Jde o doplněnou a revidovanou verzi důvodové zprávy, které není zcela totožná s verzí předloženou v rámci standardního legislativního procesu.

Dokument neobsahuje obecnou část důvodové zprávy a je určen výhradně jako informativní podklad.

DŮVODOVÁ ZPRÁVA

k vyhlášce č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností

Bezpečnostní opatření pro poskytovatele regulované služby v režimu vyšších povinností jsou vyjmenována v § 14 odst. 1 *[Seznam bezpečnostních opatření]* zákona č. 264/2025 Sb., o kybernetické bezpečnosti (dále jen „zákon“). Bezpečnostní opatření jsou organizační a technická. Pro přehlednost je níže uveden jejich výčet – tomuto výčtu ve vyhlášce č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností (dále jen „vyhláška“) odpovídají § 3 a následující. Ačkoliv je výčet bezpečnostních opatření pro poskytovatele regulované služby v režimu vyšších povinností ve většině případů obdobný s výčtem bezpečnostních opatření daných již neúčinným zákonem č. 181/2014 Sb., o kybernetické bezpečnosti, resp. již neúčinnou vyhláškou č. 82/2018 Sb., o kybernetické bezpečnosti, došlo v této vyhlášce k některým dílčím úpravám. Tyto zmíněné rozdíly jsou způsobeny především dynamickým vývojem v oblasti kybernetické bezpečnosti. Další motivací Národního úřadu pro kybernetickou a informační bezpečnosti (dále jen „úřad“) při úpravě názvů bezpečnostních opatření uvedených v této vyhlášce byla snaha o přesnější a praxi bližší pojmenování jednotlivých bezpečnostních opatření.

§ 14 odst. 1 písm. a) *[Seznam bezpečnostních opatření]* zákona – organizační opatření
1) systém řízení bezpečnosti informací
2) požadavky na vrcholné vedení
3) stanovení bezpečnostních rolí
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) provádění auditu kybernetické bezpečnosti

§ 14 odst. 1 písm. b) *[Seznam bezpečnostních opatření]* zákona – technická opatření
1) fyzická bezpečnost
2) bezpečnost komunikačních sítí
3) správa a ověřování identit
4) řízení přístupových práv a oprávnění
5) detekce kybernetických bezpečnostních událostí
6) zaznamenávání událostí
7) vyhodnocování kybernetických bezpečnostních událostí
8) aplikační bezpečnost
9) kryptografické algoritmy
10) zajišťování dostupnosti regulované služby
11) zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv

K § 1 (Předmět úpravy)

Tato vyhláška navazuje na zákonem stanovená zmocnění k vydání prováděcího právního předpisu, kterým jsou stanoveny obsahové požadavky na plnění jednotlivých bezpečnostních opatření organizačního a technického charakteru.

Vyhláškou, jejíž předmět úpravy je vymezen v § 1, realizuje úřad zmocnění, které je mu svěřeno na základě § 13 odst. 3 zákona.

K § 2 (Vymezení pojmů)

Toto ustanovení vymezuje základní pojmy používané ve vyhlášce. Tyto pojmy odpovídají terminologii běžně užívané v oblasti ICT a vycházejí mimo jiné z uznávaných standardů, zejména z norem řady ISO/IEC 27000 týkajících se informační bezpečnosti.

Do této oblasti spadají pojmy spojené především se systémem řízení bezpečnosti informací, řízením rizik nebo řízením dodavatelů. Většina pojmů v této oblasti vychází z oficiálních zdrojů (zejména v souladu s normou ISO/IEC 27001). Do této oblasti spadají i pojmy jako primární aktivum, podpůrné aktivum, technické aktivum nebo poskytovatel regulované služby. Tyto pojmy však nejsou definovány ve vyhlášce, ale přímo v zákoně.

Stejně jako v případě zákona, ani ve vyhlášce (s výjimkami) nejsou znovu definovány pojmy již obsažené ve směrnici NIS 2, kterou zákon transponuje.

Ustanovení vymezuje vzájemně související pojmy, a to uživatel, administrátor a privilegovaný uživatel. 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

(např. zaměstnance personálního nebo ekonomického oddělení) o interakce přímo ovlivňující zabezpečení regulované služby, avšak tyto osoby mohou např. významně ovlivnit nastavení zavedených bezpečnostních opatření. Osoba disponující na své koncové stanici účtem lokálního administrátora může např. podle 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 mimo jiné správu, provoz, údržbu nebo bezpečnost technického aktiva. Administrátorem je např. zaměstnanec IT oddělení odpovědný za nastavování zabezpečení technických aktiv nebo dodavatel se stejnou odpovědností.

Pojmy privilegovaný uživatel a administrátor jsou zavedeny z toho důvodu, že je potřebné mezi nimi rozlišovat. Administrátora je potřeba chápat, jako 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. Ovšem v praxi může 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 daného poskytovatele regulované služby, zavedených organizačních, technických opatřeních atd.

Bezpečnostní politikou se rozumí soubor základních pravidel, praktik, kritérií, postupů a odpovědností, které stanovují, jakým způsobem je řízena kybernetická bezpečnost a zajišťována bezpečnost informací regulované služby. Bezpečnostní politiky mohou být dále rozpracovány a specifikovány v bezpečnostní dokumentaci (např. metodika pro určování a hodnocení aktiv a rizik, přehled síťové komunikační infrastruktury). Cílem je, aby všechna pravidla, praktiky, kritéria a postupy byly aktuální, zdokumentované a schválené, tedy i vymahatelné. Z pohledu plnění požadavků této vyhlášky je jedno, v kolika dokumentech budou dané oblasti popsány a jak budou dokumenty pojmenovány. Důležitá je obsahová úplnost a zasazení do řídicí dokumentace konkrétní organizace.

Hodnocením rizik se rozumí proces, který zahrnuje určení rizik, analýzu rizik a vyhodnocení rizik. Určení rizik spočívá v tvorbě relevantních kombinací aktiv, zranitelností a hrozeb, přičemž dochází k určení pouze takových kombinací, které jsou reálně možné. Není tedy cílem určit všechny možné kombinace, ale pouze ty reálně uskutečnitelné. Analýza rizik představuje ohodnocení nalezených rizik podle zvoleného vzorce pro výpočet rizika. Vyhodnocením rizik se poté rozumí porovnání příslušné hodnoty rizika s hranicí akceptovatelnosti a následně uskutečnění rozhodnutí, zda bude dané riziko akceptováno nebo bude muset být sníženo příslušnými bezpečnostními opatřeními. Všechny kroky tohoto procesu musí být vedeny v dokumentované podobě a musí být provedeny v souladu s metodikou pro hodnocení rizik.

Řízením rizik se rozumí proces systematického uplatňování politik, postupů a praktik pro sdělování, konzultování, určování kontextu a zjišťování, analyzování, hodnocení, ošetřování, monitorování a přezkoumávání rizik. Proces řízení rizik zahrnuje proces hodnocení

rizik a jejich následné snižování prostřednictvím stanovení bezpečnostních opatření a následně komunikování určených rizik směrem k vrcholnému vedení organizace.

Systémem řízení bezpečnosti informací se rozumí soubor procesů, politik, postupů a kontrol, které organizace využívá k řízení informační a kybernetické bezpečnosti a minimalizaci určených rizik. Systém řízení bezpečnosti informací je založen na principu udržování bezpečnosti informací a jeho neustálého zlepšování využíváním tzv. PDCA cyklu (z anglického plan, do, check, act). PDCA cyklus ve vztahu k systému řízení bezpečnosti informací představuje zřízení, implementaci a provoz systému řízení bezpečnosti informací, dále monitoring a revizi a následné udržování a zvyšování zavedené úrovně systému řízení bezpečnosti informací. Všechny tyto kroky vedou k budování efektivního systému řízení bezpečnosti informací.

Významný dodavatel je dalším z pojmů převzatých z dosavadní právní úpravy. Změna v této oblasti je především ve zrušení pojmu „provozovatel informačního nebo komunikačního systému“. Významnými dodavateli jsou ti dodavatelé, kteří jsou s poskytovatelem regulované služby ve smluvním nebo jiném právním vztahu a povinnosti z něj vyplývající mají významný vliv na kybernetickou bezpečnost u poskytovatele regulované služby. V praxi se může jednat o poskytovatele klíčových služeb, ale i o dodavatele primárních nebo podpůrných (především technických) aktiv. Na základě poznatků z praxe je potřeba na tomto místě deklarovat, že z povahy věci se v případě zmíněného plnění jedná o právní vztah dodavatelský a nikoli zaměstnanecký. Zaměstnanec v daném vztahu k poskytovateli regulované služby není významným dodavatelem.

K § 3 (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 vztahujícím se k regulované službě. Stanovuje způsob ustanovení, zavádění, provozování, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací a dat (po vzoru normy ISO/IEC 27001).

V tomto ustanovení jsou zmiňovány nejdůležitější požadavky, které jako celek tvoří jádro systému řízení bezpečnosti informací. Za předpokladu aplikace všech zmíněných požadavků dodrží poskytovatel regulované služby základní princip tohoto systému – udržování bezpečnosti informací a její neustálé zlepšování.

Ustanovení systematicky shrnuje dílčí bezpečnostní opatření, která jsou nezbytná v rámci systému řízení bezpečnosti informací zavést. Tato dílčí bezpečnostní opatření jsou poté rozvedena dále v této vyhlášce. Jedná se např. o řízení rizik, stanovení bezpečnostní politiky a bezpečnostní dokumentace nebo provádění auditu kybernetické bezpečnosti a následné zlepšování kybernetické bezpečnosti.

Základem systému řízení bezpečnosti informací je stanovení cílů systému řízení bezpečnosti informací směřujících k zajištění bezpečnosti regulované služby. Tyto cíle, odrážející základní směřování organizace, by měly být stanoveny tak, aby bylo možné provádět jejich vyhodnocení (např. v souladu s metodou SMART). Cíle mohou být stanoveny jak na strategické, tak na operativní úrovni. 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, v rámci stanoveného rozsahu řízení kybernetické bezpečnosti podle § 12 zákona, řídit rizika a zavádět vhodná bezpečnostní opatření.

Za účelem stanovení hlavních zásad, práv a povinností toto ustanovení ukládá povinnost stanovit bezpečnostní politiku a bezpečnostní dokumentaci systému řízení bezpečnosti informací. Stanovení bezpečnostní politiky a bezpečnostní dokumentace představuje proces, který zajišťuje zpracování, schválení a nabytí účinnosti bezpečnostní politiky a bezpečnostní dokumentace a následnou vymahatelnost jejího dodržování. S ohledem na skutečnost, že ne vždy je možné zavést všechna pravidla stanovená v rámci bezpečnostní politiky do praxe v celém rozsahu, je nutné stanovit proces výjimek z těchto pravidel. Výjimky musí být vhodným způsobem řízeny, evidovány a musí podléhat patřičnému schválení. Aby bylo zajištěno kontinuální zlepšování systému řízení bezpečnosti informací, je kladen důraz na provádění vyhodnocení jeho účinnosti alespoň v intervalu jednoho roku a provádění jeho aktualizace. Aby vyhodnocení účinnosti systému řízení bezpečnosti informací plnilo svůj účel a vypovídalo o celkovém stavu systému řízení bezpečnosti informací, je nezbytné do něj zahrnout mimo jiné vyhodnocení cílů systému řízení bezpečnosti informací, posouzení naplňování plánu zvládání rizik, hodnocení stavu systému řízení bezpečnosti informací včetně revize hodnocení rizik, posouzení výsledků auditů kybernetické bezpečnosti a kontrol v oblasti kybernetické bezpečnosti, výsledky předchozích hodnocení účinnosti, posouzení dopadů kybernetických bezpečnostních incidentů a posouzení významných změn. Na základě vyhodnocení účinnosti je vytvořena zpráva o přezkoumání systému řízení bezpečnosti informací, která je předkládána vrcholnému vedení.

Nedílnou součástí kontinuálního zlepšování je také udržení systému řízení bezpečnosti informací ve stavu, který odpovídá skutečnosti a prováděným postupům. Je proto nutné, aby byl systém řízení bezpečnosti informací a relevantní bezpečnostní politika a bezpečnostní dokumentace aktualizovány na základě zjištění z auditů a kontrol v oblasti kybernetické bezpečnosti, výsledků vyhodnocení účinnosti systému řízení bezpečnosti informací, dopadů kybernetických bezpečnostních incidentů na poskytované služby a prováděných významných změn.

Ustanovení dále pojednává o povinnosti řídit provoz a zdroje systému řízení bezpečnosti informací a zaznamenávat činnosti spojené se systémem řízení bezpečnosti informací a řízením rizik. Tento požadavek poukazuje na nutnost plánování zdrojů, ať už se jedná o lidské, finanční nebo technické zdroje, tak je nutné s kapacitou zdrojů pracovat a plánovat jejich využití.

K § 4 (Požadavky na vrcholné vedení)

Vrcholným vedením je statutární orgán nebo jiná osoba v obdobném postavení. V případě obchodní společnosti, je to tedy přímo z definice vyplývající statutární orgán. V případě ministerstev je jím pak myšlen ministr, v případě dalších orgánů státní správy jejich nejvyšší představený – ředitel, předseda apod. Uvedené osoby mohou plnění povinností uvedených v odst. 1 písm. b) až d), f), i), l) až n), odst. 3 písm. a), c) až e) a odstavci 5 tohoto ustanovení delegovat na své zástupce. Tito zástupci však musí mít zajištěny potřebné pravomoci, a to především k výkonu řídicí funkce – může se jednat např. o vedoucího odštěpného závodu zahraniční pobočky nebo prokuristy.

