Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

DŮVODOVÁ ZPRÁVA

A. Obecná část

B. Zvláštní část

Bezpečnostní opatření pro poskytovatele regulované služby v režimu nižších povinností jsou vyjmenována v § X odst. 3 *[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 ve většině případů totožný s výčtem bezpečnostních opatření pro poskytovatele regulované služby v režimu vyšším, jsou u poskytovatelů regulované služby v režimu nižším celkově kladeny nižší nároky na úroveň jednotlivých bezpečnostních opatření.

§ X odst. 3 písm. a) *[Seznam bezpečnostních opatření poskytovatele regulované služby]* zákona – organizační opatření
1) zajišťování minimální úrovně kybernetické bezpečnosti
2) povinnosti vrcholového vedení
3) bezpečnostní role
4) řízení bezpečnostní politiky a bezpečnostní dokumentace
5) řízení aktiv
6) řízení dodavatelů
7) bezpečnost lidských zdrojů
8) řízení změn, akvizice, vývoje a údržby
9) řízení přístupu
10) zvládání kybernetických bezpečnostních událostí a incidentů
11) řízení kontinuity činností
§ 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 událostí

7) aplikační bezpečnost
8) kryptografické algoritmy
9) zajišťování dostupnosti regulované služby
10) 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 nižších povinností je především stanovení obsahu jednotlivých bezpečnostních opatření a rozsahu, v jakém jsou poskytovatelé regulované služby v režimu nižších povinností bezpečnostní opatření povinni zavést a provádět, s cílem zajištění bezpečnosti regulované služby a aktiv. Návrh vyhlášky dále stanoví způsob stanovení významnosti dopadu kybernetického bezpečnostního incidentu pro potřeby hlášení kybernetického bezpečnostního incidentu poskytovatelem regulované služby v režimu nižších povinností, jak plyne ze zákona. Návrhem vyhlášky, jehož předmět úpravy je vymezen v § 1, realizuje Úřad zmocněním, které je mu svěřeno na základě § X odst. 1 písm. e) a f) *[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 nižších 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).

V písm. e) je zaveden nový termín „zajišťování minimální úrovně kybernetické bezpečnosti“ směřující přímo na poskytovatele regulované služby v režimu nižších povinností. Cílem rozdílné terminologie oproti systému řízení kybernetické bezpečnosti je potřeba jasného oddělení režimu nižších povinností od režimu vyšších povinností, jelikož každý z nich má svoje specifika.

Svoji zásadní roli při prosazování požadavků kybernetické bezpečnosti zaujímá vrcholové vedení, které je v písm. d) 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.

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.

Jedním ze základních pojmů je rovněž bezpečnostní politika, kterou se rozumí soubor zásad a pravidel, které určují požadavky a způsoby zajištění ochrany aktiv.

K § 3 (Stanovení rozsahu)

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 (Zajišťování minimální úrovně kybernetické bezpečnosti)

Zajišťování minimální úrovně kybernetické bezpečnosti je z definice zajištění minimální úrovně kybernetické bezpečnosti aktiv poskytovatele regulované služby v režimu nižších povinností, založené na zavedení vybraných bezpečnostních opatření. Stanovuje způsob ustavení, zavádění, provozování, monitorování, přezkoumávání a zlepšování s cílem zajistit kybernetickou bezpečnost regulované služby. Je založeno na tzv. PDCA cyklu, svým principem vychází ze systému řízení bezpečnosti informací po vzoru vyhlášky o bezpečnostních opatřeních pro režim vyšších povinností či normy ISO/IEC 27001, avšak klade na povinné osoby nižší nároky. V rámci zajišťování minimální úrovně kybernetické bezpečnosti není na rozdíl od systému řízení bezpečnosti informací mj. požadavek na řízení rizik poskytovatelem regulované služby či na provádění interních auditů. Rizika byla zvažována při výběru bezpečnostních opatření do vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností na základě best practices, mezinárodně uznávaných norem a zkušeností s výkladem a kontrolou povinností obsažených v předchozím zákoně o kybernetické bezpečnosti a vyhlášce o kybernetické bezpečnosti. Požadavek na provedení interního auditu byl nahrazen povinností požádat v pravidelném intervalu o provedení kontroly prostřednicím Úřadem autorizovaného inspektora.

V rámci odst. 1 tohoto ustanovení jsou zmiňovány nejdůležitější požadavky, které jako celek tvoří jádro zajišťování minimální úrovně kybernetické bezpečnosti. Za předpokladu aplikace všech zmíněných požadavků dodrží poskytovatel regulované služby princip PDCA, což povede k udržování minimální úrovně kybernetické bezpečnosti a její neustálé zlepšování.

