úřadu pro úpravu názvů jednotlivých opatření v rámci jednotlivých bezpečnostních opatření uvedených v tomto návrhu vyhlášky byla snaha o přesnější a praxi bližší pojmenování jednotlivých požadavků.

| **§ X odst. 2 písm. a) *[Seznam bezpečnostních opatření poskytovatele regulované služby]* zákona – organizační opatření** |
|---|
| 1) systém řízení bezpečnosti informací |
| 2) povinnosti vrcholového vedení |
| 3) bezpečnostní role |
| 4) řízení bezpečnostní politiky a bezpečnostní dokumentace |
| 5) řízení aktiv |
| 6) řízení rizik |
| 7) řízení dodavatelů |
| 8) bezpečnost lidských zdrojů |
| 9) řízení změn |
| 10) akvizice, vývoj a údržba |
| 11) řízení přístupu |
| 12) zvládání kybernetických bezpečnostních událostí a incidentů |
| 13) řízení kontinuity činností |
| 14) audit kybernetické bezpečnosti |
| **§ X odst. 3 písm. b) *[Seznam bezpečnostních opatření poskytovatele regulované služby]* zákona – technická opatření** |
| 1) fyzická bezpečnost |

| |
|---|
| 2) bezpečnost komunikačních sítí |
| 3) správa a ověřování identit |
| 4) řízení přístupových oprávnění |
| 5) detekce kybernetických bezpečnostních událostí |
| 6) zaznamenávání bezpečnostních a relevantních provozních událostí |
| 7) vyhodnocování kybernetických bezpečnostních událostí |
| 8) aplikační bezpečnost |
| 9) kryptografické prostředky |
| 10) zajišťování dostupnosti regulované služby |
| 11) zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv |

**K § 1 (Předmět úpravy)**

Předmětem úpravy návrhu vyhlášky o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu vyšších povinností je především stanovení obsahu jednotlivých bezpečnostních opatření a rozsahu, v jakém jsou poskytovatelé regulované služby v režimu vyšších povinností bezpečnostní opatření povinny zavést a provádět s cílem zajištění bezpečnosti regulované služby a aktiv. Návrh vyhlášky vedle bezpečnostních opatření dále stanoví pro poskytovatele regulované služby v režimu vyšších povinností podmínky lokalizace při zpracování dat v zahraničí.

Návrhem vyhlášky, jehož předmět úpravy je vymezen v § 1, realizuje Úřad zmocnění, které je mu svěřeno na základě § X odst. 1 písm. e) a i) *[Prováděcí právní předpisy a zmocňovací ustanovení]* zákona o kybernetické bezpečnosti.

**K § 2 (Vymezení pojmů)**

V rámci předmětného ustanovení jsou vymezeny základní pojmy, které jsou ve vyhlášce o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu vyšších povinností používány. Vymezení pojmů je souladné s pojmy užívanými v oblasti ICT a vychází, mimo jiné, z terminologie obsažené v nejlepších praktikách (zejm. z normy ISO/IEC 27000). Do této oblasti spadají i definice primárního aktiva, podpůrného aktiva, technického aktiva nebo poskytovatele regulované služby podle zákona o kybernetické bezpečnosti, tyto pojmy jsou však již definovány zákonem o kybernetické bezpečnosti. Toto ustanovení obsahuje definice spojené především se systémem řízení bezpečnosti informací, řízením rizik, řízením změn či řízením dodavatelů. Většina definic v této oblasti vychází z oficiálních zdrojů (je zejm. v souladu s normou ISO/IEC 27001).

Významnou změnou se pak rozumí každá změna ovlivňující bezpečnost informací, u níž povinný subjekt, bez ohledu na již zavedená bezpečnostní opatření, může předpokládat ohrožení bezpečnosti informací. K určení významnosti změny subjekt využije pravidla, postupy a kritéria, které si sám stanoví a budou přiměřené danému konkrétnímu prostředí organizace. Běžně se za významnou změnu může považovat např. změna, která mění funkčnost, konfiguraci, integraci, či architekturu systému, popřípadě i změna významného dodavatele nebo urgentní změna.

Svoji zásadní roli při prosazování požadavků kybernetické bezpečnosti zaujímá vrcholové vedení, které je definováno jako osoba nebo skupina osob, které řídí poskytovatele regulované služby, nebo statutární orgán. Jinými slovy se jedná o nejvyšší představitele organizace jako je např. předseda představenstva či ředitel organizace. Praktickým příkladem významu pojmu vrcholového vedení v případě obchodní společnosti je přímo z definice vyplývající statutární orgán, v případě ministerstev je jím pak myšlen ministr. Tyto osoby mohou plnění po nich vyžadovaných povinností, vyplývajících z tohoto návrhu vyhlášky, delegovat na své zástupce. Tito zástupci však musí mít zajištěny potřebné pravomoci, a to především k řízení implementace bezpečnostních opatření.

Toto ustanovení dále definuje vzájemně související pojmy, a to administrátor a privilegovaný uživatel, přičemž tyto pojmy mezi sebou nelze zaměňovat. Obecně se uživatelem rozumí každý, kdo využívá aktiva (především technická). Privilegovaný uživatel může svojí činností na technickém aktivu způsobit zásadní dopad na bezpečnost regulované služby. Jedná se zpravidla o osoby disponující účtem lokálního administrátora na své koncové stanici nebo osoby, které mohou aktivně zasahovat např. do personálního nebo ekonomického systému, který je automatizovaně napojený na správu uživatelských účtů. Nejedná se tedy na první pohled z perspektivy této osoby (například zaměstnance personálního nebo ekonomického oddělení) o interakce přímo ovlivňující zabezpečení regulované služby, avšak tyto osoby mohou například významně ovlivnit nastavení zavedených bezpečnostních opatření. Osoba disponující na své koncové stanici účtem lokálního administrátora může například dle vlastní vůle instalovat software, omezovat nebo jinak přizpůsobovat zavedená bezpečnostní opatření na dané koncové stanici, což představuje značné riziko např. z pohledu nakažení škodlivým kódem, a proto je považována za privilegovaného uživatele. Zejména je takto vnímán účet lokálního administrátora v doménovém prostředí, který má nadstandardní oprávnění a privilegia, zatímco běžný uživatel s uživatelských účtem tato oprávnění nemá.

Administrátorem se rozumí privilegovaný uživatel nebo osoba, která zajišťuje mj. správu, provoz, údržbu či bezpečnost technického aktiva. Administrátorem je např. zaměstnanec IT oddělení odpovědný za nastavování zabezpečení technických aktiv nebo dodavatel se stejnou odpovědností.

Rozlišování mezi pojmy privilegovaný uživatel a administrátor je zavedeno z toho důvodu, že je potřebné rozlišit mezi chápáním pojmu administrátor, jakožto někoho, kdo zpravidla interaguje s technickými aktivy v rovině, která přímo ovlivňuje zabezpečení regulované služby (jako např. zaměstnanci IT nebo bezpečnostního oddělení nebo dodavatelé odpovědní za správu technických aktiv), a privilegovaným uživatelem, jehož např. pracovní náplní není přímo nastavování technických aktiv nebo jejich konfigurací, avšak jeho běžná činnost může ovlivnit bezpečnost regulované služby. Náplní práce privilegovaného uživatele není tedy zajišťovat správu, provoz, použití, údržbu a bezpečnost technického aktiva, což je náplní práce a odpovědností administrátora, přičemž administrátor k této činnosti vyžaduje privilegovaná oprávnění, tudíž musí být zároveň i privilegovaným uživatelem. V praxi může ovšem v tomto rozlišování vznikat tenká pomyslná hranice, kdy např. privilegovaný uživatel může dostat v rámci jeho pracovní náplně odpovědnost za zajišťování správy, provozu a údržby jeho koncové stanice, a následné záleží na kontextu organizace dané povinné osoby, zavedených organizačních, technických opatřeních, atd.

**K § 3**

Toto ustanovení na úrovni prováděcího právního předpisu navazuje na povinnost stanovení rozsahu danou § X *[Stanovení rozsahu řízení kybernetické bezpečnosti poskytovatelem regulované služby]* zákona a tím pádem také propojuje obsah vyhlášky s tímto

zákonným ustanovením. Správné stanovení rozsahu je zcela zásadní pro správnou aplikaci požadavků tohoto návrhu vyhlášky.

**K § 4 (Systém řízení bezpečnosti informací)**

Systém řízení bezpečnosti informací (nebo také „ISMS" z běžně užívaného anglického „Information Security Management System") je část systému řízení poskytovatele regulované služby, založená na přístupu k rizikům vztahujících se k regulované službě. Stanovuje způsob ustavení, zavádění, provozování, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací a dat, po vzoru normy ISO/IEC 27001.V rámci tohoto ustanovení jsou zmiňovány nejdůležitější požadavky, které jako celek tvoří jádro systému řízení bezpečnosti informací. Za předpokladu aplikace všech zmíněných požadavků dodrží povinná osoba základní princip tohoto systému – udržování bezpečnosti informací a její neustálé zlepšování. V porovnání s obsahem předchozí vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, je odst. 1 z hlediska obsažených povinností totožný, pouze vybrané povinnosti upřesňuje. Naopak zcela novým je odstavec 2 (viz odůvodnění níže).

Základem je stanovení cílů systému řízení bezpečnosti informací k zajištění bezpečnosti regulované služby. Tyto cíle odrážející základní směřování organizace by měly být stanoveny tak, aby bylo možné provádět jejich vyhodnocení. Na základě těchto cílů a bezpečnostních potřeb poskytovatel regulované služby v režimu vyšších povinností zavádí bezpečnostní opatření za účelem zajištění bezpečnosti regulované služby.

Dále je nutné řídit rizika vyplývající z rozsahu řízení kybernetické bezpečnosti stanoveného podle zákona o kybernetické bezpečnosti a zvolit vhodná bezpečnostní opatření. Na to navazují následující kroky: sledování a reakce na změny, řízení provozu a zdrojů systému řízení bezpečnosti informací, vytvoření a schválení bezpečnostních politik, zajištění pravidelného vyhodnocování účinnosti systému řízení bezpečnosti informací, včetně provádění auditu kybernetické bezpečnosti a následné zlepšování kybernetické bezpečnosti.

Aby bylo zajištěno kontinuální zlepšování, je kladen důraz na provádění pravidelného vyhodnocení účinnosti systému řízení bezpečnosti informací a provádění jeho aktualizace.

Za účelem stanovení hlavních zásad, práv a povinností toto ustanovení ukládá povinnost vytvořit a schválit bezpečnostní politiku a bezpečnostní dokumentaci systému řízení bezpečnosti informací. Schválení bezpečnostní politiky a bezpečnostní dokumentace zajišťuje mj. vymahatelnost jejího dodržování.

Dále toto ustanovení v odstavci 2 nově reaguje na v praxi bohužel doposud běžnou situaci, kdy povinná osoba z nějakého důvodu není schopna zavést řízení rizik podle odst. 1 písm. c) této vyhlášky. V takovém případě je nutné provést všechny činnosti uvedené v odst. 2. Tedy zavést všechna bezpečnostní opatření vyžadovaná touto vyhláškou v celém rozsahu. Tento závěr plyne z toho, že bez plnění povinnost řídit rizika nelze zjistit, která bezpečnostní opatření a v jakém rozsahu organizace musí zavést, aby dostatečně a efektivně zajistila kybernetickou bezpečnost regulované služby. Dále je nutné zpracovat prohlášení o aplikovatelnosti a plán zvládání rizik, ve kterých povinná osoba dokumentuje zavádění všech bezpečnostních opatření vč. rozplánování jejich zavádění.

**K § 5 (Povinnosti vrcholového vedení)**

Pro prosazování požadavků kybernetické bezpečnosti je klíčová podpora vrcholového vedení. Větší zapojení vrcholového vedení do řízení kybernetické bezpečnosti zdůrazňuje také směrnice NIS2. Proto je zcela na místě klást v tomto ustanovení důraz na vzdělávání vrcholového vedení v oblasti kybernetické bezpečnosti a na stvrzení vůdčí role a závazku

vrcholového vedení poskytovatele regulované služby k podpoře zajišťování systému řízení bezpečnosti informací, jakožto demonstrace vůle k podpoře zajišťování systému řízení bezpečnosti informací pro ostatní zainteresované strany (tedy pro bezpečnostní role, uživatele, další zaměstnance a dodavatele, kterých se problematika kybernetické bezpečnosti dotýká), a na cyklus přezkoumání systému řízení bezpečnosti informací. Z toho vyplývá, že jsou zde rozvedeny povinnosti pro vrcholové vedení ve vztahu ke kybernetické bezpečnosti, definovány bezpečnostní role a výbor pro řízení kybernetické bezpečnosti (dále také jen „výbor"), které mají být zřízeny. Většina těchto povinností byla stanovena již v dosavadní vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti a to v rámci § 6 Organizační bezpečnost.

Nově je ustanovením odst. 1 výslovně uvedeno, že je povinností vrcholového vedení účastnit se prokazatelně školení v oblasti kybernetické bezpečnosti, zajistit stanovení politik a cílů, zajistit dostupnost zdrojů a plnit další povinnosti neodmyslitelně spjaté s řádnou schopností vykonávat v zajištění kybernetické bezpečnosti svou roli a plnit péči řádného hospodáře, S tím souvisí také povinnost uvedená v odst. 2 seznamovat se s obsahem klíčových dokumentů, které jsou se zajišťováním kybernetické bezpečnosti v organizaci spojeny.

Nedílným požadavkem v této oblasti je dále aby povinná osoba prostřednictvím vrcholového vedení po osobách zastávajících bezpečnostní role a role administrátorů požadovala zajištění bezpečnosti informací. Tedy například, aby relevantní směrnice, popřípadě organizační řády a smlouvy s těmito osobami obsahovaly ustanovení o bezpečnosti informací (dohody o zachování důvěrnosti nebo mlčenlivosti).

Zapojení a účast vrcholového vedení do testování plánů kontinuity činností, plánů obnovy a procesů spojených se zvládáním kybernetických bezpečnostních incidentů vyjadřuje demonstraci podpory vedení v rámci systému řízení bezpečnosti informací. Hlavním důvodem jeho zapojení do testování těchto plánů je účast všech zainteresovaných stran tak, aby byla zajištěna úplná simulace průběhu krizové situace a její řešení aktivací plánů zpracovaných ke zvládání těchto situací. V rámci těchto testů je nutné testovat také rozhodovací schopnosti, je tedy potřebné do testů zapojit osoby mající potřebné pravomoci. Navíc v případě, že dojde k incidentu a je nutné plány aktivovat, musí být proces zvládnut i na pozici vrcholového vedení. Proces by měl být zautomatizovaný a všichni musí vědět, jaký je jejich úkol.