Pro prosazování požadavků kybernetické bezpečnosti je klíčová podpora vrcholného vedení. Větší zapojení vrcholného vedení do řízení kybernetické bezpečnosti zdůrazňuje také směrnice NIS 2, která ukotvuje větší odpovědnost vrcholného vedení za zajišťování kybernetické bezpečnosti. Vyhláška tento rámec nerozšiřuje věcně, ale pouze dále rozpracovává způsob naplnění požadavků směrnice NIS 2. Cílem není jít nad rámec požadavků směrnice NIS 2, ale zajistit praktickou vykonatelnost – tedy popsat, jak má vrcholné vedení plnit svoji roli v rámci systému řízení bezpečnosti informací, jak má být zapojeno a jaké výstupy má znát či schvalovat, včetně zajištění kontrolovatelnosti tohoto požadavku. Směrnice NIS 2 nově zavadí i možnost dočasného zákazu výkonu funkce člena statutárního orgánu, kterou upravuje § 58 zákona, který

implementuje požadavek směrnice NIS 2 čl. 32 odst. 5. Podle § 58 odst. 2 lze návrh na dočasný zákaz výkonu funkce člena statutárního orgánu podat pouze vůči osobě vykonávající řídicí funkci u poskytovatele regulované služby v režimu vyšších povinností a pouze ve vztahu k řídicí funkci, která není veřejnou funkcí vymezenou funkčním nebo časovým obdobím a obsazovanou na základě přímé nebo nepřímé volby anebo jmenováním podle zvláštních právních předpisů.

S větším zapojením vrcholného vedení do řízení kybernetické bezpečnosti je v tomto ustanovení kladen důraz na vzdělávání vrcholného vedení v oblasti kybernetické bezpečnosti a na stvrzení vůdčí role a závazku vrcholného 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 vrcholné vedení ve vztahu ke kybernetické bezpečnosti, definovány bezpečnostní role, které mají být určeny a stanovena povinnost na zřízení výboru pro řízení kybernetické bezpečnosti (dále jen „výbor"). Většina těchto povinností byla stanovena již v původní vyhlášce, a to v § 6 Organizační bezpečnost. Nově je v ustanovení odstavce 1 výslovně uvedeno, že povinností členů vrcholného vedení je prokazatelně se účastnit školení v oblasti kybernetické bezpečnosti, zajistit stanovení bezpečnostní politiky a cílů systému řízení bezpečnosti informací, zajistit integraci systému řízení bezpečnosti informací do procesů poskytovatele regulované služby, zajistit dostupnost potřebných zdrojů a plnit další povinnosti neodmyslitelně spjaté s řádnou schopností vykonávat v zajišťování kybernetické bezpečnosti svou roli a plnit péči řádného hospodáře. S tím souvisí také povinnost uvedená v odstavci 2, kdy se členové vrcholného vedení mají prokazatelně seznamovat s obsahem klíčových dokumentů, které jsou se zajišťováním kybernetické bezpečnosti v organizaci spojeny. Konkrétně se jedná o zprávu o přezkoumání systému řízení bezpečnosti informací, zprávu o hodnocení rizik, plán zvládání rizik, výsledky analýzy dopadů a výsledky auditů kybernetické bezpečnosti a kontrol v oblasti kybernetické bezpečnosti. Povinností členů vrcholného vedení je také informovat zaměstnance a všechny dotčené osoby o významu systému řízení bezpečnosti informací a významu dosažení shody s jeho požadavky. Dotčenými osobami jsou v tomto případě všechny osoby, které přichází do kontaktu s informacemi poskytovatele regulované služby, a tedy mohou být ovlivněny požadavky systému řízení bezpečnosti informací nebo jej mohou samy ovlivnit.

Ustanovení dále ukládá vrcholnému vedení povinnost zapojit se do procesu řízení kontinuity činností. Konkrétně se jedná o spolupráci na tvorbě analýzy dopadů, kdy role vrcholného vedení spočívá v poskytnutí dílčích vstupů a součinnosti při hodnocení možných dopadů kybernetických bezpečnostních incidentů u jednotlivých aktiv. Zapojení a účast vrcholného vedení je nutná také při testování plánů kontinuity činností, plánů obnovy a procesů spojených se zvládáním kybernetických bezpečnostních incidentů. Součinnost v této oblasti demonstruje podporu vrcholného vedení v rámci systému řízení bezpečnosti informací. Hlavním důvodem jeho zapojení do testování těchto plánů a procesu 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 a je tedy potřebné do testů zapojit osoby, které disponují potřebnými pravomocemi. Navíc v případě, kdy dojde k incidentu a je nutné plány aktivovat, musí být postupy uvedené v plánu zvládnuty i z pozice vrcholného vedení. Procesy po aktivaci krizové situace by měly být zautomatizovány a zainteresované strany mají mít znalosti o své roli a z ní plynoucích povinnostech při řízení kontinuity činností.

Nedílným požadavkem v této oblasti je, aby došlo ze strany vrcholného vedení ke stanovení pravidel pro určení administrátorů a osob, které budou zastávat bezpečnostní role a aby prostřednictvím vrcholného vedení byla u relevantních osob (jako jsou administrátoři, osoby zastávající bezpečnostní role, osoby s přístupem k citlivým informacím, dodavatelé apod.) vyžadována mlčenlivost. V praxi se tedy např. jedná o to, aby závazné pracovní pokyny a smlouvy uzavřené s těmito osobami obsahovaly ustanovení o zajištění důvěrnosti informací, případně samostatné dohody o zachování důvěrnosti nebo mlčenlivosti.

Požadavek na zřízení výboru je ve vyhlášce obsažen proto, aby byla u poskytovatele regulované služby ustanovena organizovaná skupina osob, která se zabývá celkovým řízením a rozvojem systému řízení bezpečnosti informací. Vrcholné vedení musí kromě zřízení výboru určit jeho členy a stanovit práva a povinnosti výboru a jeho členů související se systémem řízení bezpečnosti informací. Výbor musí být složen alespoň z jednoho zástupce vrcholného vedení nebo jím pověřené osoby, což má zajistit provázanost a informovanost vrcholného vedení o kybernetické bezpečnosti, a tím zajistit účelnou podporu celému systému řízení bezpečnosti informací. Manažer kybernetické bezpečnosti musí být členem výboru, jelikož je rolí se svěřenými pravomocemi k zajištění fungování tohoto systému a měl by úzce komunikovat nejen s lidmi, kteří se zabývají kybernetickou bezpečností a provozem systémů, ale i s vrcholným vedením (kvůli jeho rozhodovací pravomoci v organizaci). V tomto ustanovení je nově stanovena také povinnost uskutečnění jednání výboru v pravidelném intervalu, konkrétně alespoň jednou ročně, a povinnost vést o průběhu jednání výboru dokumentovaný záznam. Tímto je výslovně stanovena doposud prakticky opomíjená povinnost, která v některých organizacích vedla k tomu, že byl význam výboru snižován a závěry z jeho jednání nebyly dokumentovány. Stanovením frekvence pro konání výboru alespoň jednou ročně došlo k určení minimálního intervalu, ve kterém je nutné výbor uskutečnit. Pokud má však poskytovatel regulované služby stanoven častější interval (např. jednou za tři měsíce), není žádoucí v tomto ohledu provádět změny a interval prodlužovat, obzvlášť pokud již stanovený interval odpovídá jeho potřebám a zajistí, že je vrcholné vedení dostatečně informováno o aktuálním stavu systému řízení bezpečnosti informací.

Důležitým požadavkem této vyhlášky je dále zajištění zastupitelnosti bezpečnostních rolí manažera a architekta kybernetické bezpečnosti. Požadavek reaguje na situace, kdy osoby zajišťující pro povinnou osobu výkon těchto rolí nemají adekvátní zástup. To může mít mimo jiné vliv i na zajištění kontinuity některých činností souvisejících s poskytováním regulované služby. 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 stanoveny pro bezpečnostní role v následujícím ustanovení, použijí přiměřeně.

K § 5 (Stanovení bezpečnostních rolí)

Ustanovení navazuje na § 4 vyhlášky a definuje jednotlivé bezpečnostní role, které musí být vrcholným vedením určeny. Pro výkon jednotlivých bezpečnostních rolí jsou stanoveny kvalifikační podmínky, přičemž jsou zohledňovány všechny doklady o dosažené kvalifikaci, tedy např. diplomy, osvědčení či jiné doklady o získané relevantní praxi. Pro stanovení kvalifikačních podmínek bylo postupováno v souladu s § 26 odst. 1 zákona č. 18/2004 Sb. o uznávání odborné kvalifikace a jiné způsobilosti státních příslušníků členských států Evropské unie a o změně některých zákonů (zákon o uznávání odborné kvalifikace). Délka praxe pro jednotlivé bezpečnostní role, s výjimkou role garanta aktiva, je stanovena na dobu tří let z důvodu, že se jedná o dostatečně dlouhou dobu, za kterou je možné získat dostatek zkušeností pro výkon těchto bezpečnostních rolí. Manažer kybernetické bezpečnosti je pověřen řízením systému řízení bezpečnosti informací. Tato role je klíčová pro správné nastavení

fungování systému řízení bezpečnosti informací. Pro tuto činnost proto musí být daná osoba vyškolena a prokázat odbornou způsobilost praxí. Vyškolení pro výkon dané činnosti bezpečnostní role lze vyžadovat na základě výstupů systému řízení bezpečnosti informací v různé míře, kdy požadovanou odbornou způsobilost ve formě absolvovaných školení, certifikací, kurzů atd. lze na straně poskytovatele regulované služby přizpůsobit. 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. Tyto požadavky jsou ve vyhlášce mimo jiné proto, že osoby zastávající roli manažera kybernetické bezpečnosti mají zásadní vliv na to, jakým způsobem bude řízena a zajišťována kybernetická bezpečnosti regulovaných službeb důležitých pro chod státu nebo pro jeho obyvatelstvo. Splněnín alespoň výše popsaných nároků je tak nezbytné. Manažer kybernetické bezpečnosti má dále povinnost informovat vrcholné vedení o činnostech vyplývajících z výkonu jeho 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 informovanosti a zainteresovanosti vrcholného vedení do celé problematiky. Toto ustanovení si také klade za cíl usnadnit manažerovi kybernetické bezpečnosti prosazování jednotlivých kroků vedoucích ke zvýšení kybernetické bezpečnosti podle systému řízení bezpečnosti informací. Vzhledem k náplni práce je role manažera kybernetické bezpečnosti neslučitelná s výkonem role, která má svěřené pravomoci k provozu technických aktiv regulované služby. Tento požadavek vychází jak z nejlepší praxe, tak i z poznatků získaných kontrolní činností úřadu. V praxi je problematické, pokud je manažer kybernetické bezpečnosti zároveň pověřen výkonem funkce odpovědné za provoz technických aktiv (např. vedoucí nebo zaměstnanec ICT oddělení nebo dodavatel služeb zajišťující ICT provoz). V tomto případě manažer kybernetické bezpečnosti není schopen objektivně prosazovat všechny aspekty systému řízení informační bezpečnosti a ve stanoveném rozsahu řízení kybernetické bezpečnosti. Organizační zařazení osoby zastávající roli manažera kybernetické bezpečnosti je ponecháno na uvážení poskytovatele regulované služby, nicméně z nejlepší praxe vyplývá, že je vhodné tuto roli organizačně zařadit blízko vrcholnému vedení, aby bylo docíleno rychlé a efektivní komunikace právě s vrcholným vedením a zajištění dostatečných pravomocí, které jsou pro výkon této bezpečnostní role důležité.

Architekt kybernetické bezpečnosti je bezpečnostní rolí zajišťující návrh a implementaci bezpečnostních opatření tak, aby byla zajištěna bezpečná architektura pro regulovanou službu. V praxi má architekt kybernetické bezpečnosti svěřeny pravomoci k zajištění návrhu bezpečnostní architektury od komunikační infrastruktury, až např. po bezpečnost na aplikační úrovni. Rovněž má svěřeny pravomoci k následné 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. Varianta, kdy je v organizaci výkon role architekta kybernetické bezpečnosti rozdělen mezi více osob s přihlédnutím na jejich zaměření a k technologiím využívaným v organizaci, je přípustná.

Garant aktiva je bezpečnostní role, která je pověřená k zajištění rozvoje, použití a bezpečnosti aktiva. Má za úkol zajistit důvěrnost, integritu a dostupnost daného aktiva, a také se podílet na určení a hodnocení rizik. 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.

Auditor kybernetické bezpečnosti má svěřeny pravomoci k 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 a bezpečnostní dokumentací, vhodnými bezpečnostními standardy a s poskytováním nezávislé zpětné vazby o účelnosti a účinnosti systému řízení bezpečnosti informací a bezpečnostních opatření.

Pokud je v rámci poskytovatele regulované služby zákonem regulováno více služeb, je logické, že není zapotřebí jmenovat do jednotlivých rolí pro každou regulovanou službu rozdílné osoby (jedna bezpečnostní role může mít svěřené pravomoci vůči více regulovaným službám).