Základem je stanovení strategických cílů zajišťování minimální úrovně řízení kybernetické bezpečnosti. 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 zavádí bezpečnostní opatření za účelem zajištění bezpečnosti regulované služby.

Aby bylo zajištěno kontinuální zlepšování, je kladen důraz na provádění pravidelného vyhodnocení účinnosti zajišťování minimální úrovně kybernetické bezpečnosti a provádění jeho aktualizace.

Za účelem stanovení hlavních zásad, práv a povinností dále toto ustanovení v písm. c) ukládá povinnost vytvořit a schválit bezpečnostní politiku a bezpečnostní dokumentaci podle § 7 řízení bezpečnostní politiky a bezpečnostní dokumentace v oblasti zajišťování minimální úrovně kybernetické bezpečnosti. Schválení bezpečnostní politiky a bezpečnostní dokumentace zajišťuje mj. vymahatelnost jejího dodržování.

Dále toto ustanovení v odst. 2 ukládá povinnost zpracovat dva klíčové dokumenty, a to plán zavádění bezpečnostních opatření a přehled bezpečnostních opatření. Tyto dokumenty poskytují základní přehled o stavu bezpečnostních opatření a o tom, jak má poskytovatel regulované služby rozvrženou jejich další implementaci. Plán zavádění bezpečnostních opatření obsahuje informace o implementaci bezpečnostních opatření, odhad zdrojů potřebných pro implementaci bezpečnostních opatření a odpovědné osoby. V případě tohoto dokumentu se jedná o obdobu plánu zvládání rizik po vzoru vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností či normy ISO/IEC 27001. Druhý dokument - přehled bezpečnostních opatření obsahuje přehled všech bezpečnostních opatření požadovaných touto vyhláškou, která nebyla aplikována (vč. odůvodnění a přehledu přijatých náhradních bezpečnostních opatření) i která byla aplikována (vč. způsobu plnění). V případě tohoto dokumentu se jedná o obdobu prohlášení o aplikovatelnosti po vzoru vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností či normy ISO/IEC 27001.

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 vrcholové vedení v oblasti kybernetické bezpečnosti a na stvrzení vůdčí role a závazku vrcholového vedení poskytovatele regulované služby k podpoře zajišťování minimální úrovně kybernetické bezpečnosti, jakožto demonstrace vůle k podpoře zajišťování minimální úrovně kybernetické bezpečnosti pro ostatní zainteresované strany (tedy pro osoby zastávající bezpečnostní role, uživatele, další zaměstnance a dodavatele, kterých se problematika kybernetické bezpečnosti dotýká). Dále je nezbytné, aby bylo vrcholové vedení zapojeno do neustálého zlepšování zajišťování minimální úrovně kybernetické bezpečnosti a důraz je kladen i na cyklus přezkoumání zajišťování minimální úrovně kybernetické bezpečnosti.

Aby bylo zajištěno aktivní zapojení vrcholového vedení do zajišťování minimální úrovně kybernetické bezpečnosti, je v odst. 2 požadováno seznámení vrcholového vedení se zprávou o přezkoumání zajišťování minimální úrovně kybernetické bezpečnosti, výsledky analýzy dopadů a výsledky inspekcí a kontrol v oblasti kybernetické bezpečnosti. Cílem tohoto

ustanovení je uvedení vrcholového vedení do problematiky, zajištění jejich informovanosti a tudíž seznámení s podklady pro podporu při rozhodování.

V odst. 3 dále toto ustanovení cílí na organizační zajištění kybernetické bezpečnosti. Důvodem je, aby poskytovatelé regulované služby definovali a přidělili odpovědnosti a pravomoci ve vztahu k zajišťování minimální úrovně kybernetické bezpečnosti. Stěžejní bezpečnostní rolí je role odpovědná za kybernetickou bezpečnost. Další rolí, která musí být určena je garant aktiva.

Důležitým požadavkem je zajistit zastupitelnost osoby odpovědné za kybernetickou bezpečnost, a to z důvodu zajištění kontinuity jednotlivých činností. Pro zajištění zastupitelnosti je možné rozložit povinnosti a kompetence mezi více osob.