Požadavek na ustanovení výboru pro řízení kybernetické bezpečnosti je ve vyhlášce z toho důvodu, aby byla v rámci povinného subjektu ustanovena organizovaná skupina osob, která se zabývá celkovým řízením a rozvojem systému řízení bezpečnosti informací. Tato skupina musí být složena alespoň z jednoho zástupce vrcholového vedení, který by měl zajistit provázanost problematiky kybernetické bezpečnosti na vrcholové vedení a tím docílit zajištění podpory celému systému řízení bezpečnosti informací. V rámci odst. 4 je nově stanovena povinnost konání jednání výboru pro řízení kybernetické bezpečnosti v pravidelném intervalu a povinnost vést průběhu výboru dokumentovaný záznam. Tímto je výslovně stanovena doposud prakticky opomíjená povinnost, která v některých organizacích vedla k tomu, že byl význam výboru pro řízení kybernetické bezpečnosti snižován a jeho závěry nebyly dokumentovány. Manažer kybernetické bezpečnosti musí být součástí výboru z toho důvodu, že je rolí odpovědnou za tento systém a měl by úzce komunikovat nejen s lidmi, kteří se zabývají kybernetickou bezpečností, provozem systémů, ale i s vrcholovým vedením (kvůli jeho rozhodovací pravomoci v organizaci).

Důležitým požadavkem je zajištění zastupitelnosti bezpečnostních rolí. Tento požadavek byl do vyhlášky vložen na základě poznatků z provádění kontrol dodržování zákona. Požadavek reaguje na situace, kdy osoby zajišťující pro povinné subjekty výkon těchto rolí nemají adekvátní zástup. To může mít mimo jiné vliv i na zajištění kontinuity některých činností. Pro zajištění zastupitelnosti je možné rozložení povinností a kompetencí mezi více

osob. V případě zastupitelnosti (osobami jinými, než které byly určeny jako bezpečnostní role) se přirozeně požadavky na odbornou způsobilost a praxi, které jsou stanovené pro bezpečnostní role v následujícím ustanovení, použijí přiměřeně.

**K § 6 Bezpečností role**

Toto ustanovení úzce souvisí s předchozím ustanovením vyhlášky a popisuje jednotlivé bezpečnostní role. Znění tohoto ustanovení je shodné se zněním ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti.

Bezpečnostní role manažera kybernetické bezpečnosti je role odpovědná za systém řízení bezpečnosti informací v rozsahu stanoveném podle zákona o kybernetické bezpečnosti. Manažer kybernetické bezpečnosti tedy odpovídá za systém řízení bezpečnosti informací pouze v tomto poskytovatelem regulované služby stanoveném rozsahu. Tato role je zcela klíčová pro správné nastavení fungování systému řízení bezpečnosti informací. Pro tuto činnost proto musí prokázat odbornou způsobilost a praxi. V případě, kdy osoba, která má vykonávat tuto bezpečnostní roli, nesplňuje požadovanou délku praxe, lze praxi z části nahradit úspěšně ukončeným vysokoškolským vzděláním. Délka praxe je stanovena na dobu tří let z důvodu, že se jedná o dostatečně dlouhou dobu, za kterou je možné získat dostatek zkušeností pro výkon zmíněné role. V případě úspěšného ukončení vysokoškolského studia lze zkrátit dobu praxe na jeden rok vzhledem k tomu, že zkušenosti a teoretické dovednosti jsou získávány během studia vysoké školy. Tyto požadavky jsou v tomto návrhu vyhlášky mimo jiné proto, že osoby zastávající roli manažera kybernetické bezpečnosti mají odpovědnost za zabezpečení regulované služby, důležité pro chod státu nebo pro jeho obyvatelstvo, a splnění alespoň výše popsaných nároků je nezbytné. Manažer kybernetické bezpečnosti má dále povinnost informovat vrcholové vedení o činnostech, vyplývajících z výkonu role, tedy zejména o stavu systému řízení bezpečnosti informací. Jedná se o požadavek, který má vést k usnadnění prosazování konceptu systému řízení bezpečnosti informací a vede k dobré informovanosti a zainteresovanosti vrcholového vedení do celé problematiky. Toto ustanovení si také klade za cíl usnadnit manažerovi kybernetické bezpečnosti prosazování jednotlivých kroků, vedoucích ke zvýšení bezpečnosti podle systému řízení bezpečnosti informací. Vzhledem k náplni práce je role manažera kybernetické bezpečnosti neslučitelná s výkonem role, která je odpovědná za provoz regulované služby. Požadavek vychází z dobré praxe i z poznatků získaných během provedených kontrol u povinných subjektů. Organizační zařazení osoby zastávající roli manažera kybernetické bezpečnosti je ponecháno na uvážení povinného subjektu. V praxi bývá někdy problém, pokud manažer kybernetické bezpečnosti zároveň zastává některé výkonné funkce (např. vedoucí ICT oddělení). V těchto případech zpravidla nemůže nebo nechce prosazovat všechny aspekty systému řízení informační bezpečnosti v celém jeho rozsahu (tj. všechny aspekty manažerského systému) a ve schváleném rozsahu (tj. napříč organizací podle stanovené politiky systému řízení bezpečnosti informací) z důvodu střetu zájmů.

Architekt kybernetické bezpečnosti je bezpečnostní rolí zajišťující návrh a implementaci bezpečnostních opatření tak, aby byla zajištěna bezpečná architektura pro regulovanou službu. V praxi je architekt kybernetické bezpečnosti odpovědný za návrh bezpečnostní architektury, od komunikační infrastruktury, až například po bezpečnost na aplikační úrovni. Rovněž odpovídá za následnou implementaci navržených bezpečnostních opatření. Pro tuto činnost musí prokázat odbornou způsobilost a praxi, přičemž požadavky jsou stejné jako u manažera

kybernetické bezpečnosti. Tři roky odpovídají času, za který lze tyto zkušenosti získat. Obdobně lze v případě úspěšného ukončení vysokoškolského studia zkrátit dobu praxe na jeden rok. Varianta, kdy má organizace výkon role architekta kybernetické bezpečnosti rozdělen mezi více osob, při zohlednění jejich zaměření a vzhledem k v organizaci využívaným technologiím, je přípustná. Vzhledem k úzké specializaci a náplni práce architekta kybernetické bezpečnosti tato role nesmí vykonávat role, které jsou odpovědné za provoz regulované služby, a to ze stejných důvodů jako manažer kybernetické bezpečnosti.

Auditor kybernetické bezpečnosti je role odpovědná za provádění auditu kybernetické bezpečnosti. K požadavkům na praxi je přistupováno obdobně jako u role manažera a architekta kybernetické bezpečnosti. Klíčovou podmínkou je, že auditor kybernetické bezpečnosti vykonává svoji roli nestranně a výkon jeho role musí být zároveň neslučitelný s výkonem rolí manažera kybernetické bezpečnosti, architekta kybernetické bezpečnosti i garanta aktiv. Tento požadavek vychází z podstaty role auditora, který musí být nestranný (vůči předmětu auditu) a jehož hlavní náplní je hodnocení míry souladu systému řízení bezpečnosti informací a realizovaných bezpečnostních opatření s definovanými požadavky vyhlášky, stanovenými bezpečnostními politikami, vhodnými bezpečnostními standardy a s poskytováním nezávislé zpětné vazby o účelnosti a účinnosti systému řízení bezpečnosti informací a bezpečnostních opatření.

Garant aktiva je bezpečnostní role, která je pověřená organizací k zajištění rozvoje, použití a bezpečnosti aktiva. Má za úkol zajistit důvěrnost, dostupnost a integritu aktiv. V normách řady ISO/IEC 27000 se setkáme s pojmem vlastník aktiva, v praxi se jedná o tutéž roli. V tomto případě, však pojem vlastník neznamená, že by role měla k aktivu vlastnická práva.

V příloze tohoto návrhu vyhlášky jsou dále uvedena doporučení, která vychází z dobré praxe, ze zkušeností odborné veřejnosti a Úřadu.

Pokud je v rámci poskytovatele regulované služby zákonem regulováno více služeb, je logické, že není zapotřebí jmenovat do jednotlivých rolí pro každý systém rozdílné osoby (jedna bezpečnostní role může být odpovědná za více systémů).

**K § 7 (Řízení bezpečnostní politiky a bezpečnostní dokumentace)**

Základem tohoto ustanovení je požadavek na stanovení bezpečnostní politiky a vedení bezpečnostní dokumentace, která obsahově pokryje oblasti upravované touto vyhláškou. Toto ustanovení je dále rozvedeno přílohou č. 5 k této vyhlášce, která obsahuje výčet oblastí, které mají být v rámci bezpečnostní politiky a dokumentace po obsahové stránce pokryty. Jinými slovy z pohledu tohoto ustanovení a celé vyhlášky není kladen důraz na to, jak se který dokument jmenuje a v kolika dokumentech je celá problematika kybernetické bezpečnosti řešena, důležitá je obsahová úplnost a logické uspořádání s ohledem na organizační prostředí a zavedené zvyklosti v oblasti řídících dokumentů poskytovatele regulované služby.

Ustanovení definuje mimo jiné požadavky k zajištění bezpečnosti provozu regulované služby formou stanovení základních provozních pravidel a postupů v provozní dokumentaci. Tato pravidla by měla zohledňovat, resp. vycházet z bezpečnostní politiky a bezpečnostní dokumentace.

Ustanovení dále definuje i požadavky v oblasti řízení bezpečnostní politiky a bezpečnostní dokumentace. Řízení bezpečnostní politiky nebo bezpečnostní dokumentace znamená, že vznik, schválení, distribuce, kopírování, používání, přezkoumání, změny, archivace a likvidace těchto politik a dokumentů probíhá za podmínek specifikovaných odpovědnou osobou, která k tomu má oprávnění (obvykle vrcholové vedení nebo jiná

bezpečnostní role). Cílem je udržet politiku a dokumentaci aktuální, tedy odpovídající realitě a bezpečnostním požadavkům. Zároveň je zohledňováno, zda bezpečnostní politika a bezpečnostní dokumentace plní účel, za kterým byla vytvořena. Pravidelným přezkoumáním se rozumí interval, ve kterém dochází k pravidelnému posouzení a případné revizi. V souladu s požadavky nejlepší praxe by měl být nastaven na 1 rok. Přezkoumání a aktualizace bezpečnostních politik a bezpečnostní dokumentace má být prováděna také v souvislosti s řízením změn.

Tento paragraf kombinuje hlavně § 10 a § 30 vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, ale také např. zpřesňuje § 4 písm. d) této vyhlášky. Zmíněné dva paragrafy předchozí vyhlášky se věnovaly bezpečnostní politice a bezpečnostní dokumentaci, proto došlo k jejich spojení s cílem zvýšit přehlednost a seskupovat související povinnosti do jednoho paragrafu. Novou povinností je stanovit osobu odpovědnou za pravidelný přezkum a aktualizaci bezpečnostní politiky a bezpečnostní dokumentace. Povinnost přezkumu a stanovení odpovědností byla obsahem již předchozí vyhlášky, nyní je však povinnost mít stanovenou odpovědnou osobu uvedena explicitně.

**K § 8 (Řízení aktiv)**

Povinnost provést identifikaci primárních a podpůrných aktiv, vč. vazeb mezi nimi je uložena na úrovni zákona o kybernetické bezpečnosti. Tato vyhláška v ustanovení k řízení aktiv navazuje dalšími procesy, které na identifikaci aktiv dle zákona přímo navazují.

V rámci ustanovení o řízení aktiv došlo k sloučení požadavku odstavce 1 písmene a) a b) z původní vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti. Nejedná se tak o novou povinnost, došlo pouze k zpřehlednění, protože se v rámci požadavků obou písmen jednalo o vytvoření metodiky, která byla v praxi vytvářena jako jeden dokument. Pro větší návodnost došlo k dále k rozšíření přílohy č. 1 o aktivech a nově příloha pokrývá i oblast identifikaci aktiv

Do požadavků na řízení aktiv je také zařazena povinnost identifikovat a evidovat garanty aktiv (viz odůvodnění k předchozím ustanovením) či hodnotit aktiva. Hodnocení primárních aktiv je požadováno alespoň v rozsahu podle kritérií stanovených v příloze č. 1 tohoto návrhu vyhlášky. Evidence a hodnocení podpůrných aktiv je požadavek vyplývající zejména z potřeby vyhodnotit bezpečnostní rizika (především s ohledem na efektivní hodnocení hrozeb a zranitelností). Vzhledem ke složitosti regulovaných služeb a správnému hodnocení aktiv je nutné také znát jednotlivé závislosti mezi primárními a podpůrnými aktivy formou identifikace vzájemných vazeb.

Odstavec 2 původní vyhlášky obsahující výčet oblasti, které je třeba posoudit při hodnocení primárních aktiv, byl v rámci této vyhlášky přesunut do přílohy č. 1 a byl doplněn o příklady a vysvětlivky, s cílem zvýšení návodnosti. Nejedná se tedy o novou povinnost. Tento výčet oblastí není absolutní a povinná osoba by jej měla rozšířit podle svých potřeb a specifik. V seznamu jsou uvedeny nejdůležitější faktory, které by měly být posouzeny vždy, protože jsou významné z pohledu hodnocení aktiv. V případě, že je některý z faktorů nerelevantní, povinná osoba jej posoudí pouze v tom smyslu, že tento faktor v tomto konkrétním případě pro dané primární aktivum není relevantní.

Vzhledem k tomu, že jsou v praxi důležité i vazby mezi primárními a primárními a podpůrnými a podpůrnými aktivy (jsou používané víceúrovňové modely), rozšířilo se písmeno e) odstavce 1obecněji na to, že je potřeba evidovat pouze relevantní vazby mezi aktivy. Není tedy nutné identifikovat a evidovat úplně všechny vazby mezi všemi aktivy, ale pouze ty, které jsou významné z pohledu kybernetické bezpečnosti a promítají se do hodnocení aktiv a posléze rizik.

Nově došlo ke sloučení písmen h), i), j) v odstavci 1 původní vyhlášky do nově vytvořeného písmene g) odst. 1, které obsahuje pravidla pro ochranu aktiv. Nejedná se tedy o nový požadavek, všechny uvedené povinnosti byly v původní vyhlášce a ustanovení o řízení aktiv bylo seskupením souvisejících oblastí zpřehledněno.

Možné způsoby zacházení s aktivy je zapotřebí definovat přiměřeně k úrovni jednotlivých aktiv. Příkladem může být příloha č. 1 vyhlášky, která obsahuje možné způsoby ochrany aktiv, včetně odkazu na přílohu č. 4 vyhlášky o likvidaci dat a v neposlední řadě představuje příklad použití tzv. TLP („Traffic Light Protocol“)[1] pro sdílení informací. TLP:CLEAR, TLP:GREEN, TLP:AMBER, TLP:AMBER+STRICT a TLP:RED jsou znaky, určující ochranu předávaných informací podle metodiky TLP. TLP je systém ochrany předávaných informací, používaný zejména v rámci bezpečnostní komunity. Metodika TLP stanovuje určité příznaky, které jsou spojené s každou předávanou informací. Každý příznak pak stanovuje podmínky, jak lze danou informaci využít a jak s ní lze dále nakládat (tj. komu a za jakých podmínek ji lze dále předat). Příznak je vždy stanoven původcem informace, který má právo příznak také měnit (tzn. upravit podmínky dalšího sdílení informace).