K § 6 (Řízení bezpečnostní politiky a bezpečnostní dokumentace)

Základem tohoto ustanovení je požadavek na stanovení bezpečnostní politiky a bezpečnostní dokumentace, která obsahově pokryje relevantní oblasti upravované touto vyhláškou. V rámci 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 prostředí organizace a zavedené zvyklosti v oblasti řízení dokumentů u poskytovatele regulované služby. Je však nutné, aby byla pravidla a postupy stanovené v bezpečnostní politice a bezpečnostní dokumentaci poskytovatelem regulované služby dodržována.

Ustanovení definuje mimo jiné požadavky k zajištění bezpečnosti provozu regulované služby formou stanovení základní provozní dokumentace, pravidel a postupů. Tato dokumentace, pravidla a postupy by měly zahrnovat oblasti vycházející z bezpečnostní politiky a bezpečnostní dokumentace.

Ustanovení dále specifikuje 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 bezpečnostních politik a bezpečnostní dokumentace probíhá za podmínek specifikovaných odpovědnou osobou, která k tomu má oprávnění (obvykle vrcholné vedení nebo jiná bezpečnostní role). Toto řízení musí probíhat tak, aby bezpečnostní politika a bezpečnostní dokumentace byly přiměřeně dostupné v elektronické nebo listinné podobě dotčeným stranám, byly chráněny z pohledu důvěrnosti, integrity a dostupnosti, byly vedeny tak, aby informace v nich obsažené byly úplné, čitelné, správné, snadno identifikovatelné a vyhledatelné a aby byly dotčené osoby poskytovatele regulované služby informovány o právech, povinnostech a postupech v nich obsažených. Dotčenými stranami jsou v tomto případě ty konkrétní strany, na které se daná bezpečnostní politika nebo bezpečnostní dokumentace vztahuje a jsou dotčeny jejich práva nebo povinnosti. Pokud si poskytovatel regulované služby stanoví bezpečnostní politiku, která bude např. upravovat zařízení, která nemá ve své správě (může se typicky jednat o zařízení dodavatelů), měl by informovat osoby, které s těmito zařízeními nakládají nebo se přes ně připojují. Jako další příklad lze uvést situaci, kdy se bude bezpečnostní politika týkat zajištění bezpečné kryptografie v rámci jejich síťové komunikace, tak se s touto bezpečnostní politikou s nejvyšší pravděpodobností nebude seznamovat podpůrný technicko-hospodářský personál, pro který by tato bezpečnostní politika byla nerelevantní a navíc by tento personál nemusel disponovat potřebným know-how. Snadno identifikovatelnými informacemi se rozumí takové informace, které jsou jasné, přehledné a jednoznačně určují osobu, proces nebo objekt, kterého se týkají. Snadno vyhledatelné informace v rámci bezpečnostní politiky a bezpečnostní dokumentace představují stav, kdy je samotná bezpečnostní politika a bezpečnostní dokumentace organizována a strukturována tak, aby se v ní daly rychle a efektivně nalézt požadované informace. Informování dotčených

osob o jejich právech, povinnostech a postupech obsažených v bezpečnostní politice a bezpečnostní dokumentaci napříč celou organizační strukturou je důležité pro zajištění správné funkčnosti systému řízení bezpečnosti informací. V případě bezpečnosti lidských zdrojů se jedná např. o seznámení zaměstnanců s bezpečnostní politikou a bezpečností dokumentací, což podpoří jejich následné plnění. Dalším příkladem může být komunikace v oblasti řízení kontinuity činností, kdy je nutné, aby relevantní osoby byly seznámeny s jejich pravomocemi a odpovědnostmi k zachování kontinuity činností, a to nejen z pohledu poskytování regulované služby. Správně fungující proces řízení kontinuity je v případě výskytu mimořádné události stěžejní. Dále je nutné komunikovat např. i výstupy z interních auditů kybernetické bezpečnosti, a to z důvodu zajištění neustálého zlepšování systému řízení bezpečnosti informací nebo také výsledky hodnocení rizik a následné řízení rizik, jelikož ztráta relevantní informace o určitém riziku může poskytovateli regulované služby způsobit negativní důsledky na zajištění bezpečnosti informací regulované služby. Cílem tohoto ustanovení je, aby poskytovatel regulované služby udržoval bezpečnostní politiku a bezpečnostní dokumentaci aktuální, tedy odpovídající realitě a bezpečnostním požadavkům. Zároveň je zohledňováno, zda bezpečnostní politika a bezpečnostní dokumentace plní účel, ke kterému byla vytvořena.

Pravidelným přezkoumáním se rozumí stanovený interval, ve kterém dochází k pravidelnému posouzení a případné revizi. V souladu s požadavky nejlepší praxe by měl být nastaven na jeden rok. Přezkoumání a aktualizace bezpečnostní politiky a bezpečnostní dokumentace má být prováděno také na základě výsledků vyhodnocení účinnosti systému řízení bezpečnosti informací, dopadů kybernetických bezpečnostních incidentů, zjištění z auditů kybernetické bezpečnosti a kontrol v oblasti kybernetické bezpečnosti a také v souvislosti s prováděnými významnými změnami. Novou povinností je stanovit osobu odpovědnou za tento pravidelný přezkum a aktualizaci bezpečnostní politiky a bezpečnostní dokumentace.

Ustanovení kombinuje hlavně § 10 a 30 původní vyhlášky, ale také např. zpřesňuje § 3 písm. d) této vyhlášky. Zmíněné dva paragrafy původní vyhlášky se věnovaly bezpečnostní politice a bezpečnostní dokumentaci, proto došlo k jejich spojení s cílem zvýšit přehlednost a seskupit související povinnosti do logického celku.

Původní příloha č. 5, která obsahovala návrh struktury bezpečnostní politiky a bezpečnostní dokumentace a oblasti, které by v jednotlivých dokumentech měly být zpracovány byla z vyhlášky odebrána. Důvodem odstranění této přílohy je skutečnost, že požadavky na dokumentaci jsou nyní začleněny do ustanovení jednotlivých paragrafů. Odebrání této přílohy poskytovateli regulované služby umožňuje si individuálně určit, co je pro něj v rámci bezpečnostní politiky a bezpečnostní dokumentace relevantní. Systém řízení bezpečnosti informací však není postaven pouze na stanovení bezpečnostní politiky a bezpečnostní dokumentace, ale i na jejím začlenění do celého systému řízení bezpečnosti informací a jeho fungování. Aby mohl být systém řízení bezpečnosti informací funkční, je nutné mít správně zmapované jednotlivé procesy a organizaci, tyto procesy mít dále zdokumentované a mít za ně stanoveny odpovědné osoby.

K § 7 (Řízení aktiv)

Povinnost provést určení primárních a podpůrných aktiv, včetně vazeb mezi nimi je uložena na úrovni zákona. Ten ukládá povinnost určit všechna primární aktiva v rámci celé organizace, určit ta, která souvisejí s poskytováním regulované služby a u těchto určených primárních aktiv následně určit související organizační části organizace a podpůrná aktiva. Vyhláška v ustanovení k řízení aktiv navazuje dalšími procesy, které s určováním aktiv podle zákona přímo souvisí. V rámci tohoto procesu vyhláška ukládá povinnost stanovit metodiku pro určování aktiv i přesto, že povinnost určení primárních a podpůrných aktiv již vyplývá ze zákona, a to z důvodu, že řízení aktiv nebo obecně systému řízení bezpečnosti informací

je kontinuálním cyklem, který se neustále vyvíjí a opakuje. Metodika pro určování aktiv může obsahovat např. proces určování typových aktiv nebo postup určení nově nabytých aktiv.

Do požadavků na řízení aktiv je také zařazena povinnost určit a evidovat garanty aktiv nebo hodnotit aktiva podle stanovené metodiky. Při hodnocení primárních aktiv musí být posouzeny alespoň oblasti uvedené v příloze č. 1 k vyhlášce. Tento požadavek obsahovala již původní vyhláška, oproti té byl ale výčet těchto oblastí přesunut z těla paragrafu do přílohy. 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 znát jednotlivé závislosti mezi primárními a podpůrnými aktivy a ty určit formou vzájemných vazeb, které je následně potřeba při hodnocení podpůrných aktiv zohlednit.

Původní vyhláška požadovala určit a evidovat pouze vazby mezi primárními a podpůrnými aktivy. Vzhledem k tomu, že jsou v praxi důležité také vazby mezi jednotlivými primárními aktivy i jednotlivými podpůrnými aktivy (jsou používané víceúrovňové modely), bylo písmeno f) zobecněno na potřebu určit a evidovat pouze relevantní vazby, a to mezi všemi aktivy. Není nutné určit a evidovat všechny vazby mezi všemi aktivy, ale pouze ty, které mají vliv na kybernetickou bezpečnost regulované služby a promítají se do hodnocení aktiv a posléze rizik. Na tento požadavek navazuje písmeno g), kde zůstala zachována povinnost hodnotit určená podpůrná aktiva a zohlednit při tomto hodnocení vazby na primární aktiva.

Nově došlo ke sloučení písmen h), i), j) z odstavce 1 původní vyhlášky do jednoho písmene, které požaduje stanovení pravidel ochrany nutných pro zabezpečení důvěrnosti, integrity a dostupnosti jednotlivých úrovní aktiv. Nejedná se tedy o nový požadavek, všechny uvedené povinnosti byly v původní vyhlášce uvedeny a aktuální ustanovení o řízení aktiv bylo seskupením těchto souvisejících oblastí zpřehledněno.

Možné způsoby zacházení s aktivy je zapotřebí stanovit přiměřeně k úrovni hodnocení jednotlivých aktiv. Příkladem může být příloha č. 1 k vyhlášce, která obsahuje možné způsoby ochrany aktiv, včetně odkazu na přílohu č. 2 k vyhlášce, která se zabývá likvidací informací a dat. V neposlední řadě v rámci tabulky č. 1 přílohy č. 1 k vyhlášce je uvedeno, že lze pro klasifikaci důvěrnosti informací a dat pro účely jejich sdílení využít současnou verzi mezinárodního standardu tzv. Traffic Light Protocol[1] (dále jen „TLP“). TLP je ustálený systém označování 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).

Odstavec 2 původní vyhlášky obsahující výčet oblastí, které je třeba posoudit při hodnocení primárních aktiv, byl v rámci této vyhlášky přesunut do přílohy č. 1 k této vyhlášce a byl doplněn o příklady a vysvětlivky s cílem zvýšení návodnosti. Došlo tedy pouze k přesunutí ustanovení do přílohy č. 1 k této vyhlášce, a nikoliv k vytvoření nové povinnosti. Tento výčet oblastí není absolutní a poskytovatel regulované služby by jej měl rozšířit podle svých potřeb a specifik. V seznamu jsou uvedeny nejdůležitější faktory, které by měly být posouzeny vždy, jelikož jsou významné z pohledu hodnocení aktiv. V případě, že je některý z faktorů

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

nerelevantní, poskytovatel regulované služby jej posoudí pouze v tom smyslu, že tento faktor v tomto konkrétním případě není pro dané primární aktivum relevantní.

K § 8 (Řízení rizik)

Jelikož vyhláška přímo navazuje na obsah původní vyhlášky 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, které upravuje povinnost zavádět a provádět bezpečnostní opatření ve stanoveném rozsahu řízení kybernetické bezpečnosti.

Požadavky na poskytovatele regulované služby 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 poskytovatele regulované služby přijatelná a oproti tomu i úroveň, která přijatelná není a pro kterou je nutné přijímat vhodná bezpečnostní opatření. Proces řízení rizik musí být formalizován, musí být prokazatelný a opakovaně vykonatelný bez závislosti na konkrétní osobě, která hodnocení provádí.

V návaznosti a s ohledem na jednotlivá aktiva určená v rámci řízení aktiv podle § 7 musí být dále určeny relevantní zranitelnosti a hrozby na ně působící. Příloha č. 3 k této vyhlášce obsahuje vybrané kategorie zranitelností a hrozeb, které musí být zváženy. Při hodnocení rizik je následně potřeba tyto relevantní zranitelnosti a hrozby zohlednit a provést ho alespoň v rozsahu přílohy č. 4 k vyhlášce. V rámci hodnocení rizik (tzn. např. i v plánu zvládání rizik) je dále nutné zohlednit i další související procesy, jako je např. audit kybernetické bezpečnosti, proběhlé kybernetické bezpečnostní incidenty, protiopatření vydaná úřadem v souladu s § 20 zákona, výsledky penetračního testování a skenování zranitelností či významné změny.

V rámci tohoto ustanovení je deklarována možnost hodnotit rizika i jiným způsobem, než je popsán ve vyhlášce, avšak za předpokladu, že tento alternativní způsob zajistí stejnou nebo vyšší úroveň procesu hodnocení rizik. Tím je poskytovateli regulované služby dána možnost hodnotit rizika způsobem vyhovujícím konkrétnímu prostředí a jeho specifikům (např. používat vlastní rejstřík hrozeb a zranitelností nebo jiné stupnice pro hodnocení zranitelností, hrozeb a rizik). Vždy je ale potřeba dodržet povinnost provádět toto hodnocení rizik v pravidelných intervalech alespoň jednou ročně a při významných změnách v rámci jejich rozsahu. Pokud by pro poskytovatele regulované služby pro potřeby hodnocení rizik nebyly dostatečně návodné přílohy k vyhlášce, je možné využít podpůrný materiál Průvodce řízením aktiv a rizik podle vyhlášky o kybernetické bezpečnosti publikovaný úřadem na svých webových stránkách.