K § 6 (Bezpečnostní role)

Bezpečnostní role zodpovědná za kybernetickou bezpečnost, ve smyslu odst. 1, je pro zajišťování minimální úrovně řízení kybernetické bezpečnosti klíčová. Tato role odpovídá za řízení a rozvoj kybernetické bezpečnosti, dohled nad stavem kybernetické bezpečnosti, za naplňování plánu zavádění bezpečnostních opatření a komunikaci v oblasti kybernetické bezpečnosti směrem k vrcholovému vedení a dalším zainteresovaným stranám.

Garant aktiva, dle odst. 2, je bezpečnostní role, která je pověřená organizací k zajištění rozvoje, použití a bezpečnosti aktiva. Má za úkol zajistit důvěrnost, dostupnost a integritu aktiv, a je schopen aktivum ohodnotit. 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 porovnání s požadavky vůči poskytovatelům regulovaných služeb v režimu vyšších povinností nejsou v tomto ustanovení z důvodu ulehčení požadovány další bezpečnostní role.

K § 7 Řízení bezpečnostní politiky a bezpečnostní dokumentace

Základem tohoto ustanovení v odst. 1 je požadavek na stanovení bezpečnostní politiky a vedení bezpečnostní dokumentace, která obsahově pokryje oblasti upravované touto vyhláškou. Stejně jako v případě dosavadní právní úpravy nebo obsahu mezinárodních norem je i tato navrhovaná úprava nadále založena na tzv. dokumentačním modelu. Toto ustanovení je dále rozvedeno přílohou č. 3 k tomuto návrhu vyhlášky, která obsahuje výčet oblastí, které mají být v rámci bezpečnostní politiky a bezpečnostní 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.

Základem pro zajištění provozu z hlediska kybernetické bezpečnosti je stanovení základních provozních pravidel a postupů v provozní dokumentaci. Tato pravidla by měla zohledňovat, resp. vycházet z bezpečnostní politiky a bezpečnostní dokumentace.

Ustanovení v odst. 3, 4 a 5 definuje i další 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 probíhají za podmínek specifikovaných odpovědnou osobou, která k tomu má oprávnění (obvykle vrcholové vedení nebo bezpečnostní role). Cílem je udržet bezpečnostní politiku a bezpečnostní dokumentaci aktuální, tedy odpovídající realitě a bezpečnostním požadavkům, a aktualizace promítnout do relevantních oblastí v provozní dokumentaci. 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 stavu dokumentace a případné revizi.

V porovnání s požadavky vůči osobám v režimu vyšších povinností je znění tohoto ustanovení bez rozdílu, ovšem náročnost plnění tohoto ustanovení je reflektována v příloze č.3, kde jsou kladeny na bezpečnostní politiku a bezpečnostní dokumentaci nižší nároky.

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 na řízení aktiv navazuje dalšími procesy, které na identifikaci aktiv dle zákona přímo navazují.

Do požadavků na řízení aktiv je zařazena povinnost identifikovat a evidovat garanty aktiv (viz odůvodnění k § 6) či hodnotit aktiva. Hodnocení aktiv je požadavek vyplývající zejména z potřeby stanovení bezpečnostních požadavků pro ochranu aktiv dle jejich hodnocení. Zároveň jsou některá bezpečnostní opatření z důvodu přiměřenosti požadavku aplikována pouze na nejdůležitější aktiva. Důležitost aktiva vyplývá právě z jeho hodnocení. Toto ustanovení stanovuje v odst. 1 písm. c) a f) principy hodnocení aktiv. Požaduje primární aktiva hodnotit z hlediska důvěrnosti, dostupnosti a integrity alespoň v souladu s přílohou č. 1 vyhlášky, a při hodnocení podpůrných aktiv zohledňovat vazby na primární aktiva. Potřeba identifikace a evidence relevantních vazeb mezi aktivy vychází z toho principu, že zpracování a poskytování primárních aktiv je prováděno pomocí podpůrných aktiv. Je tedy nezbytné zmapovat relevantní vazby mezi aktivy, zejm. vazby primárních a podpůrných aktiv, a tyto závislosti promítnout do hodnocení podpůrných aktiv. Dalším požadavkem odst. 1, konkrétně písm. g) je uplatnění pravidel, která na základě hodnocení aktiv určí nezbytnou míru potřebných bezpečnostních opatření, možné způsoby zacházení s jednotlivými aktivy a stanoví způsob jejich likvidace. 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. 2 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 informací 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 dodavatelů)