**K § 9 (Řízení rizik)**

Jelikož tento návrh vyhlášky navazuje přímo na obsah dosavadní vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, a zaujímá stejně jako ona tzv. přístup orientovaný na rizika, je ustanovení tohoto paragrafu jedním z klíčových. Tento paragraf je úzce svázán také s ustanovením zákona o kybernetické bezpečnosti, které upravuje povinnost zavádět a provádět bezpečnostní opatření ve stanoveném rozsahu.

Požadavky na poskytovatele regulované služby v režimu vyšších povinností jsou stanoveny mj. v návaznosti a spojitosti s řízením aktiv a řízením změn. V rámci požadavku na stanovení metodiky pro hodnocení rizik je také zaveden požadavek na stanovení kritérií pro akceptovatelnost rizik, tedy takové úrovně rizika, která je po zvážení možných dopadů pro povinný subjekt přijatelná a oproti tomu i úroveň, která přijatelná není a pro kterou je nutné přijímat vhodná bezpečnostní opatření.

Minimální rozsah hodnocení rizik je uveden v příloze č. 2 tohoto návrhu vyhlášky. Obdobně je v příloze č. 3 tohoto návrhu vyhlášky uveden také výčet základních kategorií hrozeb a zranitelností, které musí být zváženy ve vazbě a s ohledem na jednotlivá aktiva identifikovaná v rámci řízení aktiv podle § 8.

V rámci tohoto ustanovení je deklarována možnost hodnotit rizika i jiným způsobem, než je způsob definovaný tímto návrhem vyhlášky, avšak za předpokladu, že tento jiný způsob zajistí stejnou nebo vyšší úroveň procesu řízení rizik. Tím je povinným subjektům dána možnost hodnotit rizika způsobem vyhovujícím konkrétnímu prostředí a jeho specifikům (např. používat vlastní rejstřík hrozeb a zranitelností či jiné stupnice pro hodnocení zranitelností, hrozeb a rizik). Pokud by pro poskytovatele regulované služby pro potřeby hodnocení rizik nebyly dostatečně návodné přílohy této vyhlášky, je možné využít podpůrný materiál Průvodce řízením aktiv a rizik publikovaný Úřadem na svých webových stránkách, zároveň také existuje celá řada standardů, které se touto problematikou zabývají.

Výsledky hodnocení rizik musí být obsahem zprávy o hodnocení rizik. Je samozřejmé, že celý proces řízení rizik by měl být formalizován, měl by být prokazatelný a opakovaně vykonatelný bez závislosti na konkrétní osobě, která hodnocení provádí.

[1] Blíže viz TRAFFIC LIGHT PROTOCOL (TLP) FIRST Standards Definitions and Usage Guidance — Version 1.0. Dostupné online na: https://www.first.org/tlp.

V návaznosti na výsledky hodnocení rizik má být dále, s ohledem na bezpečnostní potřeby poskytovatele regulované služby, sestaveno prohlášení o aplikovatelnosti. Jde o dokument (v tištěné či elektronické podobě), obsahující přehled zavedených a nezavedených bezpečnostních opatření podle tohoto návrhu vyhlášky, s popisem způsobu zavedení (pozn. možno řešit odkazem na plán zvládání rizik), případně s odůvodněním, proč některá bezpečnostní opatření zavedena nebyla. Cílem prohlášení o aplikovatelnosti je tedy popsat aktuální stav organizace ve vztahu k zákonu a vyhlášce. Dalším klíčovým dokumentem (v tištěné či elektronické podobě) vycházejícím z výsledků hodnocení rizik je plán zvládání rizik. Při jeho sestavování je potřeba vycházet nejen z hodnocení rizik, ale také z dalších souvisejících procesů, jako je např. audit kybernetické bezpečnosti, proběhlé kybernetické bezpečnostní incidenty, varování či reaktivní opatření vydané Úřadem, plánované významné změny apod. Cílem plánu zvládání rizik je zejména systematický přístup k zavádění bezpečnostních opatření, stanovení prioritizace při eliminaci rizik, stejně tak jako efektivní plánování finančních i lidských zdrojů potřebných pro zajištění kybernetické bezpečnosti.

Celkově došlo v tomto ustanovení pouze k dílčím úpravám textu s cílem zpřehlednění vyhlášky, např. písm. b) obsahuje navíc oproti předchozí vyhlášce „při identifikaci rizik“, aby bylo jednoznačné, že se jedná o název činnosti „s ohledem na aktiva identifikuje relevantní hrozby a zranitelnosti, přitom zvažuje zejména kategorie hrozeb a zranitelností ...“, která v předchozí vyhlášce nebyla pojmenovaná. Dalším příkladem může být rozdělení obsahu plánu zvládání rizik, který byl v předchozí vyhlášce popsán v rámci jednoho písmene, nicméně v rámci kontrolní činnosti bylo zjištěno, že plány zvládání rizik často neobsahují nějakou z vyjmenovaných oblastí, a proto byly tyto oblasti rozepsány do samostatných bodů pod písmenem g) odstavce 1 z důvodu zvýšení přehlednosti. Písmeno h) odstavce 1 bylo doplněno o další body, které musí být v rámci hodnocení rizik a plánu zvládání rizik brány v potaz. U předchozí vyhlášky nebyly body 5 až 7 explicitně uvedeny, přesto principy a fungování vyhlášky předpokládaly, že budou u těchto činností zohledněny a z důvodu zvýšení přehlednosti a uvědomění si vazeb s jinými bezpečnostními opatřeními byly doplněny. Jedinou nově vzniklou povinností je bod 7 upozornění na riziko spojené s dodavatelem, které je nově upraveno již v zákoně.

**K § 10 (Řízení dodavatelů)**

Vyhláška stanovuje základní bezpečnostní pravidla pro řízení dodavatelů a pro uzavírání dodavatelských smluv, která zohledňují požadavky systému řízení bezpečnosti informací. Cílem tohoto ustanovení je dosáhnout jasného vymezení odpovědností za plnění jednotlivých bezpečnostních opatření (nebo jejich dílčích částí) mezi dodavatelem a poskytovatelem regulované služby. V rámci tohoto ustanovení je opět kladen důraz na vlastní bezpečnostní potřeby poskytovatele regulované služby, jejichž vyhodnocení má být základním vstupem pro stanovení pravidel pro dodavatele, bezpečnostních opatření v rámci řízení dodavatelů, kontroly plnění stanovených bezpečnostních opatření a jejich případné vymáhání. Pro dosažení vyšší míry bezpečnosti aktiv regulované služby je potřebné řídit rizika související s danými dodavateli.

Ustanovení zakládá povinnost evidovat tzv. významné dodavatele, přičemž kritéria, na jejichž základě má být evidence provedena, jsou stanovena na základě vymezení pojmu významný dodavatel v zákoně o kybernetické bezpečnosti. Identifikace je tedy v kompetencích poskytovatele regulované služby, v jehož zájmu mají být významní dodavatelé evidováni. Vždy by však mezi významnými dodavateli měli být např. výrobci řídicích systémů, poskytovatelé služeb spojených se správou ICT atp.

V souvislosti s významnými dodavateli toto ustanovení definuje množinu přísnějších požadavků, mj. vymezuje povinnost přijetí ustanovení o bezpečnostních požadavcích do smluv

a dále povinnost pravidelného přezkumu plnění těchto povinností. Povinný subjekt by v těchto smluvních vztazích měl mít možnost kontroly plnění smluv a v neposlední řadě také právo tyto smluvní bezpečnostní požadavky upravovat tak, aby byly smluvní požadavky vyhovující a aby reflektovaly současné technologické možnosti a možnou úroveň zabezpečení. Ve smysluplných případech je možné povinnost kontroly dodavatelů přenést na třetí stranu (např. na nezávislého auditora).

Na ustanovení o řízení dodavatelů navazuje příloha č. 7 vyhlášky, která upřesňuje bezpečnostní opatření pro smluvní vztahy. Nově je doplněno ustanovení o povinnosti dodavatele informovat povinnou osobu o žádosti cizozemského orgánu o zpřístupnění nebo předání dat zpracovávaných na území cizího státu, vyjma situace, kdy by takové informování bylo v rozporu s právním řádem v jehož působnosti dochází ke zpracování dat nebo podle kterého byla žádost podána a dále ustanovení o zpřístupnění nebo předání dat na základě žádosti cizozemského orgánu o zpřístupnění nebo předání dat zpracovávaných na území cizího státu, až po provedení přezkoumání zákonnosti žádosti, po vynaložení úsilí o zabránění zpřístupnění nebo předání dat v rámci možností daných právním řádem, v jehož působnosti dochází ke zpracování dat nebo podle kterého byla žádost podána a pouze v nezbytném rozsahu.

Celkově došlo v této oblasti pouze k odstranění již dále nerelevantních požadavků, především v návaznosti na odstranění povinné osoby provozovatel ze zákona, a k drobným úpravám s cílem zpřehlednění textu.

**K § 11 (Bezpečnost lidských zdrojů)**

V oblasti kybernetické bezpečnosti je vyžadováno řízení bezpečnosti lidských zdrojů, což navazuje na § 5 a 6 tohoto návrhu vyhlášky a pojednává zejména o průběžném vzdělávání a udržování potřebné úrovně bezpečnostního povědomí. Důvodem pro toto ustanovení je zejména skutečnost, že velká část kybernetických bezpečnostních incidentů je způsobená vlivem nedostatečného bezpečnostního povědomí uživatelů obecně. Proto se zde cílí nejen na vrcholové vedení, bezpečnostní role a administrátory, ale i na zaměstnance a do určité míry i na jiné zainteresované strany (např. na významné dodavatele).

V této části regulace je kladen důraz na poučení vrcholového vedení o jeho povinnostech a o bezpečnostní politice, zejm. v oblasti systému řízení bezpečnosti informací a řízení rizik. Tento požadavek je stanoven proto, aby bylo vrcholové vedení uvedeno do problematiky systému řízení bezpečnosti informací a bylo se schopno na něm aktivně podílet např. při zpracování analýzy dopadů či rozhodování. Důvodem pro přidání tohoto požadavku je kladení důrazu na problematiku v rámci směrnice NIS2, nicméně vrcholové vedení by vždy mělo být minimálně v pozici uživatelů a povinnost školit uživatele byla stanovena již předchozí vyhláškou, nejedná se tedy o plně novou povinnost.

Touto regulací je dále vyžadováno poučení uživatelů, administrátorů, bezpečnostních rolí a dodavatelů o povinnostech a o bezpečnostní politice v souvislosti s regulovanou službou. To by mělo odpovídat povaze a rozsahu přístupu, který budou mít k aktivům regulované služby. Toto poučení by z důvodu vymahatelnosti mělo být prokazatelné.

Dále je požadováno například školení uživatelů, administrátorů a osob zastávající bezpečnostní role v oblasti kybernetické bezpečnosti. Školení by mělo odpovídat cílové skupině (mělo by být zohledněno, zda se jedná např. jen o uživatele, nebo o bezpečnostní role), zároveň musí být v souladu s plánem rozvoje bezpečnostního povědomí. Způsob provádění školení, ani cyklus pro jeho opakování není touto vyhláškou upraven. Měl by být přizpůsoben potřebám poskytovatele regulované služby a zároveň by měl vyplývat z odlišných potřeb jednotlivých skupin uživatelů, administrátorů a osob zastávajících bezpečnostní role. Důležitým parametrem je efektivita takového školení.

Plán rozvoje bezpečnostního povědomí zde hraje roli nástroje pro plánování výše uvedených školení a poučení zaměstnanců a zainteresovaných stran. Z toho důvodu musí být udržován v aktuálním stavu a musí být pravidelně vyhodnocován. Plán musí být optimalizován tak, aby odrážel aktuální potřeby poskytovatele regulované služby.

Součástí oblasti bezpečnosti lidských zdrojů je i řízení životního cyklu zaměstnance (nástup do pracovního poměru, případná změna pracovního zařazení, ukončení pracovního poměru), kontrola dodržování bezpečnostní politiky a stanovení bezpečnostních pravidel a postupů pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role (např. disciplinární řízení).

Úřad si uvědomuje, že informovaný a proškolený uživatel je jedním z nejefektivnějších způsobů, jak eliminovat z pohledu kybernetické bezpečnosti rizikové chování uživatele, které může mít negativní dopad na celou organizaci. Proto byla vytvořena nová příloha č. 8, na kterou odkazuje odst. 2 písm. e) obsahující doporučená témata pro rozvoj bezpečnostního povědomí reflektující nejzásadnější rizikové oblasti.

Zajištěním všech výše zmíněných oblastí by mělo být docíleno dostatečného bezpečnostního povědomí uživatelů a potřebné úrovně znalostí administrátorů a bezpečnostních rolí za účelem minimalizace počtu případných kybernetických bezpečnostních incidentů vzniklých interně.

**K § 12 (Řízení změn)**

Řízení změn je z hlediska fungování bezpečnosti a především kontinuity činností jedním z klíčových procesů. Ustanovení v této oblasti vychází z nejlepší praxe, ze zkušeností Úřadu a vymezuje základní požadavek na řízení změn a s tím spojené přezkoumání možných dopadů pro všechny změny. Na základě tohoto přezkoumání musejí být identifikovány tzv. významné změny (viz vymezení pojmů v § 2 tohoto návrhu vyhlášky), pro které jsou definována další bezpečnostní opatření zaměřená na konkrétní kroky řízení změn. Cílem je, aby byly identifikovány změny, které mají nebo mohou mít vliv na kybernetickou bezpečnost a aby na ně byla soustředěna větší pozornost. Zda se v případě dílčí změny, která má nebo může mít vliv na kybernetickou bezpečnost jedná o významnou změnu, či nikoliv, posuzuje sám poskytovatel regulované služby na základě pravidel, postupů a kritérií, které si sám stanoví.

V rámci přístupu k významným změnám pak musí být provedeno hodnocení rizik souvisejících s významnou změnou a na základě výsledků hodnocení rizik přijata opatření minimalizující možné negativní dopady změn. Na základě potřeb je rovněž nutné aktualizovat relevantní bezpečnostní politiky a bezpečnostní dokumentaci. Samozřejmostí je i testování významných změn a zajištění, že v případě potřeby bude možné jednotlivé změny navrátit do původního stavu.

Povinná osoba dále na základě hodnocení rizik musí rozhodnout o potřebě a případně o rozsahu penetračních testů, které by měly být zaměřeny především na aktiva dotčená významnou změnou. Penetrační testy jsou prováděny mj. v souladu s § 25 této vyhlášky.