Výsledky hodnocení rizik jsou obsahem zprávy o hodnocení rizik, se kterou se seznamuje vrcholné vedení. V návaznosti na výsledky hodnocení rizik má být dále, s ohledem na bezpečnostní potřeby poskytovatele regulované služby, sestaveno prohlášení o aplikovatelnosti. Prohlášení o aplikovatelnosti je dokument (v tištěné nebo elektronické podobě), obsahující přehled zavedených a nezavedených bezpečnostních opatření požadovaných touto vyhláškou včetně popisu způsobu zavedení, případně s odůvodněním, proč některá bezpečnostní opatření zavedena nebyla (pozn. možno řešit odkazem na plán zvládání rizik). Nově byla část týkající se neaplikovaných bezpečnostních opatření rozšířena o přehled přijatých náhradních bezpečnostních opatření (§ 8 odst. 1 písm. f) bod 1 vyhlášky). Tím, že některá bezpečnostní opatření nejsou aplikována, vzniká bezpečnostní riziko, které by mělo být sníženo náhradními bezpečnostními opatřeními. V praxi se může jednat např. o technické aktivum, které je již zastaralé a bez podpory, avšak z objektivního důvodu není možné jej vyměnit. Náhradními bezpečnostními opatřeními v tomto případě může být jeho oddělení do speciálního segmentu sítě, maximální omezení povolené komunikace nebo zvýšený

monitoring. Tato povinnost se nevztahuje na bezpečnostní opatření, která nejsou pro poskytovatele regulované služby relevantní např. organizace, která nevyužívá průmyslová, řídicí nebo obdobná specifická technická aktiva, nebude mít co zabezpečovat v souvislosti s požadavky § 27 a daná bezpečnostní opatření jsou tak neaplikovatelná. Cílem prohlášení o aplikovatelnosti je tedy popsat aktuální stav organizace ve vztahu k zákonu a vyhlášce.

Dalším klíčovým dokumentem (v tištěné nebo elektronické podobě) vycházejícím z výsledků hodnocení rizik je plán zvládání rizik. Cílem plánu zvládání rizik je zejména systematický přístup k zavádění bezpečnostních opatření, stanovení prioritizace při eliminaci rizik, stejně tak jako efektivní plánování technických, finančních i lidských zdrojů potřebných pro zajištění kybernetické bezpečnosti.

Celkově došlo v tomto ustanovení pouze k dílčím úpravám textu s cílem zpřehlednění požadavků. Například písmeno b) obsahuje navíc oproti původní vyhlášce „při určování rizik“, aby bylo jednoznačné, že se jedná o název činnosti „s ohledem na aktiva určuje relevantní hrozby a zranitelnosti, přitom zvažuje zejména kategorie hrozeb a zranitelností, která v původní vyhlášce nebyla pojmenovaná. Dalším příkladem může být rozdělení obsahu plánu zvládání rizik, který byl v původní vyhlášce popsán v rámci jednoho písmene, nicméně v rámci kontrolní činnosti bylo zjištěno, že plány zvládání rizik často neobsahují některou z vyjmenovaných oblastí, a proto byly tyto oblasti rozepsány do samostatných bodů pod odst. 1 písm. g) z důvodu zvýšení přehlednosti. U odstavce 1 písm. g) bylo dále doplněno o další body, které musí být v rámci hodnocení rizik a plánu zvládání rizik brány v potaz. U původní vyhlášky nebyly body 1 a 7 explicitně uvedeny, přesto principy a fungování vyhlášky předpokládaly, že budou u těchto činností zohledněny. Z důvodu zvýšení přehlednosti a lepšímu uvědomění si vazeb s jinými bezpečnostními opatřeními byly doplněny.

Ustanovení v odstavci 4 stanovuje, že poskytovatel regulované služby může vyloučit zavádění a provádění některého bezpečnostního opatření, avšak pouze na základě řízení rizik, tedy podle požadavku § 8 této vyhlášky musí provést hodnocení rizik, následně provést jejich vyhodnocení a přijmout náhradní adekvátní bezpečnostní opatření. Tento závěr plyne z toho, že bez plnění povinnosti řídit rizika nelze zjistit, která bezpečnostní opatření a v jakém rozsahu organizace nemusí zavést, aby i přesto dostatečně a efektivně zajistila kybernetickou bezpečnost regulované služby. V případě, že poskytovatel regulované služby některé bezpečnostní opatření vyloučí, je nutno tuto skutečnost řádně dokumentovat v prohlášení o aplikovatelnosti podle § 8 odst. 1 písm. f) bodu 1 vyhlášky. Příkladem může být situace, kdy je pro zajištění regulované služby využíván dispečerský systém SCADA. U těchto typů systémů je mnohdy nemožné zajistit aktuální operační systém na dispečerské stanici, která SCADA povoluje. V praxi tak poskytovatel regulované služby riziko související s neaktuálními operačním systémem vyhodnotí v rámci řízení rizik podle § 8 vyhlášky a v souladu se stanovenými kritérii pro akceptovatelnost rizik přijme adekvátní náhradní bezpečnostní opatření, např. umístění dispečerské stanice do speciálního segmentu, zamezení připojování zařízení USB zařízení ke stanici, odpojení stanice od internetu, řízení přístupů ke stanici nebo poučení dispečerů. Způsob řešení poskytovatel regulované služby dokumentuje v rámci prohlášení o aplikovatelnosti. Následně toto riziko vyhodnocuje v pravidelných intervalech v rámci standardního procesu řízení rizik. Dalším příkladem může být neimplementování antiviru nebo jiného obdobného nástroje zajišťujícího detekci kybernetických bezpečnostních událostí, např. z důvodu nedostatečného výpočetního výkonu aktiva nebo možných následků v případě nesprávného vyhodnocení detekce kybernetické bezpečnostní události a následného omezení funkčnosti aktiva. Poskytovatel regulované služby v tomto případě postupuje stejný způsobem jako v předchozím případě, tedy vyhodnotí související rizika a zavede adekvátní náhradní bezpečnostní opatření, např. implementuje jiný detekční nástroj, omezí přístup k aktivům a povolí nejnutnější služby nebo zvýší dohled nad aktivem. Zvolený způsob řešení poskytovatel

regulované služby opět řádné dokumentuje v rámci prohlášení o aplikovatelnosti a riziko vyhodnocuje v pravidelných intervalech v rámci procesu řízení rizik.

K § 9 (Řízení dodavatelů)

Ustanovení o řízení dodavatelů stanovuje základní bezpečnostní pravidla pro řízení dodavatelů a pro uzavírání dodavatelských smluv, která zohledňují požadavky systému řízení bezpečnosti informací. Cílem tohoto ustanovení je dosažení jasného vymezení odpovědností za plnění jednotlivých bezpečnostních opatření (nebo jejich dílčích částí) mezi dodavatelem a poskytovatelem regulované služby. Řízení dodavatelů je komplexní činností, která se projevuje v průběhu celého životního cyklu dodavatelského vztahu. Je žádoucí řídit dodavatele již od samotného zadávacího řízení vedoucího k výběru dodavatele, v průběhu samotné realizace plnění, jeho splnění, až po samotné ukončení smlouvy. V rámci tohoto ustanovení je opět kladen důraz na 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. I proto je důležité mít vlastní bezpečnostní potřeby řádně promítnuty do bezpečnostní politiky pro řízení dodavatelů, nepodcenit její vytvoření, zajistit její schválení, dodržování, pravidelný přezkum a aktualizaci.

Odstavec 1 písm. a) až c) tohoto ustanovení stanovuje požadavky směřující na všechny dodavatele zboží nebo služeb do stanoveného rozsahu řízení kybernetické bezpečnosti (podle § 12 zákona). Jedná se o povinnost stanovit pravidla pro dodavatele zohledňující systém řízení bezpečnosti informací, seznamovat dodavatele s pravidly, požadovat plnění těchto pravidel a kontinuálně řídit rizika spojená s dodavateli. Řízení rizik spojených s dodavateli není nutné provádět v souladu s § 8 vyhlášky, avšak ani tento způsob není vyloučen. Je ale nutné vyhodnotit rizika, která mohou dodavatelé pro poskytovatele regulované služby znamenat a tato rizika snižovat. Je však nutné mít zvolený přístup k řízení rizik řádně popsán v relevantní bezpečnostní politice či bezpečnostní dokumentaci. Ustanovení dále ukládá povinnost identifikovat a evidovat tzv. významné dodavatele, přičemž kritéria, na jejichž základě má být evidence provedena, jsou stanovena na základě vymezení pojmu významný dodavatel (podle § 2 vyhlášky), kdy významným dodavatelem je ten, kdo poskytovateli regulované služby poskytuje plnění, které je významné z hlediska zajištění kybernetické bezpečnosti regulované služby. Identifikace významného dodavatele je tedy v kompetenci poskytovatele regulované služby. Vždy by však mezi významnými dodavateli měli být např. výrobci řídicích systémů a poskytovatelé služeb spojených se správou ICT.

V souvislosti s významnými dodavateli ustanovení definuje množinu přísnějších požadavků. Je však vhodné připomenout, že poskytovatel regulované služby, se má řídit i všemi povinnostmi z odstavce 1 týkajícího se „běžných“ dodavatelů. Poskytovatel regulované služby, kromě nutné identifikace a vlastní evidence významných dodavatelů, je dále povinen prokazatelně informovat svého významného dodavatele o jeho evidenci. Způsob informování významného dodavatele je upraven náležitostmi prokazatelného informování uvedenými v odstavci 3. Konkrétně se jedná o právní identifikaci poskytovatele regulované služby (např. název společnosti, IČO, adresa sídla či provozovny), informaci o poskytování regulované služby a název regulované služby. Dále musí prokazatelné informování obsahovat právní identifikaci významného dodavatele a informaci o tom, že je daný dodavatel pro poskytovatele regulované služby významný. Od té doby může takto informovaný dodavatel očekávat, že vůči němu budou aplikovány specifické povinnosti vyplývající z ustanovení § 9 odst. 2 vyhlášky. Oproti původnímu znění vyhlášky došlo v následujícím požadavku k věcné změně, díky které následující požadavek již necílí pouze na povinnost provést hodnocení rizik v rámci veřejného

sektoru v rámci výběrového řízení a před uzavřením smlouvy, ale nově cílí také na hodnocení rizik před uzavřením smlouvy u smluv uzavíraných mimo výběrová řízení. V rámci výběrového řízení a před uzavřením smlouvy mimo výběrové řízení je tedy nutné provést hodnocení rizik související s předmětem plnění podle přílohy č. 4 k této vyhlášce a v souvislosti s řízením rizik spojených s významnými dodavateli zajistit, aby právní vztahy uzavírané s významnými dodavateli obsahovaly alespoň relevantní oblasti uvedené v příloze č. 5 k vyhlášce (jedná se o demonstrativní výčet, poskytovatel regulované služby může mít vlastní konkrétní oblasti, které bude vhodné do smluv zapracovat). Pokud významný dodavatel nebude souhlasit s návrhem nebo úpravami smluv, případně za ně bude chtít neúměrně vysoké finanční zdroje, pak je nutné tuto skutečnost zohlednit v rámci hodnocení rizik (např. v analýze rizik, prohlášení o aplikovatelnosti) či v hodnocení rizik souvisejících s plněním smluv, případně v budoucnu při obměně aktiv nastavit pravidla již při zadávacím řízení. Více dopodrobna se této problematice věnuje podpůrný materiál vydaný úřadem nazvaný Průvodce řízením dodavatelů ve vztahu k hodnocení rizik kybernetické bezpečnosti. Další povinností je zajištění pravidelného hodnocení rizik a přezkumu plnění smluv uzavřených s významným dodavatelem. V rámci tohoto hodnocení rizik je mimo jiné nutné zohlednit podle požadavku § 8 odst. 1 písm. c) vyhlášky relevantní hrozby a zranitelnosti a posoudit možné dopady na aktiva, přičemž je nutné vycházet z hodnocení aktiv. Dále je podle ustanovení týkajícího se řízení rizik nutné zohlednit také významné změny a změny stanoveného rozsahu řízení kybernetické bezpečnosti podle § 12 zákona. Při hodnocení rizik souvisejících s výběrovým řízením a hodnocení rizik před uzavřením smlouvy je nutné zohlednit také protiopatření podle § 20 zákona, kybernetické bezpečnostní incidenty, včetně dříve řešených, výsledky auditů kybernetické bezpečnosti a kontrol v oblasti kybernetické bezpečnosti, výsledky penetračního testování a skenování zranitelností a výsledky vyhodnocení účinnosti systému řízení bezpečnosti informací. Poskytovatel regulované služby by v těchto smluvních vztazích měl mít dále možnost kontroly plnění smluv a v neposlední řadě také právo tyto smluvní bezpečnostní požadavky upravovat tak, aby byly vyhovující a reflektovaly současné technologické možnosti a vhodnou úroveň zabezpečení. Ve smysluplných případech je možné povinnost kontroly dodavatelů přenést na třetí stranu (např. na nezávislého auditora). V případě, že poskytovatel regulované služby zjistí v řízení dodavatelů nedostatky, např. na základě výsledků interního auditu kybernetické bezpečnosti, z revize dodavatelských smluv nebo z vyhodnocení veřejné zakázky, je v souladu s odst. 2 písm. d) vyhlášky povinen zajistit jejich řešení.