Vyhláška stanovuje základní bezpečnostní pravidla pro řízení dodavatelů, přičemž cílí na dodavatele související se správou nebo dodávkou technických aktiv, která jsou podle hodnocení aktiv (dle § 8 vyhlášky) významná pro regulovanou službu, např. výrobci řídicích systémů, poskytovatelé služeb spojených se správou ICT atp. Ustanovení ukládá v odst. 1 písm. c) povinnost tyto dodavatele identifikovat, evidovat a řídit. Cílem tohoto ustanovení je dosáhnout jasného vymezení odpovědnosti za plnění jednotlivých bezpečnostních opatření (nebo jejich dílčích částí) mezi dodavatelem a poskytovatelem regulované služby. V rámci tohoto ustanovení v odst. 1 písm. d) je opět kladen důraz na vlastní bezpečnostní potřeby poskytovatele

[1] Blíže viz TRAFFIC LIGHT PROTOCOL (TLP) FIRST Standards Definitions and Usage Guidance — Version 2.0. Dostupné online na: https://www.first.org/tlp.

regulované služby, jejichž vyhodnocení má být základním vstupem pro stanovení pravidel pro dodavatele dle odst. 1 písm. a) a dodavatele s těmito pravidly seznamovat.

Dále v souvislosti s výše uvedenými dodavateli je poskytovatel regulované služby povinen v souladu s odst. 1 písm. d) a e) při uzavírání smluv zohledňovat přiměřená bezpečnostní opatření vycházející z identifikovaných bezpečnostních potřeb a zajistit, aby uzavírané smlouvy obsahovaly zejm. oblasti uvedené v příloze č. 4. Poskytovatel regulované služby by v těchto smluvních vztazích měl mít možnost kontroly plnění smluv ve smyslu odst. 2 písm. a) (ve smysluplných případech je možné povinnost samotného vykonání kontroly dodavatelů přenést na třetí stranu např. nezávislého auditora) a možnost plnění smluv vymáhat.

K § 10 (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 dodavatele).

Plán rozvoje bezpečnostního povědomí dle odst. 1 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 povinného subjektu.

V první řadě je tímto návrhem vyhlášky v odst. 2 písm. a) vyžadováno poučení vrcholového vedení o jeho povinnostech a o bezpečnostní politice, zejm. v oblasti zajišťování minimální úrovně řízení kybernetické bezpečnosti. Tento požadavek je stanoven proto, aby bylo vrcholové vedení uvedeno do problematiky zajišťování minimální úrovně kybernetické bezpečnosti a bylo se schopno na něm aktivně podílet např. při zpracování analýzy dopadů či rozhodování.

Dále je v odst. 2 písm. b), c) a d) 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 se jedná o 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 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.

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. 6, na kterou odkazuje odst. 2 písm. g) obsahující doporučená témata pro rozvoj bezpečnostního povědomí, reflektující nejzásadnější rizikové oblasti.

Součástí oblasti bezpečnosti lidských zdrojů je v souladu s odst. 3 písm. b) a c) i kontrola dodržování bezpečnostní politiky a stanovení pravidel a postupů pro řešení případů porušení

stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role (např. disciplinární řízení).

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 § 11 (Řízení změn, akvizice, vývoje a údržby)

Řízení změn, akvizice, vývoje a údržby důležité z hlediska fungování kybernetické bezpečnosti s ohledem na rozvoj poskytovatele regulované služby. Oproti znění tohoto ustanovení pro povinné osoby v režimu vyšších povinností, kdy je toto ustanovení rozděleno na dvě dílčí organizační opatření, tedy řízení změn a řízení akvizice, vývoje a údržby, je toto ustanovení sjednoceno a zjednodušeno, a to zejména z důvodu nižší náročnosti pro zavedení relevantních organizačních procesů a opatření. Ustanovení v této oblasti vychází z nejlepší praxe, ze zkušeností Úřadu a vymezuje v prvním odstavci základní požadavky na řízení změn. Cílem je, aby na identifikované změny, které jsou podstatné z hlediska kybernetické bezpečnosti, tedy mohou mít negativní dopad na důvěrnost, integritu nebo dostupnost regulované služby, byla soustředěna větší pozornost.

V rámci přístupu k těmto změnám pak musí být dle odst. 1 provedena jejich evidence, řízení a přijata opatření minimalizující možné negativní dopady změn. Na základě potřeb je rovněž nutné aktualizovat relevantní bezpečnostní a provozní dokumentaci.