Při kontrolní činnosti Úřadu byla tato oblast identifikována jako problematická, a proto došlo k úpravám ustanovení, které by měly tuto oblast zpřehlednit. Zejména se jedná o přeformulování odst. 1. Tento odstavec je nyní pro poskytovatele regulované služby návodnější a popisuje nastavení procesu řízení změn. Požadavek je postaven na tom, že si povinná osoba stanoví a zformalizuje proces řízení změn. Oblast řízení změn je omezena pouze na změny, které mohou mít vliv na kybernetickou bezpečnost a nezahrnuje všechny změny v organizaci, např. provozního charakteru. V praxi je řízení změn, tzv. „change management“ často postaven na mezinárodně uznávané knihovně ITIL, podle kterého je žádoucí řídit všechny změny, nicméně z důvodu snížení zatížení povinných osob jsou v této vyhlášce zdůrazněny pouze ty

změny, které se týkají oblasti kybernetické bezpečnosti. Povinná osoba by tedy měla stanovit proces identifikace všech změn, které mají nebo mohou mít vliv na kybernetickou bezpečnost. Zároveň musí mít povinná osoba pravidla, postupy a kritéria pro určení významných změn. Významné změny jsou pak určovány z těch, které byly identifikovány v prvním kroku a rozhodnutí je provedeno na základě výše zmíněných pravidel, postupů a kritérií. Povinnosti spojené s významnými změnami zůstaly zachovány.

**K § 13 (Akvizice, vývoj a údržba)**

V oblasti rozvoje a vývoje aktiv regulované služby je nutné, aby rozvoj systémů, které spadají do regulace zákonem, byl podpořen jasnými požadavky na zajištění jejich bezpečnosti, jako nedílné součásti rozvojových aktivit. Následně, po definování bezpečnostních požadavků, je nezbytné jejich promítnutí do celého životního cyklu od vlastního vývoje až do provozního využití daného systému nebo jeho části. Jedná se o prosazování principů nejlepší praxe „secure by design“ a „secure by default“. Součástí těchto požadavků je provedení hodnocení rizik z důvodu nalezení možných negativních dopadů a navržení případných bezpečnostních opatření ke zmírnění těchto dopadů. Je-li předmětem akvizice, vývoje a údržby významná změna, pak je nutné provést bezpečnostní testování před jejich nasazením.

Z pohledu akvizice, vývoje a údržby je dále nutné dbát na náležité oddělení prostředí, ve kterých budou relevantní aktiva umístěna, a to v celém jejich životním cyklu, jelikož náležité oddělení zejména technických aktiv je základním bezpečnostním opatřením plynoucích z principů „secure by desing“ a „zero trust“.

V neposlední řadě je v tomto ustanovení zohledněn požadavek vůči potenciálním akvizicím a vývoji technických aktiv, kdy je kladen důraz na vícefaktorovou autentizaci a oproti předchozímu znění Vyhlášky 82/2018 Sb. explicitně i na aktuálnost kryptografických algoritmů. Tyto požadavky jsou zde uvedeny na základě potřeby a důrazu na zavádění vícefaktorové autentizace, která je aktuálně jedním z hlavních bezpečnostních opatření, které je prokazatelně účinné proti hrozbě zneužití kompromitovaných autentizačních údajů. Požadavek na reflektování aktuálních požadavků v oblasti kryptografických algoritmů je v tomto ustanovení nově uveden i v tomto paragrafu na základě dlouhodobé udržitelnosti pořizovaných technických aktiv, kdy je potřeba zohlednit i budoucí potřeby rozvoje v této oblasti a např. zvyšování technické náročnosti na dané technické aktivum (například v případě potřeby delších kryptografických klíčů). Je tedy na místě, zohledňovat v projektech akvizice a vývoje to, aby byly vyžadovány kryptografické algoritmy, které NÚKIB doporučuje jakožto odolné a bezpečné do budoucna, a aby naopak již nebyla pořizována technická aktiva užívající dosluhující kryptografické algoritmy. Tato technická bezpečnostní opatření jsou dále více dotčena v jejich dílčích ustanoveních.

Oproti předchozímu znění Vyhlášky 82/2018 Sb. byl upřesněn požadavek písm. c) na stanovení bezpečnostních požadavků tak, aby bylo zřejmé, že se jedná o požadavky v souladu s touto vyhláškou a vlastními bezpečnostními potřebami organizace. Dále byl doplněn požadavek na oddělení prostředí jako jsou provozní a zálohovací, či jiná specifická prostředí, která nově vyhláška dále zmiňuje, např. v § 19, § 27 a požadavek na aktuálnost kryptografických algoritmů v rámci nových projektů akvizice a vývoje podle § 26.

**K § 14 (Řízení přístupu)**

Za účelem řízení přístupu k aktivům a jednoznačnému určení vykonavatele operace, je požadavkem této regulace správa životního cyklu identit a přístupových oprávnění uživatelů, administrátorů, aplikací a zařízení.

V souladu s nejlepšími praktikami (ISO/IEC 27002) musí být přístupová práva a oprávnění uživatelům a administrátorům přistupujícím k technickým aktivům přidělována

pouze v rozsahu nezbytném pro výkon činností vyplývajících z popisu pracovního místa či smluvního ujednání. Důležité je z tohoto pravidla neudělovat neopodstatněné výjimky. Nezbytná je i pravidelná kontrola přidělených identit a přístupových oprávnění a odebírání nebo změna přístupových oprávnění při změně pracovní pozice nebo zařazení uživatelů, administrátorů nebo osob zastávajících bezpečnostní role. Stejný požadavek je i v případě ukončení nebo změny smluvního vztahu. Důvodem je ochrana aktiv před jejich kompromitací a zneužitím.

Poskytovatel regulované služby musí pro řízení přístupu k aktivům všem uživatelům přidělit jedinečné identifikátory z důvodu jednoznačného stanovení vykonavatele události. Jedinou výjimku z tohoto pravidla mohou tvořit tzv. sdílené technické účty. Jejich použití by však mělo podléhat přísnému nastavení interních pravidel a být možné jen ve zcela výjimečných situacích.

V rámci této oblasti došlo pouze k drobným textovým úpravám z důvodu zvýšení přehlednosti. Nově byly doplněny časové intervaly na „bezodkladně“ pro odebírání nebo změnu přístupových oprávnění při změně pozice nebo zařazení na základě skupin a rolí a při ukončení nebo změně smluvního vztahu.

**K § 15 (Zvládání kybernetických bezpečnostních událostí a incidentů)**

Základním požadavkem v rámci tohoto ustanovení je zavedení procesu zajišťujícího detekci a vyhodnocování kybernetických bezpečnostních událostí a zvládání kybernetických bezpečnostních incidentů.

Jedním z požadavků na poskytovatele regulované služby je přidělení odpovědností a stanovení postupů pro průběžnou detekci a průběžné vyhodnocování kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů. Rovněž přidělení odpovědností a stanovení postupů pro koordinaci a zvládání kybernetických bezpečnostních incidentů. Důvodem pro tato bezpečnostní opatření jsou zejména negativní poznatky z výkonu kontrol dodržování zákona u poskytovatelů regulované služby. V rámci těchto kontrol bylo v mnoha případech zjištěno, že jsou tyto činnosti prováděny ojediněle či vůbec. To má významný negativní vliv na bezpečnost, konkrétně na včasné odhalení incidentu a případně i na jeho vyšetřování.

V této oblasti došlo s novelou ke změnám v zákoně, nicméně povinnosti dle vyhlášky zůstávají stejné. Došlo pouze k drobným textovým úpravám z důvodu zvýšení přehlednosti.

**K § 16 (Řízení kontinuity činností)**

Toto opatření cílí na schopnost organizace rychle a účinně reagovat na situace související s nepříznivými vlivy, které nemůže povinná osoba ovlivnit (např. přírodní katastrofy) nebo kybernetické bezpečnostní incidenty. V případě nepřipravenosti na takové situace by hrozilo úplné nebo částečné přerušení poskytování regulované služby na nepřijatelně dlouhou dobu. Základem řízení kontinuity činností je vypracovaná politika řízení kontinuity činností, která nastavuje základní procesy, práva a povinnosti. K písmenu d) stanoví politiku řízení kontinuity činností, která obsahuje naplnění cílů bylo připojeno písmeno a) z původní vyhlášky stanoví práva a povinnosti administrátorů a osob zastávajících bezpečnostní role. Ke spojení došlo z toho důvodu, že práva a povinnosti jsou definovány v politice. Původní rozdělení, kdy písmena ani nenásledovala po sobě bylo nepřehledné.

Metodika pro provedení analýzy dopadů byla v původní vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti součástí politiky řízení kontinuity činností (bod 1.23. písm. d) příloha č. 5 původní vyhlášky). Vytvořením samostatného písmena v § 15 tak došlo pouze k zpřehlednění, nikoliv k vytvoření nové povinnosti.

U písm. b) došlo k dílčím úpravám textu a doplnění odkazu na ustanovení o řízení rizik, který v původní vyhlášce nebyl. Opět se tedy jedná o úpravu textu, která vede ke zvýšení přehlednosti a návodnosti tohoto požadavku, nikoliv k vytvoření nové povinnosti.

Provedení analýzy dopadů je podkladem pro stanovení cílů řízení kontinuity činností ve smyslu stanovení doby obnovy chodu (dále jen „RTO" z anglického „Recovery Time Objective"), minimální úrovně poskytovaných služeb a bodu obnovy dat (dále jen "RPO" z anglického „Recovery Point Objective").

RTO je čas, za který má být orgán nebo osoba schopna obnovit produkty, služby, aktivity a zdroje do předem definované minimální úrovně po kybernetickém bezpečnostním incidentu nebo po selhání. Zdroji jsou myšlena zejména data, která je nutné obnovit pro poskytování služeb. Konkrétně je zde myšleno, za jak dlouho bude orgán nebo osoba schopna obnovit potřebná data. Rozsah dat, která je nutné obnovit, bude definováno v RPO. RPO tedy vyjadřuje, do jakého bodu v minulosti lze obnovit data. Jinými slovy RPO vymezí množství historických dat, o které může povinná osoba přijít.

K naplnění cílů a politiky řízení kontinuity činností je písmeně e) stanovena povinnost vypracovat plány kontinuity činností a plány obnovy. Zmíněné plány je nutné aktualizovat a pravidelně testovat, aby byly v případě situace, která vyžaduje jejich aktivaci, využitelné.

V původní vyhlášce byly používané pojmy plány kontinuity činností a havarijní plány. Věcně a /obsahově zůstávají plány stejné, došlo pouze k jejich přejmenování , a to z toho důvodu, že havarijní plány byly zaměňovány s havarijními plány dle jiné legislativy platné v ČR (např. havarijní plány Hasičského záchranného sboru České republiky, havarijní plány dle zákona č. 224/2015 Sb., zákona č. 239/2015 Sb., vyhlášky č. 422/2016 Sb., vyhláška 450/20058 Sb., atd.). Rovněž došlo ke sjednocení terminologie směrem k běžné praxi v oblasti informačních technologií, kde se standardně používá pojem plány obnovy. Také došlo k rozšíření přílohy o bezpečnostní politice a bezpečnostní dokumentaci, kde jsou nově plány kontinuity činností a plány obnovy popsány a současně byl upraven i obsah politiky řízení kontinuity činností. Těmito úpravami nevznikají žádné nové povinnosti, jen došlo k upřesnění a zpřehlednění.

**K § 17 (Audit kybernetické bezpečnosti)**

V rámci požadavků v oblasti auditu kybernetické bezpečnosti je zahrnuto provádění pravidelné kontroly dodržování bezpečnostních politik, bezpečnostních opatření, smluvních závazků a všech požadavků vyplývajících z této vyhlášky. V případě nalezených nedostatků musí být určena nápravná opatření pro zajištění souladu. Tento požadavek je ve vyhlášce uveden z toho důvodu, aby byl systém řízení bezpečnosti informací plně funkční a byl zde dodržen princip zlepšování, který vychází z norem řady ISO/IEC 27000.

Z hlediska posuzování souladu je vyžadováno, aby poskytovatel regulované služby identifikoval veškerou relevantní regulaci z hlediska kybernetické bezpečnosti a zajistil kontrolu jejího dodržování v praxi.

Požadavek na přezkoumání technické shody cílí na kontrolu zavedených technických bezpečnostních opatření. V praxi to znamená, že auditor provede kontrolu technických bezpečnostních opatření, v jejímž rámci sleduje, zda je vycházeno z potřeb stanovených na základě hodnocení rizik zaznamenaných v prohlášení o aplikovatelnosti a zda jsou tato technická opatření adekvátně nastavena. V případě, kdy byla předešlým auditem stanovena nápravná opatření, je požadováno, aby bylo přezkoumáno, zda byla adekvátně zavedena.

Nově je ve vyhlášce obsažen požadavek odstavce 1 na stanovení plánu provádění auditu kybernetické bezpečnosti. V praxi jsou plány pro provádění auditu kybernetické bezpečnosti

běžně používány z toho důvodu, aby mohla organizace lépe plánovat svoji činnost v průběhu roku.

Dále došlo ke zpřehlednění povinností souvisejících s auditem kybernetické bezpečnosti. Tyto povinnosti jsou v předchozí vyhlášce o kybernetické bezpečnosti popsány v odstavci 1 a nově se stejným povinnostem věnuje odstavec 2 a 3 této vyhlášky. Cílem odstavce 2 je důraz na posouzení souladu se zákonem a vyhláškou v písm. a), nicméně věcně se povinnosti shodují s předchozím zněním vyhlášky o kybernetické bezpečnosti a nové povinnosti nepřibyly. Cílem odstavce 3 je zpřehlednit, kde by výsledky auditu kybernetické bezpečnosti měly být zohledněny, toto bylo rovněž zakotveno i v předchozí vyhlášce. Nově je v tomto odstavci zmíněno prohlášení o aplikovatelnosti. Povinnost zohlednit výsledky auditu kybernetické bezpečnosti vyplývala z principu fungování vyhlášky o kybernetické bezpečnosti, nejedná se tedy o novou povinnost, pouze o snahu o zpřehlednění a upozornění na další souvislosti. Odstavec 4 rovněž nedefinuje žádnou novou povinnost. Jedním z důvodu pro provádění auditu kybernetické bezpečnosti je neustálé zlepšování úrovně kybernetické bezpečnosti a nápravná opatření jsou nezbytnou součástí. Vzhledem k tomu, že nápravná opatření nutně nemusí být součástí auditu kybernetické bezpečnosti nebyla v předchozí vyhlášce explicitně zmíněna. Opět bylo z důvodu přehlednosti při novelizaci přistoupeno k tomu, že byla tato povinnost jednoznačně uvedena.

Audit kybernetické bezpečnosti by musí být proveden dle požadavku odstavce 5 písmena a) při významných změnách, v rámci jejich rozsahu. To znamená, že by jeho předmětem měly být významné změny a oblasti, které jsou těmito změnami přímo dotčeny. Dále by měl být audit kybernetické bezpečnosti prováděn v souladu s plánem auditu kybernetické bezpečnosti v pravidelných intervalech alespoň jednou za dva roky v celém rozsahu požadavků, které vyplývají z této vyhlášky. Tento požadavek vyplývá nutnosti vyhodnocovat funkčnost celého systému řízení bezpečnosti informací. Dále je cílem zajistit, aby v případě nalezených nedostatků byly tyto nedostatky co nejdříve odstraněny.