Na ustanovení o řízení dodavatelů navazuje příloha č. 5 k této vyhlášce, která upřesňuje bezpečnostní opatření pro smluvní vztahy. Nově je v této příloze doplněno ustanovení o povinnosti dodavatele informovat poskytovatele regulované služby o žádosti cizozemského orgánu o zpřístupnění nebo předání dat zpracovávaných na území cizího státu. Výjimkou z výše uvedeného je 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 osoby provozovatele ze zákona a k drobným úpravám s cílem zpřehlednění textu.

K § 10 (Bezpečnost lidských zdrojů)

Nedílnou součástí kybernetické bezpečnosti je také bezpečnost lidských zdrojů, která přímo navazuje na § 4 a § 5 vyhlášky a pojednává zejména o průběžném vzdělávání a udržování

potřebné úrovně bezpečnostního povědomí. Poskytovatel regulované služby vypracuje plán rozvoje bezpečnostního povědomí a v souladu s ním zajišťuje odpovídající vzdělávání, zlepšování bezpečnostního povědomí, včetně formy, obsahu a rozsahu poučení a školení. Součástí plánu rozvoje bezpečnostního povědomí je také podle odst. 2 písm. d) tohoto ustanovení určení pravidel pro tvorbu bezpečných hesel, včetně zpracování relevantních témat uvedených v příloze č. 6 k vyhlášce. Důvodem tohoto bezpečnostního opatření je zejména skutečnost, že velká část kybernetických bezpečnostních incidentů je způsobená vlivem nedostatečného bezpečnostního povědomí uživatelů obecně. Proto se zde cílí nejen na vrcholné vedení, bezpečnostní role a administrátory, ale i na zaměstnance a do určité míry i na jiné zainteresované strany (např. na významné dodavatele).

Ustanovení klade důraz na poučení vrcholného vedení o jeho povinnostech a o bezpečnostní politice, zejména v oblasti systému řízení bezpečnosti informací a řízení rizik. Toto poučení by z důvodu vymahatelnosti a kontroly plnění zákonných požadavků mělo být prokazatelné (přezkoumatelné). Tento požadavek je stanoven proto, aby bylo vrcholné vedení uvedeno do problematiky systému řízení bezpečnosti informací a bylo schopno se na něm aktivně podílet, např. při zpracování analýzy dopadů, hodnocení aktiv a rizik, plánů obnovy nebo manažerském rozhodování o skutečnostech spadajících do oblasti ICT. Důvodem pro explicitní přidání tohoto požadavku je důraz, který klade na vrcholné vedení směrnice NIS 2. Nicméně vrcholné vedení by vždy mělo být minimálně v pozici uživatelů a samotná povinnost školit uživatele byla stanovena již původní vyhláškou, nejedná se tedy o zcela novou povinnost.

Ustanovení vyžaduje řádné poučení uživatelů, administrátorů, bezpečnostních rolí a dodavatelů o povinnostech a o bezpečnostní politice související s regulovanou službou. Ta by měla odpovídat povaze a rozsahu přístupu, který budou mít předmětné lidské zdroje k aktivům regulované služby. Toto poučení by z důvodu vymahatelnosti a kontroly plnění zákonných požadavků mělo být prokazatelné (přezkoumatelné).

Dále je požadováno školení uživatelů, administrátorů a osob zastávajících bezpečnostní role v oblasti kybernetické bezpečnosti. Školení by mělo odpovídat cílové skupině (mělo by být zohledněno, zda se jedná např. pouze o uživatele nebo o osobu zastávající bezpečnostní roli), zároveň školení musí korespondovat s plánem rozvoje bezpečnostního povědomí. Způsob provádění školení, ani cyklus pro jeho opakování není touto vyhláškou upraven. Měl by však 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 pro zajištění tohoto bezpečnostního opatření je efektivita takového školení. O poučení a absolvovaných školeních je nutné vést přehledy, součástí kterých je předmět poučení nebo školení, a dále seznam osob, které dané poučení nebo školení absolvovaly.

Plán rozvoje bezpečnostního povědomí plní roli nástroje pro plánování výše uvedených školení, poučení zaměstnanců a zainteresovaných stran. Z toho důvodu má poskytovatel regulované služby povinnost plán rozvoje bezpečnostního povědomí udržovat v aktuálním stavu, pravidelně jej vyhodnocovat a kontrolovat jeho dodržování a dále určit osoby, které budou odpovědné za realizaci jednotlivých činností, které jsou v plánu uvedeny. Plán musí být optimalizován tak, aby odrážel aktuální potřeby poskytovatele regulované služby a definoval pravidla a postupy pro řešení případů jeho porušení. Další často podceňovanou povinností je mít definován postup a pravidla pro případ ukončení smluvního vztahu s administrátorem nebo osobou zastávající bezpečnostní roli (tzv. problematika předání odpovědnosti).

Toto ustanovení dále vyžaduje kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role. V praxi se může jednat např. o pravidlo

čistého stolu (zákaz uchovávání citlivých dat, jako např. heslo, viditelně na pracovním stole) nebo provádění phishingových kampaní.

Součástí oblasti bezpečnosti lidských zdrojů je i řízení životního cyklu zaměstnance (nástup do pracovního poměru, případná změna pracovního zařazení, ukončení pracovního poměru) a 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). Dále je ve vyhlášce stanovena povinnost určit osoby odpovědné za realizaci jednotlivých činností, které jsou v plánu rozvoje bezpečnostního povědomí, aby byla jasně vymezena odpovědnost za plnění dílčích činností, což by mělo přispět ke zvyšování bezpečnosti lidských zdrojů.

Úřad si je plně vědom skutečnosti, že řádně informovaný, pravidelně a efektivně proškolený uživatel je jedním z nejefektivnějších způsobů, jak eliminovat z pohledu kybernetické bezpečnosti rizikové chování uživatele, které může mít velmi rychle přímý nežádoucí dopad na celou organizaci. Proto byla vytvořena nová příloha č. 6 k této vyhlášce, 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 zneužitím interních lidských zdrojů.

K § 11 (Řízení změn)

Řízení změn je z hlediska zajištění bezpečnosti, a především kontinuity činností jedním z klíčových procesů. Ustanovení v této oblasti vychází z nejlepší praxe a ze zkušeností úřadu a vymezuje základní požadavek na řízení změn a s tím spojené přezkoumání možných dopadů pro všechny změny přímo i nepřímo související s kybernetickou bezpečností regulované služby. Poskytovatel regulované služby si sám musí stanovit závazná pravidla, postupy a kritéria pro určení vyznaných změn postupem podle odst. 1 písm. a). Cílem je, aby byly určeny změny, které mají nebo mohou mít vliv na kybernetickou bezpečnost a poskytovatel regulované služby jim věnoval adekvátní pozornost. Zda se v případě dílčí změny, která má nebo může mít vliv na kybernetickou bezpečnost jedná o významnou změnu nebo nikoliv, posuzuje sám poskytovatel regulované služby na základě pravidel, postupů a kritérií, které si sám stanoví. S ohledem na performativnost tohoto pravidla, by poskytovatel regulované služby neměl ve vlastním zájmu podceňovat důležitost řízení změn pro zachování kontinuity činností, a tím pádem i důležitost samotné kybernetické bezpečnosti regulované služby.

V případě, že je daná změna označena jako významná, je nutné celý proces řízení této změny dokumentovat. V rámci přístupu k významným změnám pak musí být provedeno hodnocení rizik souvisejících s významnou změnou a z výsledků hodnocení rizik přijata bezpečnostní opatření minimalizující možné negativní dopady změn. Řízení rizik v souvislosti s významnou změnou nemusí být nutně provedeno podle § 8 vyhlášky. Je na poskytovali regulované služby, jakým způsobem posoudí rizika, která jsou s danou významnou změnou spojena, nicméně je nutné, aby byl tento způsob pro poskytovatele regulované služby smysluplný a aby byl popsán v relevantní bezpečnostní politice či bezpečnostní dokumentaci. Na základě potřeb poskytovatele regulované služby 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 realizované změny navrátit do původního stavu.

Poskytovatel regulované služby má dále na základě hodnocení rizik rozhodnout o potřebě provedení penetračního testování, které by mělo být zacíleno především na aktiva dotčená významnou změnou. Penetrační testování je prováděno mj. v souladu s § 24 vyhlášky.

Na základě zkušeností z kontrolní činnosti úřadu byla tato oblast identifikována jako problematická, a proto došlo k úpravám ustanovení, které měly za cíl tuto oblast zpřehlednit. Zejména se jedná o přeformulování odstavce 1. Tento odstavec je nyní pro poskytovatele regulované služby návodnější a popisuje nastavení procesu řízení změn. Požadavek je postaven na tom, že si poskytovatel regulované služby stanoví a zformalizuje proces řízení změn. Oblast řízení změn je omezena pouze na změny, které mohou mít vliv na kybernetickou bezpečnost a nezahrnuje tedy všechny změny v organizaci, např. provozního charakteru. V praxi je řízení změn, tzv. „change management“, často postaveno na mezinárodně uznávané knihovně ITIL, podle které je žádoucí řídit všechny změny, nicméně z důvodu snížení zatížení poskytovatelů regulované služby jsou v této vyhlášce zdůrazněny pouze ty změny, které se týkají oblasti kybernetické bezpečnosti. Poskytovatel regulované služby by tedy měl stanovit proces určení všech změn, které mají nebo mohou mít vliv na kybernetickou bezpečnost. Zároveň musí disponovat pravidly, postupy a kritérii pro určení významných změn. Rozhodnutí o tom, zdali změna spadá do kategorie významných změn je provedeno na základě výše zmíněných pravidel, postupů a kritérií, které si poskytovatel regulované služby stanovil v bezpečnostní politice či bezpečnostní dokumentaci. Povinnosti spojené s významnými změnami zůstaly ve vyhlášce zachovány.

K § 12 (Akvizice, vývoj a údržba)

V oblasti rozvoje a vývoje aktiv regulované služby je nutné, aby byl rozvoj regulované služby vymezen konkrétními požadavky na zajištění její bezpečnosti, jež je nedílnou součástí rozvojových aktivit. Následně, po definování bezpečnostních požadavků, je nezbytné jejich promítnutí do celého životního cyklu, od vlastního vývoje až do provozního využití dané služby nebo její části. Jedná se o prosazování principů nejlepší praxe „secure by design“ a „secure by default“. Při vytváření těchto bezpečnostních požadavků je také na místě přihlížet k aktuálnímu dění v oblasti kybernetické bezpečnosti jako např. k aktuálním trendům mezi útoky, které útočníci využívají. Součástí těchto požadavků je řízení rizik z důvodu nalezení možných negativních dopadů a navržení případných bezpečnostních opatření ke zmírnění těchto dopadů. Řízení rizik je možné provést způsobem, který si poskytovatel regulované služby stanoví, nicméně je možné řídit se § 8 vyhlášky. V obou případech je však nutné mít proces řízení rizik řádně popsán. V souvislosti s plánovanou akvizicí, vývojem nebo údržbou je dále nutné řídit významné změny podle § 11 vyhlášky a plnit všechny náležitosti, které vyhláška v této oblasti požaduje.

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 plynoucím z principů nulové důvěry tzv. „zero-trust“ a „secure by design“. Dále je zapotřebí uvést, že tento požadavek je důvodně obecný, protože s ohledem na konkrétní řízení rizik poskytovatele regulované služby může být oddělení prostředí uchopeno např. v rámci komunikační sítě pouze pomocí firewallu, jindy může poskytovatel regulované služby naznat, že je zapotřebí dané prostředí oddělit do tzv. ostrovního režimu (třeba galvanicky), jindy bude stačit pouze v rámci aplikační vrstvy mít jen jiný virtualizovaný modul. Současně požadavek stanovuje povinnost zajistit ochranu informací a dat, které se v nich vyskytují. Tato část může být např. u vývojového nebo testovacího prostředí řešena pomocí anonymizace informací a dat sloužících k vývoji nebo testování, šifrováním informacích a dat (nebo podepisováním a šifrováním dílčích částí kódu či v rámci aplikačních balíčků) při přenosu mezi prostředími nebo v nich uložených.

Oproti původní vyhlášce byl upřesněn požadavek na stanovení bezpečnostních požadavků tak, aby bylo zřejmé, že se mimo specifické požadavky vztahující se k dané akvizici, vývoji nebo údržbě jedná také o relevantní požadavky této vyhlášky (např. řízení změn, řízení aktiv nebo relevantní technická bezpečnostní opatření). Dále byl doplněn požadavek na oddělení prostředí jako jsou provozní a zálohovací nebo jiná specifická prostředí, která nově vyhláška dále zmiňuje, např. v § 18, 26 a požadavek na aktuálnost kryptografických algoritmů v rámci nových projektů akvizice a vývoje podle § 25 vyhlášky.