V oblasti akvizice,vývoje a údržby aktiv je dále dle odstavce 2 nutné, aby byly tyto činnosti podpořeny jasnými požadavky na zajištění jejich kybernetické bezpečnosti jako nedílné součásti rozvojových aktivit. Při stanovení bezpečnostních požadavků je nutno vycházet mj. z požadavků tohoto návrhu vyhlášky a specifických potřeb organizace. Rovněž se lze inspirovat v nejrůznějších normách relevantních pro jednotlivá odvětví. Následně, po definování bezpečnostních požadavků, je nezbytné jejich promítnutí do celého životního cyklu od vlastního vývoje až do provozního využití technických aktiv. Jedná se o prosazování principů nejlepší praxe „secure by design“ a „secure by default“.

Oproti znění tohoto ustanovení pro povinné osoby v režimu vyšších povinnosti zde absentuje požadavek na oddělení jednotlivých prostředí, vícefaktorovou autentizaci a kryptografické algoritmy. Tyto požadavky byly z důvodu maturity v oblasti kybernetické bezpečnosti u povinných osob v režimu nižší na základě uvážení Úřadu neuvedeny a jsou pouze reflektovány v jejich relevantních ustanoveních, jelikož není předpoklad, že povinné osoby v režimu nižší mohou dostatečně a náležitě reflektovat požadavky všech bezpečnostních ustanovení v rámci plánovaných akvizic a vývoje.

K § 12 (Řízení přístupu)

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

V souladu s ustanoveními odst. 2 a 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 v souladu s odst. 2 písm. a) a b) 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 přísné regulaci a být možné jen ve zcela výjimečných situacích.

Oproti znění tohoto ustanovení pro povinné osoby v režimu vyšších povinností zde absentuje požadavek na řízení přístupů na základě skupin a rolí, kdy je ze strany Úřadu předpokládáno, že povinné osoby v režimu nižších povinností budou mít v porovnání s povinnými osobami v režimu vyšších povinností řádově mnohem méně zaměstnanců a tudíž i potřebných přístupů k řízení. Tento požadavek by tedy představoval nadměrnou zátěž a nejpravděpodobněji by byl kontraproduktivní, kdy by byla způsobena nepřehlednost v řízení přístupů. V neposlední řadě není odebírání nebo změna přístupových oprávnění oproti ustanovení pro povinné osoby v režimu vyšších povinností vyžadováno bezodkladně například v případě změny nebo ukončení pracovního poměru, a to opět z důvodu snížení náročnosti. Nicméně požadavek jako takový je stále v ustanovení obsažen, pouze s menší časovou urgencí.

K § 13 (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 v režimu nižších povinností v prvním odstavci 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. Cílem ustanovení je zajistit včasné odhalení kybernetického bezpečnostního incidentu a jeho vyšetřování.

Důraz je dále kladen v odst. 1 písm. d) a e) na tzv. kybernetické bezpečnostní incidenty s významným dopadem. Významnost je posuzována v rámci klasifikace kybernetických bezpečnostních incidentů. Tyto incidenty je poskytoval regulované služby povinen hlásit v souladu s požadavky zákona o kybernetické bezpečnosti, a dále u těchto incidentů v souladu s odst. 1 písm. j) a k) prošetřit jejich příčiny, vyhodnotit účinnost řešení těchto incidentů a na základě vyhodnocení přijmout případná další nutná bezpečnostní opatření k zamezení opakování takového incidentu.

K § 14 (Řízení kontinuity činností)

Toto opatření cílí na schopnost organizace rychle a účinně reagovat na situace související s nepříznivými vlivy, které nemůže poskytovatel regulované služby ovlivnit (např. přírodní katastrofy, hackerské útoky) a které mohou mít za následek úplné přerušení či výpadky v poskytování regulované služby. V případě nepřipravenosti na takové situace by hrozil úplný nebo částečný výpadek funkčnosti regulované služby na nepřijatelně dlouhou dobu. Toto opatření vychází z požadavků ISO 22301.

Základem řízení kontinuity činností je vyhodnocení možných dopadů kybernetických bezpečnostních incidentů, tzv. analýza dopadů v souladu s odst. 1 písm. b). Na základě výsledků analýzy dopadů jsou vypracovány plány kontinuity činností a plány obnovy. Zmíněné plány je

nutné aktualizovat a testovat, aby byly v případě situace, která vyžaduje jejich aktivaci, využitelné.

Dále toto ustanovení v odst. 1 písm. e) až h) požaduje provádění pravidelného zálohování a kontrolu použitelnosti provedených záloh, vč. stanovení pravidel a postupů pro tyto činnosti. Zálohy a jejich použitelnost jsou základem řízení kontinuity činností a dále jsou v praxi poslední linií obrany např. v případě útoků typu ransomware.