V případech, kdy audit kybernetické bezpečnosti nelze provést v plném rozsahu ve stanovené lhůtě (zejm. z důvodu časové náročnosti), je možné audit rozdělit systematicky na dílčí části. Takovýto postup je nutné zdůvodnit a postupovat tak, aby vždy po ukončení všech částí auditu, byl výsledkem audit kybernetické bezpečnosti v celém rozsahu požadavků tohoto návrhu vyhlášky, nejpozději v 5letém intervalu.

Z ustanovení o auditu kybernetické bezpečnosti byly odstraněny povinnosti, které jsou po novele již nerelevantní.

**K § 18 (Fyzická bezpečnost)**

V rámci tohoto ustanovení musí povinné subjekty nastavit postupy a pravidla, kterými bude všeobecně chránit aktiva a kontinuitu regulovaných služeb. Pro tyto účely stanoví fyzický bezpečnostní perimetr nebo perimetry (někdy označovány jako zóny) a jejich úrovně fyzické ochrany, v jejichž rámci musí být tato pravidla prosazována a dodržována, užije relevantní prostředky fyzické bezpečnosti a zavede adekvátní bezpečnostní opatření, kterými zajistí fyzickou bezpečnost. Takto určené bezpečnostní perimetry a jejich úrovně fyzické ochrany náležitě dokumentuje. Prostředky fyzické bezpečnosti se rozumí zejména mechanické zábranné prostředky, zařízení elektrické zabezpečovací signalizace, prostředky omezující působení požárů, prostředky omezující působení projevů živelních událostí či systémy pro kontrolu a evidenci vstupu. Součástí fyzické bezpečnosti je zvážení všech bezpečnostních aspektů jednotlivých lokalit, ve kterých je regulovaná služba provozována. Je klíčové si uvědomit, že k zajišťování bezpečnosti je nutné přistupovat komplexně, a že bez dostatečného fyzického zabezpečení aktiv povinného subjektu může být mnohdy zbytečné investovat do zabezpečení např. na aplikační úrovni modelu ISO/OSI.

**K § 19 (Bezpečnost komunikačních sítí)**

Se zajištěním kybernetické bezpečnosti aktiv úzce souvisí zabezpečení komunikační sítě, která je tvořena technickými aktivy regulované služby podle vyhlášky a využívá se zejména k provozování regulované služby a práci s ní. Tato oblast je upravena na základě standardů v oblasti síťových komunikací a nejlepších praktik (např. ISO/IEC 27002).

Zajištění segmentace komunikační sítě znamená její rozdělení do jednotlivých síťových segmentů např. na základě důvěryhodnosti (např. segment s veřejným přístupem, segment s koncovými stanicemi, segment se servery), organizačních jednotek (např. segment ekonomického oddělení, personálního oddělení, marketingového oddělení) nebo jejich vhodné kombinace. Dále je nutné prostřednictvím segmentace od sebe oddělit jednotlivá prostředí komunikační sítě (např. prostředí provozní, zálohovací, vývojové a testovací). Toto oddělení prostředí může být provedeno fyzicky (např. na úrovni metalických nebo optických kabelů) nebo logicky na vyšších úrovních modelu ISO/OSI (např. na síťové, transportní nebo aplikační vrstvě). Způsob provedení segmentace je v gesci povinného subjektu, který zajistí, aby komunikace byla adekvátně řízena mezi jednotlivými segmenty v rámci interní komunikační sítě nebo jejím perimetru (potažmo externí komunikační sítí), současně také i mezi jednotlivými prostředími

Vzdálený přístup (např. VPN připojení do interní komunikační sítě) a vzdálená správa technických aktiv (např. prostřednictvím vzdálené plochy nebo terminálového připojení na serveru) musí být také náležitě řízena a omezena na pouze nezbytně nutnou míru. Tento princip „povolení pouze nezbytně nutné komunikace“ pro řádné zajištění regulované služby a omezení či zakázání neřízené komunikace je best-practice v oblasti bezpečnosti komunikačních sítí a ověřenou cestou pro dosažení základní úrovně síťové bezpečnosti a slouží tak ke zvýšení úrovně kybernetické bezpečnosti u povinné osoby, jelikož dochází k omezení případného šíření nebezpečného kódu nebo případného útočníka v interní komunikační síti v případě její kompromitace.

Oproti původnímu znění bylo z tohoto paragrafu vypuštěn požadavek na aktivní blokování nežádoucí komunikace, jelikož je tento požadavek již zahrnut v § 22 odst. 1 písm. c) tohoto návrhu vyhlášky.

Kryptografickými algoritmy k zajištění důvěrnosti a integrity, jsou myšleny především různé zabezpečené protokoly nebo šifrování síťové komunikace (např. aktuální verze protokolu TLS a v nich používané kryptografické algoritmy jako AES). Nástrojem pro zajištění ochrany integrity komunikační sítě je myšlen nástroj využívající např. mechanismus na bázi protokolu 802.1x, který povoluje připojení ke komunikační síti nebo jejímu jednotlivému segmentu pouze autentizovaným technickým aktivům, kdy tento nástroj zabraňuje připojení ke komunikační síti neznámým aktivům a zabraňuje tak například připojení potenciálního útočníka.

**K § 20 (Správa a ověřování identit)**

Tyto požadavky stanovují minimální úroveň pro správu a ověření identit, které by měly povinné subjekty prosazovat. Tento paragraf vychází zejm. ze standardu NIST SP 800-63B.

U nástroje pro ověření identity (uživatelů, administrátorů a technických aktiv) je mimo jiné stanoven i požadavek na odolnost ukládaných autentizačních údajů, přičemž tento požadavek míří mimo jiné i na tzv. odolnost proti off-line útokům, jak byl tento požadavek stanoven v předchozím znění Vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti. Pojmem off-line útok je myšlen útok, při kterém útočník odcizí databázi hesel a následně má možnost s touto databází manipulovat např. ve svém zařízení (obecně v jiném prostředí). V případě, kdy k tomuto odcizení dojde a databáze hesel není dostatečně zabezpečena (např. pomocí aktuálně odolných šifrovacích nebo hašovacích funkcí), pak se útočník rovnou dostane ke konkrétním

heslům k jednotlivým účtům. Proto je ve vyhlášce uveden požadavek, aby byly zajištěna odolnost ukládaných autentizačních údajů, tedy aby tyto údaje byly zašifrovány dostatečně silnou šifrou. Útočník, i když odcizí tuto databázi hesel, se dostane pouze k zašifrovaným údajům (zde je samozřejmě nutné zvolit odolnou kryptografii). Tento požadavek významným způsobem zvyšuje zabezpečení autentizačních údajů.

Z pohledu bezpečnosti lze v ustanovení shledat tři úrovně nastavení správy a ověřování identit. V první řadě je ve vyhlášce zakotveno úsilí směřující k využívání autentizačního mechanismu, který není založený jen na použití identifikátoru účtu a hesla, ale na vícefaktorové autentizaci s nejméně dvěma různými typy faktorů. Různými typy autentizačních faktorů je myšleno ověření identity na základě něčeho, co daná entita zná, čím je nebo co má. Tento způsob je z pohledu kybernetické bezpečnosti v současné době nejvhodnější a používání pouze jednoho autentizačního faktoru v podobě hesla se v porovnání nepovažuje za bezpečné např. z pohledu možné kompromitace nebo úniku hesel. V případě dvou faktorů funguje tak, že daná entita, která se autentizuje vůči technickým aktivům, musí znát např. PIN nebo heslo a dále musí pro úspěšnou autentizaci mít k dispozici i druhý faktor, např. token. Z pohledu finanční náročnosti a procesu zavedení vícefaktorové autentizace u technických aktiv, která jsou již v provozu a jsou např. i nějakým způsobem v tomto ohledu omezena, je však pořízení a implementace tohoto způsobu autentizace náročnější.

Jelikož zavádění autentizačních mechanismů na bázi vícefaktorové autentizace je stěžejním bezpečnostním opatřením v oblasti správy a ověřování identit, má povinná osoba nově povinnost vést evidenci technických aktiv, účtů a autentizačních mechanismů, které nesplňují tento bezpečnostní požadavek, a to včetně odůvodnění. Tento požadavek utváří v rámci povinné osoby ucelený přehled o tom, kde ještě je potřeba zavést vícefaktorovou autentizaci, případně kde je třeba zavést jiná bezpečností opatření, která zaručí obdobnou nebo vyšší úroveň zabezpečení.

V případě, kdy není možné výše uvedený požadavek na vícefaktorovou autentizaci splnit, například z důvodu velikosti organizace nebo specifičnosti technických aktiv, a není možné zavést vícefaktorovou autentizaci, musí nástroj pro ověřování identity uživatelů, administrátorů a aplikací využívat alespoň autentizaci pomocí kryptografických klíčů. Z hlediska bezpečnosti jde také o přípustný způsob autentizace. Může se jednat například o autentizaci pomocí SSH klíče.

Dále jsou v případě, kdy není možné použít z určitého důvodu ani autentizaci pomocí kryptografických klíčů, ve vyhlášce stanovena pravidla, která je nutné vynucovat v případě autentizace za pomocí pouze identifikátoru účtu (např. přihlašovacího jména) a hesla. Tento způsob z bezpečnostního hlediska není ideální, protože je ve velké míře závislý na samotných uživatelích, kteří jej vytváří a nakládají s ním. Proto jsou stanoveny požadavky, které je nutné dodržet. Jde zejm. o minimální délku hesla, skladbu hesla, pravidla pro tvorbu a životnost hesel atp. Minimální délka hesla byla pro uživatele zvolena na 12 znaků z toho důvodu, že při výpočetním výkonu (1,5 Th/s) a typu hashe NTLM (NT Lan Manager, který je dnes běžně využívaný) s délkou hesla 8 znaků a využití komplexity, bude trvat prolomení tohoto hashe cca 12 minut. V případě, kdy bude zvoleno heslo tvořené např. frází o délce 12 a více znaků, se čas na prolomení hashe prodlužuje na vyšší úroveň. Stále však platí doporučení, že při jakémkoliv podezření na kompromitaci hesla je nutné toto heslo bezodkladně změnit.

K těmto příkladům je však nutné uvést ještě několik poznámek. Výpočetní výkon 1,5Th/s je možné získat při investici nižší než 1 mil. Kč. Dalším aspektem, kterým je nutné se zabývat, je také Mooreův zákon, který tvrdí, že „Každý rok dojde ke zdvojnásobení počtu tranzistorů na čipu.“ To znamená, že každých deset let stoupne výkon počítačů přibližně tisícinásobně a z toho plyne, že se doba prolomení hashe bude i nadále zkracovat. Tato varianta výpočtu taktéž

nepočítá s tím, že by útočník využil slovník, který může také výrazně snížit dobu prolomení hashe. Vzhledem k faktům popsaným výše je u administrátorů nastaven požadavek na délku hesla na 17 znaků a pro účty technických aktiv na 22 znaků, což při dodržení komplexity odpovídá entropii na úrovni zhruba 128 bitů. Za účelem zvýšení komplexity hesel a tím i ztížení využití slovníkových útoků by měl mít uživatel při tvorbě hesla možnost vybírat nejen malá a velká písmena, číslice, ale i běžné speciální znaky. Ze standardu NIST je současně odvozen požadavek na možnost uživatelům nebo administrátorům v nástroji zadat heslo také alespoň o délce 64 znaků.

Uživatelům a administrátorům by dále měla být umožněna změna hesla, přičemž by však mělo být technicky zajištěno, aby tuto změnu nešlo provádět opakovaně v příliš krátkém časovém intervalu. Tento interval je stanoven na 30 minut, avšak povinná osoba si může na základě výstupů systému řízení bezpečnosti informací a bezpečnostních potřeb tento interval přizpůsobit. Cílem je zamezit případům, kdy uživatel opakovaně mění heslo během krátkého časového intervalu (např. během jediného dne), čímž se může snažit vrátit ke svému původnímu heslu. S tímto požadavkem je provázán požadavek na znemožnění použití dříve používaných hesel s pamětí alespoň 12 předchozích hesel. Nastavení by mělo být tedy takové, že čím je počet možných změn hesla větší, tím by měl být počet hesel, které budou „uloženy v paměti“ větší. Další požadované pravidlo je, aby uživatelům a administrátorům nebylo umožněno zvolit si nejčastěji používaná hesla. Tento požadavek je ve vyhlášce z toho důvodu, aby se předešlo používání hesel, které jsou zveřejněny ve slovnících často používaných hesel (mezi těmito hesly jsou např. „admin“, „heslo1234“, „123456“, „123123“, „P@$$w0rd“ atp.).

Další část tohoto ustanovení se věnuje výchozím heslům uživatelů a heslům pro obnovu jejich přístupu. Změna výchozích hesel je důležitá k zajištění důvěrnosti používaných hesel, jelikož existují zdroje, ze kterých lze zjistit např. výchozí hesla některých technických aktiv. To znamená, že je nutné změnit veškerá výchozí hesla, ať se jedná o uživatelské účty či výchozí účty ke správě nově zakoupených technických aktiv. Požadavek na zneplatnění hesla pro zřízení přístupu nebo jeho obnovu po jeho prvním použití nebo po uplynutí 24 hodin je zde z toho důvodu, aby heslo nebylo zneužitelné např. pokud by se útočník dostal k e-mailu, ve kterém je toto heslo uvedeno.

V neposlední řadě se toto ustanovení věnuje zabezpečení administrátorských účtu určených zejména pro případ obnovy po kybernetickém bezpečnostním incidentu, tedy např. účtu recovery, superadmin nebo root. Tyto účty by měly být používány pouze pro velmi omezený rozsah činností a nemělo by s nimi být za jiných okolností nadbytečně manipulováno. Od povahy těchto účtu se odvíjí i bezpečnostní požadavky tohoto usnesení na ně kladené, kdy je vyžadována bezodkladná změna jejich hesla, jeho komplexita, délka 22 znaků, jeho bezpečné uložení, omezení užití tohoto účtu, změna jeho hesla v určitém intervalu a evidence manipulace nebo pokusů o manipulaci s tímto účtem nebo jeho heslem.

**K § 21 (Řízení přístupových oprávnění)**

Pro řízení přístupových oprávnění je vymezen požadavek na zajištění řízení oprávnění pro přístup k jednotlivým aktivům a pro čtení dat, zápis dat a změnu oprávnění, zejména s cílem omezení oprávnění u osob bez potřebného need-to-know nebo pracovnímu zařazení. Toto řízení musí být prováděno pomocí centralizovaného nástroje s ohledem na vazby mezi aktivy, kdy tímto požadavkem je mířeno na možnost, kdy v rámci povinné osoby bude např. provozováno více systematických celků technických aktiv, které tvoří pomyslný „informační systém“ dle předchozího zákona č. 181/2014 Sb., o kybernetické bezpečnosti, a dává logický smysl mít centralizovaná technická aktiva centralizována s ohledem na daný „informační systém“, nikoliv na celou organizaci povinné osoby. V takovém případě je ovšem nutné odůvodnění pro volbu takového řešení. Pokud by např. byly v rámci regulované služby některé komunikační sítě

tvořeny technickými aktivy a jejich programovými prostředky a vybaveními fyzicky odděleny od jiných komunikačních sítí bude pro řízení oprávnění použito více těchto nástrojů. Řízení těchto oprávnění by mělo být dále zajištěno v maximální možné míře pomocí rolí a uživatelských skupin.