V neposlední řadě je v tomto ustanovení zohledněn požadavek vůči potenciálním akvizicím a vývoji technických aktiv, kdy je kladen důraz na vícefaktorovou autentizaci. Tyto požadavky jsou zde uvedeny na základě potřeby a kladení 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 na základě potřeby dlouhodobé udržitelnosti pořizovaných technických aktiv, kdy je žádoucí zohlednit i budoucí potřeby rozvoje v této oblasti a např. zvyšování technické náročnosti na dané technické aktivum (související s potřebou používání delších kryptografických klíčů). Je tedy na místě zohledňovat v projektech akvizice a vývoje to, aby byly vyžadovány kryptografické algoritmy, které úřad 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 rozvedena v jejich dílčích ustanoveních. V neposlední řadě je na místě již při akvizici nebo vývoji technického aktiva řešit otázku bezpečnostních aktualizací, která je zpravidla závislá na konkrétním dodavateli, který se zavazuje k tomu, že pro dané technické aktivum bude do určité doby vydávat tyto aktualizace a ošetřovat tak zjištěné zranitelnosti. V praxi se jedná o tzv. podporu nebo anglicky „support“ daného technického aktiva. V případě, že již není možné zajistit tuto podporu a získávat tak bezpečnostní aktualizace, je potřebné zajistit v rámci akvizice náhradu za tato již zranitelná technická aktiva, tedy dostatečně s předstihem plánovat finanční zdroje a investice na akvizici technických aktiv.

K § 13 (Řízení přístupu)

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

V souladu s nejlepší praxí (např. normou ISO/IEC 27002) musí být přístupová práva a oprávnění uživatelům a administrátorům přistupujícím k aktivům přidělována pouze v rozsahu nezbytném pro výkon činností vyplývajících z jejich popisu pracovního místa nebo smluvního ujednání. Důležité je z tohoto pravidla neudělovat neopodstatněné výjimky a případné výjimky řádně řídit. Tato práva by měla být řízena na základě skupin nebo rolí z důvodu jejich přehlednějšího řízení, revize a přezkoumatelnosti. V případě udělení výjimky musí být každému uživateli a administrátorovi přidělen jedinečný identifikátor z důvodu jednoznačného stanovení vykonavatele činnosti. Výjimku z tohoto pravidla mohou tvořit tzv. sdílené technické účty, avšak jejich použití by mělo podléhat přísnému nastavení interních pravidel a mělo by být možné jen ve zcela výjimečných a řízených případech. Samozřejmostí by mělo být tento stav náležitě zohlednit v rámci hodnocení rizik, uvést v prohlášení o aplikovatelnosti, případně zvážit zavedení jiného přiměřeného bezpečnostního opatření (např. dohled kamerového systému).

Oproti původní vyhlášce toto ustanovení explicitně uvádí požadavek na oddělení uživatelských a administrátorských účtů jedné osoby, tedy aby jedna osoba disponovala jak uživatelským účtem pro běžné činnosti (např. pro vyřizování e-mailů a běžné agendy), tak odděleným

administrátorským účtem pro výkon takových činností, kdy je nezbytné disponovat vyššími oprávněními (např. správa technických aktiv). Oddělení uživatelského a administrátorského účtu jednoho uživatele v souladu s nejlepší praxí snižuje např. riziko kompromitace sítě v případě zneužití jeho identity, kdy dojde ke kompromitaci uživatelského účtu, zatímco u privilegovaného účtu též osoby je z důvodu oddělení od uživatelského účtu snížena šance zneužití administrátorských oprávnění. Poskytovatel regulované služby může v rámci řízení přístupu využít např. nástroje typu PAM. Kumulace oprávnění v rámci jednoho účtu stále představuje riziko, a to např. v případě kompromitace privilegovaného účtu z důvodu využívání takového účtu pro běžnou agendu (např. čtení e-mailů), při které může uživatel neúmyslně kompromitovat tento účet (např. otevřením phishingového e-mailu).

V rámci řízení přístupu technických aktiv musí být řízeny identifikátory, přístupová práva a oprávnění účtů těchto technických aktiv a v souladu s politikou řízení přístupu jsou přidělována a odebírána. Obdobně vůči uživatelským a administrátorským účtům musí být zaváděna bezpečnostní opatření pro řízení přístupů technických aktiv, která jsou v praxi často opomíjena a dochází např. ke zneužití účtů technických aktiv, služeb nebo aplikací, jelikož mívají udělena vysoká oprávnění a nejsou tolik monitorována (např. u nich nejsou zavedena všechna pravidla heslové politiky, jsou využívána výchozí hesla a nejsou logovány jejich přístupy).

Důležité je rovněž neopomíjet mobilní zařízení a obdobná technická aktiva a zavádět bezpečnostní opatření pro jejich bezpečné používání. Může se jednat např. o centralizovanou správu těchto zařízení známou jako tzv. MDM. V případě, že se v rámci organizace využívají technická aktiva, která nemá poskytovatel regulované služby ve své správě (tzv. BYOD), je nezbytné přijmout vhodná bezpečnostní opatření spojená s jejich využíváním (např. tato zařízení umístit do jiného síťové segmentu nebo technicky vynucovat po uživatelích jejich pravidelnou aktualizaci). Součástí řízení přístupů je také omezení a kontrola používání programových prostředků a vybavení, které mohou překonat systémové nebo aplikační kontroly. V praxi se jedná např. o omezení nebo kontrolu připojovaných datových nosičů prostřednictvím USB, externích zařízení ke koncovým stanicím (např. klávesnice, myši, Wi-Fi adaptéry), spouštění aplikací, které nevyžadují instalaci (v případě zavedené správy nainstalovaných aplikací) a další potenciální vektory útoku, kterých by útočník mohl zneužít za překonání běžných bezpečnostních opatření.

Nezbytná je i pravidelná kontrola veškerých přístupových práv a oprávnění (včetně rozdělení do skupin a rolí) a odebírání nebo změna těchto práv a oprávnění při změně pracovní pozice nebo zařazení uživatelů, administrátorů nebo osob zastávajících bezpečnostní role. Obdobný požadavek je i v případě ukončení nebo změny smluvního vztahu. V tomto případě to je požadavek na deaktivaci daného účtu a odebrání či změnu přístupových práv a oprávnění. Není na místě uživatelské účty kompletně odebírat z důvodu možnosti zpětného přezkumu, ale je vhodné je pouze deaktivovat a odebrat či změnit jejich přístupová práva a oprávnění. Je tak prakticky zamezeno dalšímu užívání daného uživatelského účtu a zároveň lze dohledávat informace např. v bezpečnostních záznamech o událostech vůči tomuto účtu. V oblasti přezkumu řízení přístupu je v tomto ohledu dále nezbytné i řádně dokumentovat přidělování a odebírání přístupových práv a oprávnění, jelikož je nutné mít doložitelné informace o tom, kdo (případně i co, v případě technického aktiva) a v jakém časovém období měl přístup k jakým aktivům a mohl je ovlivnit.

V rámci této oblasti dále došlo především k drobným textovým úpravám z důvodu zvýšení přehlednosti. Nově byl doplněn požadavek „bezodkladné“ odebírání nebo změnu přístupových oprávnění při změně pozice nebo zařazení na základě skupin a rolí a při ukončení nebo změně smluvního vztahu.

V neposlední řadě je v rámci tohoto ustanovení uvedena provazba na relevantní technická bezpečnostní opatření a nástroje v § 19 a 20 v zájmu zpřehlednění vyhlášky, kdy při vynucování bezpečnostních opatření z tohoto ustanovení o řízení přístupu bude v praxi na místě zároveň užívat nástroje uvedené v těchto technických bezpečnostních opatřeních a zohledňovat požadavky na ně kladené.

K § 14 (Zvládání kybernetických bezpečnostních událostí a incidentů)

V této oblasti zůstávají povinnosti podle vyhlášky stejné a došlo pouze k drobným textovým úpravám z důvodu zvýšení přehlednosti.

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. Nastavení těchto procesů, včetně stanovení odpovědností, má významný vliv na kybernetickou bezpečnost, zejména na včasné odhalení kybernetického bezpečnostního incidentu i na jeho zvládání. Pro stanovení odpovědností lze využít matice odpovědnosti (např. RACI matice nebo eskalační matice). V rámci nastavení procesu zvládání kybernetických bezpečnostních incidentů je nutné definovat a dodržovat také pravidla a postupy pro identifikaci, sběr a uchování věrohodných podkladů, které jsou potřebné pro následnou analýzu kybernetického bezpečnostního incidentu.

Poskytovatel regulované služby je dále povinen zajistit, že uživatelé, administrátoři, osoby zastávající bezpečnostní role, zaměstnanci a dodavatelé budou oznamovat neobvyklé chování technických aktiv a podezření na jakékoliv zranitelnosti. V této věci je nutné stanovit postupy pro hlášení těchto událostí a je vhodné tuto problematiku zařadit do pravidelných školení prováděných v rámci § 10 vyhlášky.

Nedílnou součástí těchto procesů je posuzování kybernetických bezpečnostních událostí, při kterém musí být rozhodnuto, zda se jedná o kybernetické bezpečnostní incidenty, tedy povinnost rozlišovat kybernetické bezpečnostní události a incidenty. Rozhodování o klasifikaci kybernetických bezpečnostních událostí a incidentů je prováděno na základě dostupných informací při jejich detekci, avšak při zjištění nových informací je nutné provést znovu posouzení a případnou reklasifikaci.

Za účelem komplexnosti povinností souvisejících se zvládáním kybernetických bezpečnostních událostí a incidentů odkazuje písmeno j) tohoto ustanovení na § 15 zákona upravující hlášení kybernetických bezpečnostních incidentů.

Poskytovatel regulované služby vede o kybernetických bezpečnostních incidentech a jejich zvládání záznamy. Formu vedení těchto záznamů vyhláška neupravuje. V praxi se zpravidla jedná o elektronickou evidenci vytvořenou pomocí běžných kancelářských aplikací nebo evidenci v tiketovacích nástrojích.

Za účelem zamezení opakování stejného nebo obdobného kybernetického bezpečnostního incidentu stanovuje písmeno n) tohoto ustanovení povinnost vyhodnocení účinnosti řešení již vyřešeného kybernetického bezpečnostního incidentu, tedy přezkum toho, zda přijatá bezpečnostní opatření zafungovala tak, jak byla zamýšlena a jsou tedy dostačující. Na základě tohoto vyhodnocení poskytovatel regulované služby stanoví nutná bezpečnostní opatření, příp. aktualizuje stávající bezpečnostní opatření. Jedná se tedy o prosazování principu tzv. lessons learned.

Odstavec 2 tohoto ustanovení uvádí, jaké nástroje poskytovatel regulované služby při detekci a vyhodnocování používá, ty jsou blíže popsány v § 21 a 23 této vyhlášky.

K § 15 (Řízení kontinuity činností)

Bezpečnostní opatření v oblasti řízení kontinuity činností cílí na schopnost organizace rychle a účinně reagovat na úmyslné a neúmyslné kybernetické bezpečnostní incidenty (např. sabotáž nebo přírodní katastrofy). V případě nepřipravenosti na takové situace by hrozilo úplné nebo částečné přerušení poskytování regulované služby na nepřijatelně dlouhou dobu. Základem řízení kontinuity činností je stanovená politika řízení kontinuity činností, která nastavuje základní procesy, práva a povinnosti k naplnění stanovených cílů řízení kontinuity činností. V této vyhlášce došlo ke spojení dvou písmen původní vyhlášky, konkrétně písmen a) a d), jelikož práva a povinnosti administrátorů a osob zastávajících bezpečnostní role jsou definovány v politice řízení kontinuity činností. Stanovení metodiky pro provedení analýzy dopadů bylo v původní vyhlášce ustanoveno v příloze č. 5, konkrétně v bodě 1.23. písm. d). Vytvořením samostatného písmena v § 15 tak došlo pouze k zpřehlednění, nikoliv k vytvoření nové povinnosti.

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

Výstupy analýzy dopadů a hodnocení rizik slouží jako podklad 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 poskytovatel regulované služby schopen obnovit produkty, služby, činnosti a zdroje do předem definované minimální úrovně např. po kybernetickém bezpečnostním incidentu nebo po selhání technického aktiva. Konkrétně se zde jedná o časový údaj, za který má být poskytovatel regulované služby schopen 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 poskytovatel regulované služby přijít. Stanovení cílů kontinuity činností je důležité pro celou oblast řízení kontinuity činností, protože tyto cíle se dále promítají do politiky řízení kontinuity činností, plánů kontinuity činností a plánů obnovy.

K naplnění cílů a politiky řízení kontinuity činností je v písmeně e) stanovena povinnost vypracovat plány kontinuity činností a plány obnovy. Zmíněné plány je nutné aktualizovat a pravidelně testovat, aby byly v případě mimořádné situace, která vyžaduje jejich aktivaci, využitelné a zainteresované osoby znaly své pravomoci, odpovědnosti a povinnosti a celý proces fungoval bez časových průtahů, které by mohly mít negativní dopad na celou situaci a její zvládání.

Ustanovení dále odkazuje na implementaci bezpečnostních opatření, která slouží ke zvýšení odolnosti a zajištění dostupnosti regulované služby v souladu s § 26.

V původní vyhlášce byly používány pojmy plány kontinuity činností a havarijní plány. Věcně a obsahově zůstávají plány v této vyhlášce stejné jako tomu bylo v původní vyhlášce. Došlo pouze k jejich přejmenování na plány obnovy, a to z toho důvodu, že havarijní plány byly zaměňovány s havarijními plány podle jiné legislativy platné v České republice (např. havarijní plány Hasičského záchranného sboru České republiky, havarijní plány podle zákona č. 224/2015 Sb., zákona č. 239/2015 Sb., vyhlášky č. 422/2016 Sb., vyhláška 450/20058 Sb.). Rovněž tímto přejmenováním došlo ke sjednocení terminologie směrem k běžné praxi v oblasti

informačních technologií, kde je pojem plány obnovy standardně používán. Těmito úpravami nevznikají žádné nové povinnosti, jen došlo k jejich upřesnění a zpřehlednění.