Za účelem zvýšení odolnosti regulované služby vůči možným kybernetickým bezpečnostním incidentům a omezením dostupnosti je pak v odst. 1 písm. i) kladen důraz na aplikaci bezpečnostních opatření podle § 23 vyhlášky požadující např. redundanci aktiv či oddělení zálohovacího prostředí od jiných prostředí.

K § 15 (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) 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. V tomto režimu není potřebné stanovovat úrovně jednotlivých perimetrů, jako je tomu u režimu vyšších povinností. Takto určené bezpečnostní perimetry 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 živelných událostí či systémy pro kontrolu vstupu. V porovnání s požadavky vyššího režimu zde není vynucena evidence vstupů a přístupů. 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 kontraproduktivní investovat do zabezpečení např. na aplikační úrovni atp.

K § 16 (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). Jelikož jsou v tomto paragrafu popsány obecné a nezbytné základy pro zajištění bezpečnosti komunikačních sítí, není zde kromě odst. 1 písm. g) rozdíl mezi režimem vyšších povinností a nižších povinností.

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 nebo logicky. 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, terminálového připojení na serveru) musí být také náležitě řízena a omezena na 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 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 § 19 odst. 1 písm. c) tohoto návrhu vyhlášky.

Kryptografickými algoritmy k zajištění důvěrnosti a integrity, jsou myšleny především různé zabezpečené protokoly nebo šifrování síťové komunikace. Pro zajištění ochrany integrity komunikační sítě lze využít např. mechanismus na bázi protokolu 802.1x, který povoluje připojení ke komunikační síti nebo jejímu jednotlivému segmentu pouze autentizovaným technickým aktivům. Pro zajištění této ochrany může být využito různých mechanismů nebo způsobů, nicméně pro tento režim není zapotřebí mít specifický nástroj pro řízení této ochrany, jako je tomu u požadavků režimu vyšších povinností.

K § 17 (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 offline útokům, jak byl tento požadavek stanoven v předchozím znění vyhlášky 82/2018 Sb, o kybernetické bezpečnosti. Pojmem offline 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 v návrhu vyhlášky uveden požadavek, aby byla 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.

Oproti tomuto ustanovení pro povinné osoby v režimu vyšších povinností není na povinné osoby v režimu nižších povinností kladen požadavek na vedení evidence nezavedené vícefaktorové autentizace (účtů, technických aktiv a autentizačních mechanismů) z důvodu

snížení procesní zátěže. Přestože tento požadavek absentuje, je doporučováno obdobu takovéto evidence v rámci povinné osoby mít a postupně vícefaktorovou autentizaci zavádět.

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 popsaných 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 § 18 (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. 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 § 19 (Detekce kybernetických bezpečnostních událostí)

V rámci tohoto ustanovení je oproti původnímu znění vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, nově spojeno ustanovení paragrafu 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 kyberbezpečnosti v České republice, postupně se zvyšujícími hrozbami v kyberprostoru a jelikož tyto dva paragrafy byly spolu úzce spjaty v rámci plnění požadavků technických bezpečnostních opatření, tak s rozvojem nových nástrojů, které zajišťují ochranu a plnění těchto požadavků vedly 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 předchozím znění vyhlášky o kybernetické bezpečnosti. Od demonstrativního výčtu bylo v tomto znění vyhlášky opuštěno, 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. Pro režim nižších povinností může být detekce kybernetických bezpečnostních událostí zajištěna více nástroji, oproti centrálně spravovanému nástroji požadovanému pro povinné osoby v režimu vyšších povinností, což vede k větší volnosti kombinaci nástrojů a nižší finanční zátěži, jelikož se nemusí jednat o komplexní řešení. Stejně tak je snížen požadavek na vlastnosti tohoto nástroje, kdy oproti režimu vyšších povinností není vyžadována schopnost tohoto nástroje provádět řízení a sledování komunikace aplikací, služeb a procesů a stejně tak detekce na základě chování technického aktiva, uživatele nebo aplikace, jelikož tyto nástroje jsou zpravidla náročnější na pořízení, údržbu i provoz.

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. Do této kategorie patří nástroje pro detekci škodlivého kódu, skenery zranitelností, antivirové programy, EDR, XDR, nástroje pro detekci/prevenci průniku (IDS/IPS), nástroje pro detekci anomálií, nástroje pro síťovou analýzu, nástroje pro behaviorální analýzu atp.