Centralizovaný nástroj je požadován pro zajištění bezpečnějšího provozu především v návaznosti na potřebu snadného řízení změn přístupových oprávnění (např. při přidělení, při změně pracovní pozice nebo jeho odebrání) a jejich promítání do všech dílčích částí regulované služby a dále pro udržování jednotného nastavení napříč všemi technickými aktivy s ohledem na vazby mezi aktivy. Řízení oprávnění musí být jedním z kontrolních bodů v rámci řízení změn (zejména změn souvisejících s personálním obsazením bezpečnostních rolí a pozic administrátorů, ale také běžných uživatelů).

**K § 22 (Detekce kybernetických bezpečnostních událostí)**

V rámci tohoto ustanovení je oproti původnímu znění vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, nově spojen paragraf ochrany před škodlivým kódem s paragrafem detekce kybernetických bezpečnostních událostí. Jedná se o změnu, která byla provedena s ohledem na obecné zvýšení maturity v oblasti kybernetické bezpečnosti v České republice a postupně se zvyšujícími hrozbami v kyberprostoru. Jelikož spolu byly tyto dva paragrafy úzce spjaty v rámci plnění požadavků technických bezpečnostních opatření, tak rozvoj nových nástrojů, které zajišťují ochranu a plnění těchto požadavků vedl přirozeně ke sloučení těchto paragrafů do jednoho. Stále je tedy požadováno nasazení nástrojů, které jsou schopny detekovat kybernetické bezpečnostní události, které mohou vést ke kybernetickým bezpečnostním incidentům a tyto události buď detekovat, nebo jim současně mohou účinně čelit. Z hlediska kategorizace je možné využít tyto prostředky na úrovni komunikační sítě či nasazené v rámci technických aktiv, které již nejsou uvedeny demonstrativním výčtem, jak tomu bylo v předchozích znění vyhlášky 82/2018 Sb. Od demonstrativního výčtu bylo v tomto znění vyhlášky upuštěno, jelikož je aktuální znění postaveno na posouzení povinné osoby, kdy je třeba rozhodnout, která technická aktiva jsou z pohledu kybernetické bezpečnosti a detekce kybernetických bezpečnostních události relevantní. Podobně, z hlediska funkcionality, je možné rozlišit fungování těchto nástrojů na ty, které provádí pasivní detekci událostí, bez aktivního ovlivňování komunikace, kdy na druhé straně jsou prostředky, které rovnou provádí zásahy podle stanovených pravidel, a tím aktivně brání rozvoji kybernetické bezpečnostní události nebo incidentu a snaží se tak minimalizovat případné dopady.

Vyhláška v tomto ustanovení definuje požadavek na nástroje, které budou splňovat minimálně vyhláškou stanovené parametry. Jedním z takových parametrů je schopnost ověření a kontroly dat přenášených v rámci komunikační sítě a mezi sítěmi, a to včetně perimetru interní komunikační sítě – tedy schopnost kontrolovat příchozí a odchozí provoz, případně blokovat nežádoucí komunikaci.

Pro zajištění vyšší úrovně zabezpečení si povinný subjekt musí určit relevantní technická aktiva, v jejichž rámci lze zajistit detekci kybernetických bezpečnostních událostí, včetně ochrany před škodlivým kódem, jako například u koncových stanic, mobilních zařízení (především notebooků), serverů, aktivních síťových prvků (například routerů či switchů) a všech dalších obdobných technických aktiv. Detekce kybernetických bezpečnostních událostí má být zajištěna nástrojem, který je s ohledem na vazby mezi aktivy centrálně spravován, kdy „s ohledem na vazby mezi aktivy“ je myšleno to stejné, jako u odůvodnění pro § 21 tohoto návrhu vyhlášky.

Ochrana před škodlivým kódem je důležitou součástí dnešních nástrojů pro detekci kybernetických bezpečnostních událostí také vzhledem k faktu, že množství škodlivého kódu neustále narůstá a je stále sofistikovanější. Je proto vyžadováno, aby povinné subjekty za

účelem ochrany před škodlivým kódem používaly vhodné nástroje pro detekci kybernetických bezpečnostních událostí, které zajišťují nepřetržitou automatickou ochranu a aby tyto nástroje a jejich detekční pravidla byly pravidelně aktualizovány. Oproti předchozímu znění vyhlášky 82/2018 Sb. je nově uveden požadavek na tyto nástroje zajišťující detekci v podobě vlastnosti umožňující sledování chování technického aktiva, uživatelů, aplikací a procesu, jelikož se tyto nástroje neustále rozvíjí a aktuální detekční mechanismy na těchto principech fungují. Do této kategorie patří nástroje pro detekci škodlivého kódu,skenery zranitelností, antivirové programy, EDR, XDR, nástroje pro detekci/prevenci průniku (IDS/IPS), nástroje pro síťovou analýzu, nástroje pro detekci anomálií, behaviorální analýzu atp. Nasazení konkrétního nástroje a způsob jeho implementace na daném technickém aktivu by vždy měly vycházet z výsledků analýzy rizik a z bezpečnostních potřeb organizace.

**K § 23 (Zaznamenávání bezpečnostních a relevantních provozních událostí)**

Povinná osoba si musí určit na základě hodnocení aktiv a bezpečnostních požadavků, určit rozsah technických aktiv, která jsou relevantní z pohledu zaznamenávání událostí, a také jaké bezpečnostní a relevantní provozní události budou u nich zaznamenávány. Návrh vyhlášky v tomto směru předepisuje minimální rozsah pořizovaných záznamů o událostech, a to jak z pohledu samotných událostí, které je nutné zaznamenat (např. činnosti vyžadující privilegovaná oprávnění, kritická chybová hlášení atd.), tak i s ohledem na to, jaké podrobnosti musí být zaznamenány (např. datum a čas, typ činnosti, identifikace účtů a původců atp.).

Požadavek na zaznamenávání provozních událostí je zde uveden z důvodu, že provozní událost může být například při vyhodnocování nebo vyšetřování útoku důležitá. A neobvyklé provozní události jsou indiciemi toho, že se technické aktivum nechová standardním způsobem. Provozní událostí je např. docházející místo na uložišti disku. Bezpečnostní událost je událost přímo spojená s bezpečností informací. Může to být například zašifrování pevného disku. Určení rozsahu technických aktiv, u kterých bude zaznamenávání prováděno, je zde uvedeno z důvodu, že není nutné bezpečnostní a provozní události sledovat na všech technických aktivech, protože by to organizaci neadekvátně zatížilo, ale pouze na těch technických aktivech, která jsou pro pořizování záznamů vyhodnocena jako relevantní na základě hodnocení aktiv a bezpečnostních požadavků. Cílem tohoto ustanovení tedy není zaznamenávat všechny bezpečnostní a provozní události ze všech technických aktiv, ale na základě posouzení určit, u kterých technických aktiv budou jaké události zaznamenávány, jelikož je neekonomické, nepřehledné a neuchopitelné z pohledu provozu i bezpečnosti zaznamenávat vše (případně i vyhodnocovat). Takto určený rozsah technických aktiv a zaznamenávaných událostí je ovšem potřeba udržovat náležitě aktuální, proto je zde požadavek na jeho aktualizaci v povinném intervalu a při významných změnách (jako např. při pořízení nového technického aktiva, ze kterého by mohly být významné právě záznamy o bezpečnostních událostech).

Novým požadavkem v této oblasti je, že zaznamenávání bezpečnostních a relevantních provozních událostí má zajišťovat jednoznačnou síťovou identifikaci původce, je-li v komunikační síti použit nástroj, který mění jeho síťovou identifikaci. Požadavek cílí na skutečnost, aby použité bezpečnostní nástroje zcela nepřepisovaly identifikátory původců (např. IP adresy), ale aby je zachovávaly. To zejména z důvodů správného vyhodnocování událostí i pro případy vyšetřování incidentů. Příkladem je předcházení situacím jako např. použití nástroje typu “web application firewall” (neboli WAF), který je nasazen před webový server. Přičemž logy na webovém serveru poukazují, že veškeré dotazy přicházejí z IP adresy WAF, IP adresa skutečného původce dotazu, např. pomocí HTTP metod POST nebo GET, je v tomto případě zahazována.

Všechny takto zaznamenané události je nutné po určitou dobu uchovávat (některé kybernetické bezpečnostní incidenty jsou detekovány až v korelaci určitých událostí v čase).

U poskytovatelů regulované služby v režimu vyšších povinností je doba uchovávání záznamů nastavena na 18 měsíců. Důvod, proč je doba pro ostatní systémy nastavena takto, je zejména zkušenost Úřadu a také skutečnost, že střední doba detekce incidentu v regionu EMEA (Europe Middle East And Africa) je 24 měsíců. To znamená, že v případě, kdy dojde ke kybernetickému bezpečnostnímu incidentu, trvá organizaci 24 měsíců, než zjistí, že se u ní vůbec incident stal. Při vyšetřování takového incidentu je pak zcela klíčové, zda jsou tyto záznamy k dispozici či nikoliv. Hodnotou 18 měsíců tedy zvyšujeme šanci na zajištění potřebných důkazů k případnému šetření a analyzování incidentů. Stanovené období, po které mají být logy uchovávány, se ale vztahuje pouze na logy týkající se bezpečnosti informací, tedy logy související s důvěrností, dostupností a integritou informací (zpravidla bezpečnostní logy). Opět je potřeba zdůraznit, že účelem tohoto ustanovení není povinnost uchovávat všechny logy ze všech technických aktiv po dobu 18 měsíců. V rámci povinné osoby by mělo dojít mimo určení rozsahu technických aktiv a jejich bezpečnostních a relevantních provozních událostí i k posouzení toho, jaké logy budou po jakou dobu uchovávány, zejména vzhledem k např. vlastním zdrojům pro vyhodnocování kybernetických bezpečnostních událostí, přičemž 18 měsíců je ovšem výchozí hodnota, která když bude nastavena jinak, vyžaduje řádné odůvodnění na základě výstupů systému řízení bezpečnosti informací a bezpečnostní potřeb povinné osoby.

Novým požadavkem v oblasti zaznamenávání událostí oproti předchozímu znění této vyhlášky je povinnost používat centrální nástroj (s ohledem na vazbu mezi aktivy, viz odůvodnění k § 21) pro uchovávání záznamů (například nástroj pro správu logů), který by měl zajišťovat i plnění předchozích požadavků jako zajištění důvěrnosti, integrity a dostupnosti ukládaných záznamů. V žádném případě není cílem této vyhlášky stav, ve kterém bude tento nástroj pro centrální uchovávání záznamů absentovat a všechny záznamy budou uchovávány v rámci nástroje pro vyhodnocování kybernetických bezpečnostních událostí (např. SIEM), kdy účinnost a ekonomičnost tohoto nástroje je naopak snížena při zahlcení nadměrným množstvím záznamů.

**K § 24 (Vyhodnocení kybernetických bezpečnostních událostí)**

Toto ustanovení cílí na to, aby povinné subjekty disponovaly nástroji umožňujícími provádět kontinuální a centralizované vyhodnocování kybernetických bezpečnostních událostí z bezpečnostních a relevantních provozních záznamů. Mezi těmito daty se následně vyhledávají korelace, vyhodnocuje se relevance zdrojů a v reálném čase se vytváří varování, ať už automatizované nebo na základě manuálního posouzení bezpečnostního analytika, který s nástrojem pracuje. V případě, že je tento nástroj správně nasazen, nakonfigurován a zároveň obsluhován kvalifikovaným personálem, mělo by být dosaženo včasné detekce a rychlé reakce na kybernetické bezpečnostní události a incidenty, a to včetně včasného varování určených bezpečnostních rolí. Současně jsou získávány automatické statistiky o infrastruktuře, takže je zefektivněna i její správa a celkový stav systému řízení bezpečnosti informací.

Pro efektivní fungování nástroje je nutným předpokladem, že je pravidelně obsluhován osobou (nebo osobami), která má pokročilé znalosti v oblasti síťové analýzy. Tato osoba by měla dohlédnout i na aktuálnost nakonfigurovaných pravidel tohoto nástroje pro lepší nastavení ostatních zavedených bezpečnostních opatření a vyhodnocování jednotlivých záznamů a korelací, aby nedocházelo k zahlcení tohoto nástroje nebo jeho neefektivnosti z důvodu např. nadměrného množství automatizovaného nesprávného vyhodnocení tzv. „false positive“.

Oproti předchozímu znění tohoto bezpečnostního opatření ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, nedošlo ke zásadním změnám, pouze byly reflektovány změny ve zněních ostatních ustanovení a zpřehledněna jeho struktura.

**K § 25 (Aplikační bezpečnost)**

Aplikační bezpečnost se nejvíce dotýká oblasti software, u kterého je nutné, aby v rámci technických aktiv byl podporován, ať už výrobcem, dodavatelem nebo jinou osobu (například komunitou v případě open source software). U nepodporovaného software není totiž možné zaručit jistou úroveň bezpečnosti formou vydávání bezpečnostních záplat a aktualizací. Z tohoto důvodu je novou povinností v rámci tohoto ustanovení oproti předchozímu znění ve vyhlášce 82/2018 Sb. vést v rámci povinné osoby evidenci technických aktiv, která již nejsou podporována, a zavádět bezpečnostní opatření, která tuto problematiku adresují (například prostřednictvím segmentace komunikační sítě, kdy jsou nepodporovaná technická aktiva ve vlastním segmentu, který není považován za zabezpečený).

Dále se toto ustanovení věnuje zavedení bezpečnostních opatření, která zajistí trvalou ochranu aplikací, informací a transakcí před neoprávněnou činností a popřením provedených činností. Neoprávněná činnost může být například kompromitace, což může být případ, kdy mezi interní komunikaci dvou osob vstupuje třetí, která tuto komunikaci kompromituje. Součástí neoprávněných činností je i neautorizovaná změna. Jako příklad neautorizované změny je možné uvést změnu vykonanou osobou, která měla přístup na server, ale provedla činnost, na kterou neměla oprávnění (změnila nastavení serveru). Požadavek nasazovat opatření proti popření provedených činností, zjednodušeně řečeno, vychází z potřeby zajištění tzv. nepopiratelnosti. To znamená, že digitální stopa by měla být nepopiratelná (tedy taková, aby nešlo popřít, že dané zařízení, aplikace nebo daný uživatel provedl určitou činnost). Toto jsou dva důležité požadavky v rámci aplikační bezpečnosti, které je nutné dodržovat, aby byla zajištěna bezpečnost regulované služby.