K § 16 (Provádění auditu kybernetické bezpečnosti)

V rámci požadavků v oblasti auditu kybernetické bezpečnosti je zahrnuto provádění pravidelné kontroly dodržování bezpečnostní politiky a bezpečnostní dokumentace, 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 neustálého zlepšování, který vychází z norem řady ISO/IEC 27000.

Z hlediska posuzování souladu s příslušnou regulací je vyžadováno, aby poskytovatel regulované služby identifikoval veškerou relevantní regulaci z hlediska kybernetické bezpečnosti a zajistil kontrolu jejího dodržování v praxi. Mimo posuzování souladu s příslušnou regulací je nutné také ověřit soulad s dalšími právními předpisy, vnitřními předpisy, smluvními závazky.

Požadavek na přezkoumání technické shody cílí na kontrolu zavedených technických bezpečnostních opatření. V praxi to znamená, že auditor kybernetické bezpečnosti 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 bezpečnostní 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 provádění auditu kybernetické bezpečnosti běžně používány z toho důvodu, aby byla organizace schopna lépe plánovat svoji činnost v průběhu roku.

Dále došlo ke zpřehlednění povinností souvisejících s auditem kybernetické bezpečnosti. Tyto povinnosti byly v původní vyhlášce popsány v odstavci 1 a nově se stejným povinnostem věnuje odstavec 2 a 3 této vyhlášky. Odstavec 2 písm. a) klade důraz na posouzení souladu se zákonem a vyhláškou, nicméně věcně se povinnosti shodují s původní vyhláškou a nové povinnosti nepřibyly. Cílem odstavce 3 je zpřehlednit, kde mají být výsledky auditu kybernetické bezpečnosti zohledněny, což bylo rovněž zakotveno i v původní vyhlášce. Povinnost zahrnout výsledky auditu kybernetické bezpečnosti do plánu rozvoje bezpečnostního povědomí a řízení rizik vyplývá z principu fungování této vyhlášky, nejedná se tedy o novou povinnost, pouze o snahu o zpřehlednění a upozornění na další souvislosti. Toto ustanovení dále cílí na povinnost stanovení případných nápravných opatření, čímž rovněž nedefinuje žádnou novou povinnost.

Jedním z důvodů pro provádění auditu kybernetické bezpečnosti je neustálé zlepšování úrovně kybernetické bezpečnosti a nápravná opatření jsou toho nezbytnou součástí. Audit kybernetické bezpečnosti má probíhat při významných změnách a v rámci jejich rozsahu. To znamená, že jeho předmětem mají být významné změny určené podle § 11 a oblasti, které jsou těmito změnami přímo dotčeny. Dále má být audit kybernetické bezpečnosti prováděn v pravidelných intervalech alespoň jednou za dva roky, kdy musí pokrýt celý rozsah požadavků vyplývajících z této vyhlášky a relevantních požadavků zákona a v souladu se stanoveným plánem auditu kybernetické bezpečnosti. Tento požadavek vychází z 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 dvou let (zejména z důvodu časové náročnosti), je možné audit systematicky rozdělit na dílčí části. Takovýto postup je nutné řádně zdůvodnit např. v prohlášení o aplikovatelnosti a postupovat tak, aby po ukončení všech dílčích částí auditu byl výsledkem audit kybernetické bezpečnosti, který pokryje celý rozsah požadavků této vyhlášky a zákona, nejpozději v pětiletém intervalu.

Audit kybernetické bezpečnosti musí být prováděn nestrannou osobou, která splňuje požadavky na roli auditora kybernetické bezpečnosti a je schopna nezávisle zhodnotit skutečný stav organizace v oblasti kybernetické bezpečnosti a účinnost zavedených bezpečnostních opatření, díky čemuž zůstane zachován princip neustálého zlepšování systému řízení bezpečnosti informací. V praxi to tedy znamená, že audit kybernetické bezpečnosti nemůže provádět osoba pověřená výkonem jiné bezpečnostní role nebo která se např. podílí na provozu. Požadavky na osobu auditora kybernetické bezpečnosti jsou pak přehledně uvedeny v § 5 odst. 4 vyhlášky.

K § 17 (Fyzická bezpečnost)

V rámci tohoto ustanovení má poskytovatel regulované služby nastavit postupy a pravidla, kterými bude komplexně chránit aktiva z hlediska fyzické bezpečnosti a kontinuitu regulované služby. Účelem bezpečnostních opatření zaměřených na zajištění fyzické bezpečnosti je předcházení negativním vlivům na aktiva ve fyzickém světě. Oproti technickým opatřením, která ve vyhlášce následují a jsou zaměřena převážně na zabezpečení v oblasti informačních technologií, je cílem tohoto bezpečnostního opatření zabezpečit často opomíjené aspekty kybernetické bezpečnosti před fyzickým poškozením, krádeží nebo odcizením, neoprávněným zásahům, zneužitím nebo obecným narušením bezpečnosti poskytování regulované služby. Fyzická bezpečnost je poskytovateli regulované služby často přehlížena, přestože fyzické poškození aktiv regulované služby je často jeden z nejsnazších způsobů, jakým může útočník bez odbornějších znalostí narušit zejména dostupnost regulované služby. Pro tyto účely je nutné stanovit fyzický bezpečnostní perimetr nebo perimetry (někdy označovány jako zóny) a s ohledem na hodnocení aktiv v nich umístěných rozdělit jejich úrovně fyzické ochrany (např. primární serverovna organizace může disponovat přísnějším dohledem než kancelář zaměstnance, který nemá přístup k regulované službě). V rámci jednotlivých úrovní fyzického bezpečnostního perimetru musí být tato pravidla prosazována a dodržována, musí být přijaty relevantní prostředky fyzické bezpečnosti a zavedena adekvátní bezpečnostní opatření, kterými bude fyzická bezpečnost zajištěna. Takto určené bezpečnostní perimetry a jejich úrovně fyzické ochrany je nutné náležitě dokumentovat. Prostředky fyzické bezpečnosti se rozumí např. mechanické zábranné prostředky, kamerové systémy, zařízení elektrické zabezpečovací signalizace, prostředky omezující působení požárů, prostředky omezující působení projevů živelních událostí nebo systémy pro kontrolu a evidenci vstupu. Součástí fyzické bezpečnosti je také zvážení všech bezpečnostních aspektů jednotlivých lokalit a objektů, ve kterých je regulovaná služba provozována. Je klíčové si uvědomit, že k zajišťování bezpečnosti regulované služby je nutné přistupovat komplexně a že bez dostatečného fyzického zabezpečení aktiv může být mnohdy zbytečné investovat do zabezpečení např. na aplikační úrovni v rámci ISO/OSI modelu.

K § 18 (Bezpečnost komunikačních sítí)

Součástí zajištění kybernetické bezpečnosti aktiv je 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 nejlepší praxe (např. normy 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. provozní, zálohovací, vývojová, testovací, administrátorská a jiná specifická prostředí. 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). Je také zapotřebí, aby veškerá segmentace byla řádně zdokumentována, čímž poskytovatel regulované služby získá ucelený pohled na svou síťovou infrastrukturu (např. v rámci evidence v IP plánech nebo v rámci síťové topologie). Způsob provedení segmentace je v gesci poskytovatele regulované služby, který zajistí, aby komunikace byla adekvátně řízena mezi jednotlivými segmenty v rámci interní komunikační sítě nebo jejím perimetru (příp. s externí komunikační sítí) a současně také i mezi jednotlivými prostředími komunikační sítě.

Vzdálený přístup (např. VPN připojení do interní komunikační sítě), vzdálená správa technických aktiv (např. prostřednictvím vzdálené plochy nebo terminálového připojení na serveru) a komunikace v rámci komunikační sítě 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 nebo zakázání neřízené komunikace je nejlepší praxe v oblasti bezpečnosti komunikačních sítí a ověřenou cestou pro dosažení základní úrovně síťové bezpečnosti. Slouží tak např. ke zvýšení úrovně kybernetické bezpečnosti u poskytovatele regulované služby, jelikož dochází k omezení případného šíření nebezpečného kódu nebo pohybu případného útočníka v interní komunikační síti v případě její kompromitace.

Obdobně je zapotřebí, aby komunikace poskytovatele regulované služby zejména v rámci vzdáleného přístupu a vzdálené správy technických aktiv byla časově omezena a bylo zajištěno, že dojde k opětovnému ověření identit administrátorů a uživatelů před opětovným navázáním komunikace. Tento požadavek více přibližuje koncept nulové důvěry neboli „zero-trust“, jelikož snižuje riziko zneužití aktivního spojení případným útočníkem. Jedná se také např. o běžnou praxi využívanou v rámci řízení vzdálené komunikace dodavatelských účtů.

Oproti původní vyhlášce byl z tohoto paragrafu vypuštěn požadavek na aktivní blokování nežádoucí komunikace, jelikož je tento požadavek již zahrnut v § 21 odst. 1 písm. c) této vyhlášky.

Kryptografickými algoritmy k zajištění důvěrnosti a integrity jsou myšleny především různé zabezpečené protokoly nebo šifrování síťové komunikace (např. aktuální odolná verze protokolu TLS a v nich používané kryptografické algoritmy). Tyto algoritmy současně upravuje požadavek § 25 této vyhlášky. 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 např. připojení potenciálního útočníka.

V neposlední řadě, poskytovatel regulované služby pro zajištění bezpečnosti své komunikační sítě a infrastruktury potřebuje mít přehled nad její architekturou. K tomu se typicky využívá topologie, která zaznamenává danou komunikační síť nebo infrastrukturu. Topologii lze vytvořit v různých pohledech a různých úrovních, kdy záleží na kontextu a potřebách organizace, jaký typ topologie komunikační sítě a infrastruktury představuje dostatečný detail, aby zajistila zmíněný přehled o propojení technických aktiv.

K § 19 (Správa a ověřování identit)

Požadavky tohoto ustanovení stanovují minimální úroveň pro správu a ověření identit, které by měli poskytovatelé regulovaných služeb prosazovat. Tento paragraf vychází zejména z kontrolní a metodické činnosti úřadu, partnerských organizací, standardů publikovaných organizací NIST (např. 800-63B) a nejlepší praxe v oblasti kryptografie a zabezpečení správy a ověřování identit.

U nástroje pro ověření identity (uživatelů, administrátorů a technických aktiv) je mimo ty zřejmé (dnes již standardní požadavky jako ověření identity nebo řízení možných pokusů o přihlášení) stanoven i požadavek na odolnost ukládaných autentizačních údajů, přičemž tento požadavek míří mimo jiné i na tzv. odolnost proti off-line útokům. Tento požadavek byl stanoven již v původní vyhlášce a nejedná se tedy o zavádění nové povinnosti. 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 hashovacích funkcí) se potenciální útočník rovnou dostane ke konkrétním heslům k jednotlivým účtům. Z těchto důvodů je ve vyhlášce uveden požadavek vedoucí k zajištění odolnosti ukládaných a přenášených autentizačních údajů, tedy aby tyto údaje byly zašifrovány dostatečně silnou šifrou (aktuálně odolnou kryptografií). Útočník, i když odcizí tuto databázi hesel, se dostane pouze k zašifrovaným údajům. Tento požadavek významným způsobem zvyšuje zabezpečení autentizačních údajů.

Dalším požadavkem je opětovné ověření identity po stanovené době nečinnosti, které reflektuje problém trvale přihlášených uživatelských nebo administrátorských účtů, které potenciální útočník může v případě jejich nevynuceného odhlášení kompromitovat a zneužít např. prostřednictvím ukradení relace daného uživatele. Dále je také nutné dodržovat důvěrnost při vytváření výchozích nebo obnovovacích přihlašovacích údajů, kdy není na místě sdílet důvěrná hesla prostřednictvím komunikačních kanálů, ze kterých může potenciální útočník odposlechnout komunikaci nebo je možné přečíst heslo v jeho otevřené podobě. V neposlední řadě má nástroj na správu a ověřování identit zajišťovat tuto správu centralizovaně s ohledem na vazby mezi aktivy. Není požadováno ve všech případech mít centralizovanou správu identit na úrovni celé organizace, ale je nutné mít centralizovanou správu identit s ohledem na vazby mezi aktivy např. potřebnými k poskytování určité regulované služby, pokud poskytovatel regulované služby těchto služeb poskytuje více. Není tedy nutné disponovat jednou centralizovanou správou pro vícero regulovaných služeb, pokud spolu tyto služby nesouvisí, nesdílí aktiva a řízení jejich identit dohromady by naopak bylo kontraproduktivní.