Pro zjednodušení a ulehčení povinností pro povinné osoby v režimu nižším, byl dále oproti vyššímu režimu odstraněn celý paragraf pro vyhodnocování kybernetických bezpečnostních událostí. Dále se proto ukládá v požadavcích další obecný parametr pro detekční nástroje pro nepřetržité poskytování informací o detekovaných kybernetických bezpečnostních událostech a včasné varování určených rolí (např. detekční nástroj zahlásí varování na detekovanou událost a určené roli dojde upozornění; z helpdesku dojde e-mail určené osobě, že uživatel zaznamenal podezřelé chování koncové stanice). S ohledem na obecnost tohoto požadavku, nepředstavuje nutnost vynaložit další prostředky, jelikož se jedná o běžnou součást detekčních nástrojů.

K § 20 (Zaznamenávání bezpečnostních a relevantních provozních událostí)

Povinná osoba si musí určit na základě hodnocení aktiv a bezpečnostních požadavků, 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 úložišti 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.

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 nižších povinností je doba uchovávání záznamů nastavena na 12 měsíců oproti režimu vyšších povinností, kde je retence stanovena 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 12 měsíců tedy zvyšujeme šanci na zajištění potřebných důkazů k případnému šetření a analyzování incidentů, přičemž oproti režimu vyšších povinností je zde brán zřetel zejména na na finanční náročnost uchovávání těchto záznamů a tudíž jsou kladeny menší nároky na jejich retenci. Stanovené období, po které mají být záznamy 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 12 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 12 měsíců je ovšem výchozí hodnota, která

když bude nastavena jinak, vyžaduje řádné odůvodnění v prohlášení o zavádění bezpečnostních opatření.

Novým požadavkem v oblasti zaznamenávání událostí, oproti předchozímu znění vyhlášky č. 82/2018 Sb., je v případě tohoto návrhu vyhlášky povinnost používat nástroj pro uchovávání záznamů (například nástroj pro správu logů), který by měl zajišťovat i plnění předchozích požadavků jako zajištění důvěrnosti, integrity a dostupnosti ukládaných záznamů. Přestože nasazení tohoto nástroje pro režim nižších povinností může být finančně náročné, představuje z pohledu zejména potenciálního řešení kybernetických bezpečnostních incidentů částečné řešení ve formě zdroje podkladů a nevyžaduje takové odborné personální kapacity, jako např. nástroj pro vyhodnocování kybernetických bezpečnostních událostí u vyššího režimu.

K § 21 (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 osobou (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 vyhlášky č. 82/2018 Sb., je v případě tohoto návrhu vyhlášky 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. Oproti režimu vyšších povinností je v tomto ustanovení explicitně uvedeno, že provádění penetračního testování má být prováděno přiměřeně, tedy zejména s ohledem na finanční možnosti a zdroje povinné osoby.

Tyto penetrační testy povinná osoba provádí před uvedením těchto významných technických aktiv do provozu. 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 určení rozsahu technických aktiv v § 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 režimu vyšších povinností není stanoven interval na provádění penetračních testů, jelikož se jedná o finančně a organizačně náročné bezpečnostní opatření, u kterého je v režimu nižších povinností kladen důraz zejména na testování daného významného technického aktiva před jeho uvedením do provozu.

K § 22 (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 řádně 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 vyhlášky č. 82/2018 Sb., je v případě tohoto návrhu vyhlášky stanoveno, že povinné osoby musí 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, nezbytné ochrany 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.

Oproti režimu vyšších povinností nejsou v tomto ustanovení žádné dílčí změny, jelikož v případě kryptografických algoritmů se jedná o oblast bezpečnostních opatření, kdy pokud daná povinná osoba problematiku nějak řeší nebo musí řešit (například v případě, kdy používá systém správy klíčů a certifikátů), tak nelze tuto oblast obecně plnit částečně nebo o něco méně než režim vyšších povinností, kdy zpravidla pokud tato oblast již je nějak řešena v rámci povinné osoby, tak je řešena uvědoměle a komplexně. Naopak v případě, kdy se povinná osoba touto oblastí nezajímá (například nemá dostačující odborné znalosti), tak ji zpravidla neřeší vůbec a zcela jistě pak existují zranitelnosti v zabezpečení jednotlivých technických aktiv. Ústupky v tomto ustanovení oproti režimu vyšších povinností tudíž nedávají logický smysl, jelikož by se jednalo o ústupky tvořící prostor pro prokazatelné zranitelnosti.

K § 23 (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., o kybernetické bezpečnosti, 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.

Oproti znění tohoto ustanovení pro režim vyšších povinností nejsou žádné dílčí změny, jelikož se jedná o stěžejní oblast z pohledu zajišťování dostupnosti regulované služby a nelze tedy náročnost požadavků v této oblasti snižovat.