Oproti předchozímu znění této vyhlášky je v tomto ustanovení uvedena povinnost provádět skenování zranitelností technických aktiv, a to z interní a externí komunikační sítě například formou veřejně dostupných nástrojů pro skenování zranitelností IP rozsahu vystavených vůči veřejnému internetu, kdy tyto nástroje mohou povinné osobě říct, jak jsou její technická aktiva zranitelná z pohledu externího útočníka (např. otevřené porty, zranitelné operační systémy a nezabezpečené vzdálené přístupy. U této povinnosti je stanoven požadavek na interval jednoho roku, který lze v odůvodněných případech rozdělit až do dvou let, ovšem v praxi je provádění skenování zranitelností finančně nenáročný proces realizovatelný pomocí veřejně dostupných nástrojů, tudíž je doporučeno tento interval snižovat a zavést skenování zranitelností jako součást běžných procesů.

Obdobně jako u skenování zranitelností, musí povinné subjekty na základě tohoto ustanovení provádět penetrační testování, avšak pouze u významných technických aktiv. Tyto penetrační testy provádí před jejich uvedením do provozu a v souvislosti s významnou změnou. Požadavek ve vyhlášce klade důraz na provedení penetračního testu především u významných technických aktiv, kdy významná technická aktiva jsou zde uvedena z toho důvodu, že není nutné provádět penetrační testy u všech aktiv (aplikací, systémů atd.), protože by to organizaci neadekvátně zatížilo, ale pouze u těch aktiv, které si organizace vyhodnotí jako důležitá na základě analýzy, obdobně jako u § 23. Penetrační testy je nutné provádět za účelem nalezení případných slabých míst (zranitelnosti) z pohledu bezpečnosti a tato slabá místa odstranit, aby nemohla být ohrožena bezpečnost regulované služby. Oproti předchozímu znění této vyhlášky musí povinné osoby provádět penetrační testování provádět v intervalu dvou let nebo je možné v odůvodněných případech (například vysoké komplexnosti prováděného testu) rozdělit toto testování do systematických celků a rozdělit je do rozsahu pěti let.

**K § 26 (Kryptografické algoritmy)**

Zabezpečení komunikace, bezpečnost technických aktiv a bezpečné používání nástrojů a mechanismů, které využívají kryptografii (např. komunikační protokoly), je podmíněno

volbou aktuálně odolných kryptografických algoritmů. Dále je nezbytné, aby povinné subjekty prosazovaly bezpečné nakládání s kryptografickými algoritmy, například stanovením pravidel a postupů pro užívání kryptografických algoritmů a působením na uživatele cestou školení v této oblasti. Toto ustanovení dále odkazuje povinné subjekty na doporučení v oblasti kryptografických algoritmů, např. dokument Minimální požadavky na kryptografické algoritmy, vydávaných Úřadem, který je zveřejňuje na jeho webových stránkách a řádné je dle vývoje v této oblasti na základě odborné výzkumné činnosti aktualizuje. Tato doporučení nejsou vzhledem k dynamickému vývoji této problematiky zahrnuta ve vyhlášce, ani jejích přílohách, právě z důvodu potřeby četnějších aktualizací a doplnění o relevantní informace.

Oproti předchozímu znění této vyhlášky musí v rámci tohoto ustanovení povinné osoby zajistit zabezpečení hlasové, audiovizuální, textové a nouzové komunikace. Toto ustanovení explicitně zahrnuje e-mailovou komunikaci, která je velice často využívána pro předávání informací nejen v rámci povinné osoby a její zabezpečení bývá opomíjeno, zejména pak zachování její důvěrnosti a integrity.

V případě, kdy povinná osoba využívá kryptografických klíčů nebo certifikátů, musí zajistit jejich potřebnou kvalitu, nezbytnou ochranu a správu těchto klíčů a certifikátů, kdy je v tomto usnesení uvedeno, jaké minimální parametry musí být zajištěny. Je tomuto tak z důvodu jejich praktické implementace a možné přezkoumatelnosti ze strany povinné osoby, kdy je cílem zajištění efektivnosti tohoto bezpečnostního opatření.

**K § 27 (Zajišťování dostupnosti regulované služby)**

Cílem tohoto ustanovení je zavedení nezbytných bezpečnostních opatření k zajištění dostupnosti regulované služby. Zde je nutné zmínit, že splnění požadavků tohoto ustanovení mnohdy začíná již samotným návrhem architektury komunikační sítě. Je také nezbytné, aby se povinná osoba zamyslela, jaké hrozby a zranitelnosti mohou dostupnost její regulované služby, a to včetně jednotlivých aktiv, ohrozit a současně dle potřeb organizace zavede bezpečnostní opatření, aby snížila jejich možný dopad na dostupnost této služby. Lze zde zařadit např. problematiku návrhů redundance jednotlivých technických aktiv (včetně jejich vhodného rozmístění) a síťové infrastruktury. Dále je možné použít clustery, virtualizace, zajistit dostupnost v případě výpadku elektrické energie pomocí záložního napájení (například UPS nebo diesel-agregát), ale také např. držení jistých skladových zásob technických aktiv či dostatečně smluvně ošetřeno dodání služeb souvisejících s dostupností u třetích stran (např. připojení k internetu) atp.

V neposlední řadě se toto ustanovení věnuje problematice zálohování, která v předchozím znění vyhlášky č. 82/2018 Sb. nebyla dostatečně dotčena, přestože představuje z pohledu zajištění dostupnosti regulované služby stěžejní téma, a to zejména vzhledem ke zvýšenému výskytu kybernetických bezpečnostních událostí a incidentů v České republice v posledních letech, které měly například za dopad zašifrování a tedy nepoužitelnost aktiv regulovaných služeb (ransomware). Povinná osoba tak musí vytvářet pravidelné zálohy svých technických aktiv pro účely případné obnovy po kybernetickém bezpečnostním incidentu. Současně musí zajistit oddělení zálohovacího prostředí v rámci komunikační sítě od ostatních prostředí, které je ze zkušenosti Úřadu jedním ze spolehlivých způsobů pro zajištění dlouhodobé dostupnosti (případně obnovení) regulované služby (například rozšíření ransomware v komunikační síti regulované služby). Toto ustanovení současně uvádí požadavky pro bezpečné nakládání s těmito zálohami a zabezpečení dat v nich obsažených, včetně jejich testování a dokumentování těchto testů.

**K § 28 (Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv)**

Navzdory tomu, že se technická opatření této vyhlášky již věnují okruhům, které slouží pro zajištění kybernetické bezpečnosti regulované služby, a to včetně kybernetické bezpečnosti jejich technických aktiv, slouží tento paragraf pro zdůraznění specifických potřeb nad rámec předchozích paragrafů, a to pro průmyslová, řídící nebo jiná obdobná specifická technická aktiva.

Název tohoto ustanovení byl změněn na základě zkušeností z prováděných kontrol Úřadu, kdy povinné subjekty disponovali technickými aktivy, která byla atypická od např. běžných koncových stanic a serverů, avšak nejednalo se přímo o průmyslová či řídící technická aktiva v běžném slova smyslu. Přestože tato technická aktiva s nimi sdílela obdobné vlastnosti, jako je např. zastaralost požadovaných operačních systémů, používání komunikačních protokolů (zpravidla nezabezpečených) specifických pro dané prostředí a závislost na dodavateli a jeho vzdálené správě daného technického aktiva, nebyla pro ně zavedena obdobná specifická bezpečnostní opatření jako například zvláštní segmentace sítě pro tato technická aktiva nebo vyšší bezpečnostní požadavky na zabezpečení vzdáleného připojení a správy. S těmito technickými aktivy nebylo nakládáno obdobně jako s průmyslovými a řídícími technickými aktivy, jelikož tak nebyly vnímány, přestože by to bylo z pohledu kybernetické bezpečnosti na místě.

S ohledem na význam těchto aktiv pro fungování regulované služby vyhláška v § 28 rozšiřuje již zmíněná bezpečnostní opatření z jiných paragrafů, která jsou využívána pro zajištění kybernetické bezpečnosti těchto specifických technických aktiv. V rámci těchto aktiv je předpokládáno zavádění všech technických bezpečnostních opatření z předchozích ustanovení vyhlášky, ovšem v tomto ustanovení jsou explicitně uvedena znovu. Při formulování těchto základních doplňujících požadavků byla také využita doporučení NIST („National Institut of Standard and Technology“ – Americký úřad pro standardizaci), mezinárodní normy, poznatky z mezinárodních jednání a nejlepší praxe z této oblasti.

**K § 29 (Lokalizace při zpracování dat v zahraničí)**

Určení dat a informací, na které se povinnosti jejich lokalizace uvedené v ustanovení tohoto paragrafu uplatní, je dáno stanoveným rozsahem, do kterého data a informace spadají, a dopadovými kritérii, které stanoví závažnost možného dopadu kybernetického bezpečnostního incidentu postihujícího tato data a informace.

Dopadová kritéria vychází především z Vodítka pro hodnocení dopadů vydaného Úřadem, přičemž pro stanovení dat a informací, na které se povinnost stanovená v tomto odstavci uplatní přibližně odpovídá úroveň kritická v hodnocení dopadů kybernetického bezpečnostní incidentu na důvěrnost, dostupnost a integritu dat a informací.

Proces vyhodnocení aplikace povinnosti lokalizace dat a informací je stanoven tak, že poskytovatel regulované služby v režimu vyšších povinností posoudí, jestli data a informace zpracovávané v rámci stanoveného rozsahu naplní alespoň jedno z dopadových kriterií stanovených v jednotlivých odstavcích. Pokud naplní dopadová kritéria uvedená v odst. 2, pak je třeba na tyto data a informace vzhledem k jejich kritičnosti uplatnit povinnost lokalizace pouze na území České republiky. Pokud ani jedno dopadové kritérium uvedené v odst. 2 nenaplní, posoudí naplnění dopadových kritérií podle odst. 4 a případně na ně uplatnit povinnosti lokalizace dat a informací na území členských států Evropské unie, Evropského sdružení volného obchodu, Organizace Severoatlantické smlouvy, Organizace pro ekonomickou spolupráci a rozvoj.

V souvislosti s hodnocením naplnění dopadových kritérií dle odst. 2 a 4 se očekává, že poskytovatel regulované služby provede na základě jemu dostupných informací úvahu nad možným naplněním jednotlivých kritérií a kvalifikovaný odhad ve vztahu k možnému naplnění

číselně vyjádřených hodnot (např. finanční ztráty). Výsledek této úvahy, resp. odhadu, je třeba dokumentovat. Poskytovatel regulované služby se vyjádří ke všem dílčím dopadovým kritériím, případně zhodnotí, která kritéria nejsou s ohledem na stanovený rozsah vůbec relevantní. Poskytovatel regulované služby by měl brát v úvahu nejhorší možné důsledky případného kybernetického bezpečnostního incidentu a nezohledňovat přitom již zavedená bezpečnostní opatření. Některá kritéria nejsou specifikována binárně nebo neobsahují jasnou hodnotu, může tak potenciálně docházet k částečně subjektivnímu hodnocení některých dopadových kritérií, resp. důležitosti zpracovávaných dat a informací. Je na poskytovateli regulovaných služeb, aby při hodnocení vzal v úvahu kontext vlastní organizace, veškeré relevantní okolnosti fungování regulovaných služeb a využívání zpracovávaných dat a informací a vzájemné závislosti a provázání jednotlivých technických aktiv.

Poskytovatel regulované služby může v rámci regulované služby, resp. stanoveného rozsahu, zpracovávat širokou škálu dat a informací k zajištění řádného fungování regulované služby. Různé kategorie dat přitom mohou mít různou úroveň citlivosti či významnosti s ohledem na jejich vlastní povahu a s ohledem na fungování regulované služby. S přihlédnutím k této skutečnosti je akceptovatelným postupem vyčlenění určité skupiny či množiny dat, v souvislosti se kterými nemůže dojít k naplnění dopadových kritérií dle odst. 2 nebo 4, a neuplatnění pravidel a podmínek lokalizace vůči takto vyčleněné množině dat. V takovém případě však musí poskytovatel regulované služby vzít důkladně v potaz vztah takto vyčleněné části informací a dat vůči regulované službě jako celku, obdobně jako je tomu např. při zařazování části informačního či komunikačního systému do bezpečnostní úrovně dle vyhlášky č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci.

Praktickým příkladem takové dekompozice, resp. vyčlenění množiny dat a neuplatnění pravidel lokalizace dle řešeného ustanovení vůči této množině, může být například ukládání čistě provozních dat, jako například logů či informací o nestabilním chování (*crash dump* souborů) či dat sloužících ke korelaci signálů z bezpečnostních senzorů mimo území členských států Evropské unie, Evropského sdružení volného obchodu, Organizace Severoatlantické smlouvy, Organizace pro ekonomickou spolupráci a rozvoj. To však pouze za předpokladu, že kybernetické bezpečnostní incident postihující tato data nemůže vést k naplnění dopadových kritérií podle odst. 2 a 4.

Rozdělením informací a dat na menší celky však nemůže redukovat jejich důležitost jako celku (resp. bagatelizovat dopady případného kybernetického bezpečnostního incidentu). Jestli by k naplnění dopadových kritérií došlo, pokud by byla všechna data jako celek uložena na jednom místě, nemůže jejich rozdělením na více částí dojít k úplnému neuplatnění pravidel lokalizace. Minimálně jedna z dílčích množin tvořících celek stále bude naplňovat dopadová kritéria a bude třeba uplatnit pravidla lokalizace dle řešeného ustanovení.

Pro výjimečné situace (např. hrozby konfliktu s cizími státy, válečný stav, přírodní katastrofa velkého rozsahu atp.), pro které by nebylo vhodné zcela zakázat využití záložních datových center v zahraničí (resp. na území členských států Evropské unie, Evropského sdružení volného obchodu, Organizace Severoatlantické smlouvy, Organizace pro ekonomickou spolupráci a rozvoj), poskytuje odst. 3 výjimku z povinnosti uvedené v odst. 2, přičemž tuto výjimku je možné aplikovat pouze při dodržení podmínky šifrování dat a informací podle § 26 této vyhlášky.

Omezení zpracování dat a informací podle tohoto paragrafu je odstupňováno podle kritičnosti dat podle postupu uvedeného v předchozích odstavcích, a to de facto do tří kategorií. Nejkritičtější data a informace by měly pro jejich potřebu ochranu z důvodu národní bezpečnosti zpracovávány pouze na území České republiky, tak aby rizika vyplývající z exportu

dat a informací mimo území České republiky byla mitigována v nejvyšší možné míře. Pro data a informace, u nichž by kybernetický bezpečnostní incident měl vysoký dopad, nikoliv však kritický, byl okruh států, na jejichž území mohou být tato data a informace zpracovávány omezen na státy s důvěryhodným právním prostředím. U dat a informací, u nichž dopad kybernetického bezpečnostního incidentu nedosáhne závažnosti předchozích dvou kategorií převáží práva na svobodu podnikání nad zájmem státu na zajištění národní bezpečnosti.

V souladu s Doporučením pro hodnocení důvěryhodnosti dodavatelů technologií do 5G sítí v České republice,[2] vydaným Úřadem spolu s Ministerstvem průmyslu a obchodu, Ministerstvem zahraničních věcí, Bezpečnostní informační službou, Úřadem pro zahraniční styky a informace a Vojenským zpravodajstvím, jakožto veřejnoprávními zástupci bezpečnostní komunity České republiky lze za státy s důvěryhodným právním prostředím považovat státy:

a. které mají demokraticky volenou vládu, což mj. zahrnuje existenci nezávislé opozice, svobodných voleb, na základě jejichž výsledku může být stávající vláda vyměněna, a fungující princip tzv. brzd a protivah,
b. které mají nezávislý soudní systém, jenž nepodléhá přímým politickým zásahům, jsou v něm dodržována závazná pravidla, zvyklosti a zásady právního státu, jako je právo na spravedlivý proces vč. ctění presumpce neviny, práva na veřejné projednání věci a práva být souzen bez zbytečného odkladu,
c. jejichž právní předpisy a veřejné politiky se řídí zásadami právního státu a jsou vydávány s ohledem na ně,
d. které dbají na ochranu duševního vlastnictví,
e. které dlouhodobě či systematicky neporušují mezinárodní právo a vůči nimž nebo vůči jejichž aktivitám se oficiálně nevymezují mezinárodní a nadnárodní organizace či aliance, kterých je Česká republika členem, a to např. v podobě rezoluce Rady bezpečnosti Organizace spojených národů či omezujícího opatření společné zahraniční a bezpečnostní politiky Evropské unie,
f. které udržují s Českou republikou partnerské vztahy a neprovádí činnosti, které jdou proti základním zájmům České republiky nebo jejích spojeneckých států,
g. které nepovažují Českou republiku za nepřátelský stát.

Členské státy Evropské unie, Evropského hospodářského prostoru, Organizace pro hospodářskou spolupráci a rozvoj či Severoatlantické aliance jsou skupinou států, které disponují důvěryhodným právním prostředím, rizika spojená s exportem dat mimo území České republiky jsou v těchto státech výrazně menší než ve státech, které do tohoto okruhu nespadají. Česká republika je zároveň členem všech těchto uskupení a jedná se tak o její spojenecké státy v různých oblastech od ekonomické a hospodářské spolupráce až po spolupráci vojenskou.

**K § 30 (Přechodné ustanovení)**

Smyslem přechodných ustanovení v tomto návrhu vyhlášky je v souladu s přechodnými ustanoveními zákona o kybernetické bezpečnosti zachovat dosavadní obsah vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti aplikovatelný na ty povinné osoby, které byly povinnými osobami již za účinnosti dosavadního zákona č. 181/2014 Sb., o kybernetické bezpečnosti, a to do doby, než těmto povinným osobám přejdou přechodné lhůty a bude se na ně vztahovat tento návrh vyhlášky.



[2] Dostupné zde: https://www.nukib.cz/cs/infoservis/doporuceni/1801-doporuceni-pro-hodnoceni-duveryhodnosti-dodavatelu-technologii-do-5g-siti-v-ceske-republice/

**K § 31 (Účinnost)**

Protože podstatnou část návrhu zákona, resp. z něj odvozeného návrhu této vyhlášky tvoří transpozice směrnice NIS2, je také stanovení účinnosti nové právní úpravy s požadavky této směrnice úzce spojeno. V souladu s obsahem čl. 41 odst. 1 jsou členské státy povinny přijmout a zveřejnit opatření nezbytná pro dosažení souladu s touto směrnicí do 17. října 2024, přičemž od 18. října 2024 se tato opatření použijí. Z tohoto důvodu je také nutné, aby byla právní úprava podle tohoto návrhu zákona a jeho prováděcích právních předpisů přijata nejpozději k 18. říjnu 2024 a zároveň ještě předtím byla zajištěná dostatečná legisvakanční lhůta, aby se povinné orgány a osoby stihly připravit na veškeré povinnosti.

**K příloze č. 1 (Identifikace a hodnocení aktiv)**

Cílem přílohy je představit jeden z možných způsobů identifikace a hodnocení aktiv. Tato příloha obsahuje stupnice pro hodnocení důvěrnosti, integrity a dostupnosti stejně jako ta v předchozí vyhlášce s drobnými textovými úpravami. Příloha byla doplněna o popis identifikace a hodnocení aktiv, který by měl usnadnit povinným osobám aplikaci tohoto bezpečnostního opatření a slouží především ke zvýšení návodnosti. Jednotlivé tabulky definují čtyři základní úrovně aktiv, jejich popis, základní formy ochrany, sdílení s třetími stranami podle TLP a požadavky na způsob likvidace (odkazem na další z příloh vyhlášky). Jednotlivé úrovně byly stanoveny na základě dobré praxe. Při tvorbě metodiky hodnocení aktiv je vhodné, aby poskytovatelé regulované služby vycházeli z této přílohy (to však není podmínkou, pokud poskytovatel regulované služby prokáže, že jím používaná metoda hodnocení aktiv a následně i hodnocení rizik zajišťuje minimálně stejnou úroveň procesu řízení rizik).

Zároveň byly do přílohy přesunuty oblasti pro hodnocení primárních aktiv a doplněny o příklady z důvodu zvýšení přehlednosti a návodnosti.

Z této přílohy je možné vycházet při zpracování metodiky pro identifikaci a hodnocení aktiv.

**K příloze č. 2 (Hodnocení rizik)**

Příloha obsahuje doporučení pro výpočet rizik a jednotlivé stupnice pro hodnocení dopadů, hrozeb, zranitelností i rizik. Každá stupnice pracuje se čtyřmi úrovněmi možného hodnocení. Jednotlivé úrovně byly stanoveny na základě dobré praxe, nicméně je vhodné, aby poskytovatel regulované služby při stanovení metodiky pro hodnocení rizik zvážil vhodnost nastavení jednotlivých úrovní a v případě potřeby jednotlivá kritéria upravil podle vlastních potřeb.

Stejně jako v příloze o identifikaci a hodnocení aktiv došlo v této příloze k drobným úpravám textu za účelem zvýšení přehlednosti a návodnosti. Nově byly doplněny způsoby zvládání rizik pro snižování či eliminaci rizik a zajišťování požadované úrovně dostupnosti, integrity a důvěrnosti.

**K příloze č. 3 (Zranitelnosti a hrozby)**

V této příloze je poskytovatelům regulované služby předložen seznam obecných kategorií zranitelností a hrozeb, které je nutné zvážit při hodnocení rizik. Tento seznam není úplným výčtem a je tedy nezbytné a žádoucí, aby jej poskytovatel regulované služby podle potřeby doplnil o další specifické zranitelnosti a hrozby. Existuje velké množství veřejně dostupných katalogů zranitelností a hrozeb, např. ISO/IEC 27005.

Oproti verzi v předchozí vyhlášce došlo k doplnění několika nových hrozeb a zranitelností, které byly identifikovány v rámci činnosti Úřadu, např. zranitelnosti 15 a 16 a hrozby 19 a 20 reagují na zkušenosti s problematikou cloud computingu.

**K příloze č. 4 (Likvidace dat)**

Příloha si klade za cíl popsat možnosti, jak přistoupit k mazání a likvidaci technických nosičů informace, provozních údajů, informací a jejich kopií. Stanovená pravidla pro likvidaci musí být stanovena přiměřeně tak, aby neúměrně nezatížila poskytovatele regulované služby, ale aby byly dodrženy popsané postupy s ohledem na hodnotu aktiv a další aspekty. Stanovené postupy v příloze jsou tímto způsobem formulovány proto, aby bylo zajištěno, že dojde ke správnému posouzení a následnému využití odpovídajícího způsobu likvidace. V další části přílohy jsou popsány samotné způsoby likvidace technických nosičů informace, provozních údajů, informací a jejich kopií. V tabulce, která je uvedená v poslední části této přílohy, jsou uvedeny možné způsoby likvidace podle úrovně důležitosti aktiv.

V této příloze byly provedeny pouze drobné úpravy textu za účelem zvýšení přehlednosti.

**K příloze č. 5 (Obsah bezpečnostní politiky a bezpečnostní dokumentace)**

Příloha obsahuje návrh struktury bezpečnostní politiky a bezpečnostní dokumentace, která vychází především z požadavků kladených v jednotlivých paragrafech vyhlášky a slouží jako přehled požadované dokumentace. Obecně požadavky na bezpečnostní politiku a bezpečnostní dokumentaci upravuje § 7 Řízení bezpečnostní politiky a bezpečnostní dokumentace.

Přílohu zaměřenou na obsah bezpečnostní politiky a bezpečnostní dokumentace obsahovala i předchozí vyhláška, došlo tedy k aktualizaci v souvislosti se změnami v textu vyhlášky.

**K příloze č. 6 (Výbor pro řízení kybernetické bezpečnosti a bezpečnostní role)**

Tato příloha souvisí s § 5 a 6 této vyhlášky. Má doporučující charakter a podrobněji popisuje výbor pro řízení kybernetické bezpečnosti a bezpečnostní role. Doporučení zde uvedená vycházejí z dosavadní praxe Úřadu, z nejlepší praxe a reagují na naléhání poskytovatelů regulovaných služeb na vytvoření alespoň částečné standardizace v této oblasti.

Klíčové činnosti uvedené u jednotlivých bezpečnostních rolí jsou doporučeními, co by mělo být běžnou agendou role a každodenní pracovní náplní. Znalosti, zkušenosti a relevantní certifikace slouží nejen pro potřebu posuzování vhodnosti kandidátů u přijímacích pohovorů, ale současně jako oblasti pro zvyšování znalostí osob již zastávajících bezpečnostní role. Dalšími podmínkami je řešena především neslučitelnost bezpečnostních rolí s ostatními rolemi, jejichž společný výkon by byl ve vzájemném konfliktu.

Tato příloha byla součástí předchozí vyhlášky a došlo pouze k drobným textovým úpravám, např. doplnění klíčové činnosti u garanta aktiva, kterou je provádění identifikace a hodnocení aktiv a rizik. Předchozí vyhláška toto předpokládala, nicméně to explicitně neuváděla.

**K příloze č. 7 (Řízení dodavatelů – bezpečnostní opatření pro smluvní vztahy)**

Obsahem této přílohy je přehled základních bezpečnostních opatření pro smluvní vztahy v oblasti ICT z hlediska bezpečnosti.

Tato příloha vznikla na základě nejlepší praxe. V úvodu je nutné poznamenat, že se i zde využívá přístup orientovaný na rizika. Tzn., že pokud na základě výstupů z hodnocení rizik nebude některé bezpečnostní opatření nezbytné, nebude třeba jej přijímat a aplikovat. Stejně tak by tomu mělo být v případě, kdy některá bezpečnostní opatření nelze aplikovat. To vše by ale mělo být uvedeno v dokumentu nazvaném „Prohlášení o aplikovatelnosti“. Správné a dostatečné ošetření smluvních vztahů z pohledu bezpečnosti je základním předpokladem k zajištění bezpečnosti aktiv regulované služby, kde hrají významnou roli dodavatelé. V příloze je popsán příkladný výčet ustanovení, která by měla obsahovat každá

smlouva. Ustanovení o bezpečnosti informací (z pohledu důvěrnosti, dostupnosti a integrity; možné řešit např. pomocí dohody o mlčenlivosti) je v této příloze zmíněno z toho důvodu, že je nutné nastavit pravidla mezi organizací a dodavatelem při sdílení dokumentů a informací získaných v průběhu plnění smlouvy.

Nutné je zabezpečit také to, aby organizace, která odebírá službu či produkt od dodavatele, měla možnost provést zákaznický audit u tohoto dodavatele. Toto ustanovení je důležité zejména v tom případě, kdy si chce společnost ověřit, zda dodavatel opravdu v praxi dodržuje dohodnuté podmínky a pravidla.

Ustanovení upravující řetězení dodavatelů je ve smlouvách důležité z toho důvodu, že povinný subjekt vybírá dodavatele například dle určitých kritérií, která kladou jisté nároky např. i na bezpečnost. V případě, kdy dodavatel zainteresuje do plnění smlouvy třetí stranu – poddodavatele, není žádoucí, aby se na tohoto poddodavatele tato kritéria nevztahovala. Proto je nutné, aby bylo zajištěno, že i poddodavatel musí splňovat stejné povinnosti jako dodavatel, který tuto zakázku získal. Tento požadavek je zcela klíčový pro bezpečnost a pro správné řízení dodavatelů. Poddodavatel navíc musí samozřejmě dodržovat v plném rozsahu i ujednání mezi dodavatelem a poskytovatelem regulované služby, což je velice důležité pro celý systém řízení bezpečnosti informací.

Další část tohoto ustanovení se věnuje povinnosti dodavatele informovat poskytovatele regulované služby o kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy, způsobu řízení rizik na straně dodavatele a o zbytkových rizicích souvisejících s plněním smlouvy, a o významné změně ovládání tohoto dodavatele podle zákona o obchodních korporacích nebo změně vlastnictví zásadních aktiv využívaných tímto dodavatelem, popřípadě změně oprávnění nakládat s těmito aktivy, k plnění podle smlouvy se správcem. Všechny tyto informace jsou pro odběratele z hlediska kybernetické bezpečnosti důležité. U takto ošetřených smluv se zamezí případům, kdy dodavatel zatají incidenty svému odběrateli nebo kdy ho neupozorní na možná zbytková rizika. Důležité je také vědět, kdo má vliv na ovládání a řízení dodavatele, proto je zde uveden i tento požadavek.

Ustanovení o řízení kontinuity činností v souvislosti s dodavateli je zmíněno v této příloze proto, aby i ve smlouvách bylo jasně uvedeno, jak bude dodavatel zapojený a jaké na něj budou kladeny požadavky v případě nutnosti aktivovat plány kontinuity činností a plány obnovy, které jsou velice významné zejména u kritických systémů státu a jsou nedílnou součástí systému řízení bezpečnosti informací. Zjednodušeně je cílem zainteresovat do plánu kontinuity činností i do plánu obnovy klíčové dodavatele.

Tato příloha vychází z přílohy č. 7 předchozí vyhlášky a doplňuje ji na základě zkušeností Úřadu např. z oblasti cloud computingu.

**K příloze č. 8 (Doporučená témata pro rozvoj bezpečnostního povědomí)**

Na tuto přílohu nově odkazuje § 11 vyhlášky. Cílem této přílohy je snaha Úřadu předat nejlepší praxi získanou vzdělávací činností, vytvořením výčtu nejzásadnějších tématických oblastí, které je dobré zohlednit v plánu rozvoje bezpečnostního povědomí uživatelů. Témata uvedená v této příloze jsou standardní součástí vzdělávacích aktivit Úřadu a jejich promítnutí do rozvoje bezpečnostního povědomí je silně doporučeno všem povinným osobám.