K § 24 (Průmyslová, řídící a obdobná specifická technická aktiva)

Navzdory tomu, že se technická opatření tohoto návrhu 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 stanoven na základě zkušeností z prováděných kontrol NÚKIB, kdy povinné subjekty disponovaly 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 § 24 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 § 25 (Stanovení významnosti dopadu kybernetického bezpečnostního incidentu)

Ustanovení zakotvuje způsob určení významnosti dopadu kybernetického bezpečnostního incidentu na poskytování regulované služby ze strany povinné osoby. Určení významnosti dopadu je stěžejní pro případnou aktivaci dalších povinností v procesu hlášení kybernetických bezpečnostních incidentů. Pravidla a postupy pro identifikaci a klasifikaci incidentů s významným dopadem jsou součástí politiky zvládání kybernetických bezpečnostních incidentů. Povinná osoba má v rámci organizačních opatření pro zvládání kybernetických bezpečnostních událostí a incidentů povinnost vypracovat metodiku pro posuzování kybernetických bezpečnostních incidentů.

Povinná osoba si nejprve stanoví únosnou míru újmy způsobené kybernetickým bezpečnostním incidentem. Následně povinná osoba stanoví oblasti pro posouzení významnosti dopadu kybernetických bezpečnostních incidentů na organizaci zohledňující provozní dopad, množství osob zasažených incidentem, čas a zdroje potřebné pro obnovu, lokaci incidentu, citlivost zasažených dat a příčinu incidentu.

Dopad kybernetického bezpečnostního incidentu na poskytování regulované služby se považuje za významný, pokud překročí stanovenou únosnou míru újmy, a zároveň je na základě oblastí pro posouzení dopadu incidentů posouzen jako významný.

Uvedené požadavky na stanovení oblastí pro posouzení významnosti incidentu vycházejí ze systému americké Agentury pro kybernetickou bezpečnost a infrastrukturu (CISA) (CISA National Cyber Incident Scoring System | CISA), jedná se o mezinárodně uznávaný model, jehož funkčnost je ověřena v praxi. Únosná míra újmy v kombinaci s oblastmi pro posouzení významnosti naplňuje požadavky směrnice NIS2 na stanovení významnosti incidentu.

K § 26 (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)

Příloha obsahuje ve formě tabulek doporučené úrovně pro hodnocení důvěrnosti, integrity a dostupnosti primárních aktiv. Jednotlivé tabulky definují čtyři základní úrovně důležitosti 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 důležitosti aktiv je vhodné, aby povinné subjekty vycházely z této přílohy (to však není podmínkou, pokud povinný subjekt prokáže, že jím používaná metoda hodnocení aktiv a následně i hodnocení rizik zajišťuje minimálně stejnou úroveň procesu řízení rizik).

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

K příloze č. 2 (Likvidace dat)

Při tvorbě této přílohy bylo vycházeno zejm. ze standardu NIST Special Publication 800 - 88 - Guidelines for Media Sanitization. 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 povinný subjekt, 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.

K příloze č. 3 (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.

K příloze č. 4 (Požadavky na smluvní ujednání s dodavateli)

Obsah přílohy stanovuje doporučená ustanovení, která je potřeba zohlednit v rámci obsahu smluv s dodavateli. Obsah smlouvy uzavírané s dodavateli stanoví způsoby realizace bezpečnostních opatření a určuje obsah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření.

K příloze č. 5 (Plán kontinuity činností)

Vzhledem k tomu, že poskytovatelé regulované služby v režimu nižším budou organizace, na které ve většině případů dopadne regulace nově, byl z důvodu větší návodnosti vytvořen vzor Plánu kontinuity činností, který povinné osoby mohou, ale nemusejí využít. Vzor slouží pouze jako ukázka, jak je možné plán zpracovat. Obsah si musí každá povinná osoba vytvořit v souladu se specifickým prostředím organizace. V praxi plánů kontinuity činností bývá více a musí vycházet z analýzy dopadů zpracované podle § 14 odst. 1 písm. a) a b) tohoto návrhu vyhlášky. Plán musí v souladu s přílohou č. 3 bodem 2.8. obsahovat podmínky aktivace plánu, specifikaci osob, které se mají plánem řídit a dočasná řešení a postupy pro zajištění kontinuity služby v případě realizace krizového scénáře.

K příloze č. 6 (Doporučená témata pro rozvoj bezpečnostního povědomí)

Na tuto přílohu nově odkazuje § 10 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.