Z pohledu kybernetické 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 je založený na vícefaktorové autentizaci s nejméně dvěma různými typy faktorů. Tento způsob doporučuje také standard NIST 800-63B. 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 s vícefaktorovou autentizací nepovažuje za bezpečný např. také z pohledu možné kompromitace nebo úniku hesel. V případě vícefaktorové (např. dvoufaktorového) autentizace by daná entita, která se autentizuje vůči technickým aktivům, musela znát např. PIN nebo heslo a dále by musela pro úspěšnou autentizaci mít k dispozici i druhý faktor, např. OTP token nebo biometrický údaj. U technických aktiv, která jsou již v provozu a jsou např. nějakým způsobem v tomto ohledu omezena, může být pořízení a implementace tohoto způsobu autentizace náročnější. Dále je možné využít autentizační mechanismus založený na aktuálně odolné kontinuální autentizaci, která je založena na modelu nulové důvěry tzv. „zero-trust“. Podstatou tohoto autentizačního mechanismu je, že identita uživatele není ověřena pouze při

prvotní interakci se systémem, nýbrž dochází k neustálému ověřování identity uživatele např. na základě biometrických údajů v kombinaci s monitorováním jeho interakce se systémem (např. údery na klávesnici nebo pohyb myši). Využití kontinuálního autentizačního mechanismu tak může dále snížit rizika např. kompromitace regulované služby v případech, kdy by potenciální útočník dokázal překonat autentizační mechanismus sloužící pro prvotní ověření identity.

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

V případě, kdy není možné požadavek na vícefaktorovou autentizaci naplnit např. z důvodu velikosti organizace a nutnosti rozsáhlého projektu nebo přílišné specifičnosti technických aktiv, musí nástroj pro ověřování identity uživatelů, administrátorů a aplikací využívat alespoň autentizaci pomocí kryptografických klíčů nebo certifikátů. Z hlediska kybernetické bezpečnosti jde také o přípustný způsob autentizace. Může se jednat např. o autentizaci pomocí SSH klíče s aktuálně odolnou délkou.

Dále jsou v případě, kdy není možné použít z určitého důvodu ani autentizaci pomocí kryptografických klíčů nebo certifikátů, ve vyhlášce stanovena pravidla, která je nutná nástrojem sloužícím pro ověřování identit vynucovat v případě autentizace za pomocí pouze identifikátoru účtu (např. přihlašovacího jména) a hesla. Tento způsob není z bezpečnostního hlediska 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 zejména o minimální délky hesel, skladbu hesel, pravidla zahrnující životní cyklus hesel např. pro tvorbu a životnost hesel a jiné. 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 i při využití komplexity, bude trvat prolomení tohoto hashe pouze cca 12 minut. V případě, kdy bude zvoleno heslo tvořené frází o délce 12 a více znaků, se čas na prolomení hashe prodlužuje na vyšší úroveň. Nicméně je nově ukotveno v požadavcích vyhlášky, že při jakémkoliv podezření na kompromitaci hesla je nutné toto heslo bezodkladně změnit.

K těmto příkladům je však nutné uvést několik dalších poznámek. Výpočetní výkon 1,5 Th/s je možné získat při investici nižší než 1 milion 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, což při dodržení komplexity odpovídá entropii na úrovni zhruba 128 bitů a pro účty technických aktiv na 22 znaků.

U účtů technických aktiv je nutné připomenout, že tyto účty slouží často k automatizovaným procesům, mohou mít (v porovnání s běžnými uživatelskými nebo administrátorskými účty) vyšší oprávnění a z těchto důvodů je jejich kompromitace potenciálně závažnější. Požadavek na minimální délku hesla 22 znaků u účtů technických aktiv je proto odůvodněn potřebou výrazně zvýšit entropii hesla, a tím i jeho odolnost vůči útokům hrubou silou. Rovněž tím dochází ke kompenzaci rizik spojených s dlouhodobým používáním hesla, možné limitace při

plnění dalších požadavků vyhlášky na identity a hesla (např. nemožnost zajištění opětovného ověření identity po stanovené době nečinností) a také je tím zajištěna vyšší úroveň ochrany s ohledem na potenciálně široký rozsah jejich oprávnění. V neposlední řadě délka 22 znaků při použití běžného znakového prostoru (malá a velká písmena, číslice a speciální znaky) odpovídá entropii přes 140 bitů, což je považováno za velmi silné heslo i podle mezinárodních bezpečnostních standardů (např. NIST) a v případech, kdy by nemohla být zajištěna plná komplexita využívaných znaků se entropie pohybuje kolem 103.4 až 130.9 bitů, což odpovídá entropii 17 znakového hesla s využitím komplexity (entropie cca 111.7 bitů).

Za účelem zvýšení komplexity hesel, a tím i ztížení využití slovníkových útoků musí být u účtů uživatelů, administrátorů a technických účtů 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 je umožněna změna hesla, přičemž je nutné technicky zajistit, aby tuto změnu nebylo možné provádět opakovaně v příliš krátkém časovém intervalu. Tento interval je stanoven na 30 minut, avšak poskytovatel regulované služby 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 svázána nutnost znemožnění použití dříve používaných hesel s pamětí alespoň 12 předchozích hesel. Dalším požadavkem je nutnost změny hesla v intervalu alespoň jednou za 18 měsíců, který v této vyhlášce přetrval na základě zkušeností úřadu plynoucích z kontrolní činnosti a nahlášených kybernetických bezpečnostních incidentů, při kterých byla zneužita kompromitovaná hesla, která byla např. zveřejněna na dark webu před několika lety. Jedná se o kompromis mezi aktuálními trendy, které inklinují k tomu, že na jedné straně hesla není obecně nutné periodicky obměňovat, jelikož se dnes již běžně využívá vícefaktorová autentizace a implementují se bezpečnostní opatření postavené na principu nulové důvěry tzv „zero-trust“, zatímco na druhé straně jsou trendem heslové politiky s nucenými krátkými periodicitami pro změnu hesla, které mají za následek používání odvoditelných hesel. Další požadované pravidlo tohoto ustanovení je, aby uživatelům a administrátorům nebylo umožněno zvolit si jednoduchá a často 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“). Stejně tak tento požadavek míří na již zmíněná odvoditelná hesla, kdy je při znalosti předchozích hesel možné odvodit heslo aktuální.

Další část tohoto ustanovení se věnuje výchozím heslům uživatelů a heslům k obnově jejich přístupu. Při vytváření nebo obnově přístupu je nezbytné zajistit důvěrnost těchto údajů od vytvoření, až po případné předání uživateli a nevyužívat např. jednotné počáteční heslo pro všechny nově nastupující zaměstnance, ale vytvořit tato hesla náhodně. K zajištění důvěrnosti používaných hesel je důležitá také změna výchozích hesel, jelikož existují zdroje pro některá technická aktiva, ze kterých lze zjistit jejich výchozí hesla. To znamená, že je nutné změnit veškerá výchozí hesla, ať se jedná o uživatelské účty nebo 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 účtů 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 účtů se odvíjí i bezpečnostní požadavky tohoto usnesení na ně kladené, kdy je vyžadována bezodkladná změna jejich hesla, jejich komplexita, délka 22 znaků, jejich bezpečné uložení, omezení užití tohoto účtu, změna jeho hesla v určitém intervalu a evidence manipulace nebo pokusů o manipulaci s těmito účty nebo jejich hesly.

K § 20 (Řízení přístupových práv a oprávnění)

Pro řízení přístupových práv a oprávnění je vymezen požadavek na zajištění řízení práv pro přístup k jednotlivým aktivům (v praxi se tedy jedná např. o právo přístupu k datovému úložišti, do konkrétní adresářové složky nebo ke konkrétnímu rozhraní) a oprávnění pro čtení dat, zápis informací a dat a změnu oprávnění (např. známé také z anglického read, write, modify and execute), zejména s cílem omezení oprávnění u osob bez potřebného need-to-know nebo pracovního zařazení. Toto řízení musí být prováděno pomocí centralizovaného nástroje s ohledem na vazby mezi aktivy. Tento požadavek míří na situaci, kdy bude v rámci poskytovatele regulované služby např. provozováno více systematických celků technických aktiv, která tvoří pomyslný „informační systém“ podle původního zákona, nikoliv na celou organizaci poskytovatele regulované služby. Je tak reflektováno pomyslné technické oddělení dílčích „informačních systémů“, u kterých v praxi často není možné nebo žádoucí z pohledu kybernetické bezpečnosti nebo provozu, aby jejich správa identit a řízení přístupových práv a oprávnění byla provázána nebo centralizována. 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 vybavením fyzicky odděleny od jiných komunikačních sítí bude pro řízení práv a oprávnění použito více těchto nástrojů. Řízení těchto práv a oprávnění by mělo být dále zajištěno v maximální možné míře prostřednictvím rolí a uživatelských skupin, jak je uvedeno v § 14 vyhlášky.

Centralizovaný nástroj je požadován pro zajištění bezpečnějšího provozu především v návaznosti na potřebu snadného řízení změn přístupových práv a oprávnění (např. při přidělení přístupových práv a oprávnění, při jejich změně nebo 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 práv a 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 § 21 (Detekce kybernetických bezpečnostních událostí)

V rámci tohoto ustanovení je oproti původnímu znění vyhlášky nově spojeno ustanovení ochrany před škodlivým kódem s ustanovením detekce kybernetických bezpečnostních událostí. Jedná se o změnu, která byla provedena s ohledem na vývoj v oblasti informačních technologií, na obecné zvýšení maturity v oblasti kybernetické bezpečnosti v České republice a postupně se zvyšující počet hrozeb v kyberprostoru. Jelikož spolu byly tyto dva paragrafy úzce spjaty v rámci plnění požadavků technických bezpečnostních opatření a i rozvoj nových nástrojů, které zajišťují ochranu a plnění těchto požadavků vedl přirozeně ke sloučení těchto paragrafů do jednoho. Stále je tedy vyhláškou požadováno nasazení nástrojů, které jsou schopny buď detekovat nebo současně i účinně čelit kybernetickým bezpečnostním událostem, které mohou vést ke kybernetickým bezpečnostním incidentům. Z hlediska kategorizace je možné využít tyto prostředky na úrovni komunikační sítě nebo nasazené v rámci technických aktiv, které již nejsou uvedeny demonstrativním výčtem, jak tomu bylo v původní vyhlášce. Od demonstrativního výčtu bylo v této vyhlášce upuštěno, jelikož je aktuální znění postaveno na posouzení poskytovatele regulované služby, kdy je třeba rozhodnout, která technická aktiva jsou z pohledu kybernetické bezpečnosti a detekce kybernetických bezpečnostních událostí relevantní. Podobně, z hlediska funkcionality, je možné rozlišit fungování těchto nástrojů na ty, které provádí pasivní detekci kybernetických bezpečnostních událostí bez aktivního

ovlivňování komunikace, a ty, 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 (v rámci jednotlivých segmentů a mezi segmenty), a to včetně perimetru interní komunikační sítě – tedy schopnost kontrolovat příchozí a odchozí provoz, případně aktivně blokovat nežádoucí komunikaci.

Pro zajištění vyšší úrovně zabezpečení si poskytovatel regulované služby musí určit relevantní technická aktiva, v jejichž rámci lze zajistit detekci kybernetických bezpečnostních událostí, včetně ochrany před škodlivým kódem, jako např. u koncových stanic, mobilních zařízení (především mobilních telefonů a notebooků), serverů, aktivních síťových prvků (např. routerů nebo switchů) a všech dalších obdobných technických aktiv. V rámci ochrany před škodlivým kódem je také nutné řídit a sledovat používání vyměnitelných zařízení (např. myši, klávesnice, tiskárny nebo externí Wi-Fi karty) a datových nosičů (typicky flash disky, velkokapacitní paměťová zařízení nebo paměťové karty) a zejména ve vztahu ke koncovým zařízením (především mobilní telefony, tablety, notebooky a stolní počítače) pak řídit automatické spouštění obsahu. Detekce kybernetických bezpečnostních událostí má být zajištěna nástrojem, který je s ohledem na vazby mezi aktivy centrálně spravován.

Ochrana před škodlivým kódem je důležitou součástí dnešních nástrojů pro detekci kybernetických bezpečnostních událostí také vzhledem k faktu, že množství a využití škodlivého kódu neustále narůstá a je stále sofistikovanější. Je proto vyžadováno, aby poskytovatel regulované služby za účelem ochrany před škodlivým kódem používal vhodné nástroje pro detekci kybernetických bezpečnostních událostí, které zajišťují nepřetržitou automatickou ochranu a aby tyto nástroje a jejich detekční pravidla i nastavení byly pravidelně a bezodkladně (např. v případě potřeby ošetřit nově zneužívané tzv. „zero-day“ zranitelnosti) aktualizovány. Tento požadavek je vztažen jak k nástrojům detekujícím kybernetické bezpečnostní události na úrovni komunikační sítě, tak u jednotlivých technických aktiv. Oproti původní vyhlášce je nově uveden požadavek na tyto nástroje zajišťující detekci v podobě vlastnosti umožňující sledování chování technických aktiv, uživatelů, aplikací a procesů, 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 výstupů řízení rizik a z bezpečnostních potřeb poskytovatele regulované služby.

K § 22 (Zaznamenávání událostí)

Poskytovatel regulované služby na základě hodnocení aktiv a bezpečnostních požadavků určí rozsah technických aktiv, která jsou relevantní z pohledu zaznamenávání událostí, a také jaké bezpečnostní a relevantní provozní události budou u nich zaznamenávány. Vyhláška 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), tak i s ohledem na to, jaké podrobnosti musí být zaznamenány (např. datum a čas, typ činnosti, identifikace účtů a původců).

Požadavek na zaznamenávání relevantních provozních událostí je zde uveden z důvodu, že provozní událost může být např. 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 např. šifrování na disku, které může být žádoucí (např. v případě použití šifrovacího nástroje BitLocker) i nežádoucí (např. v případě zašifrování pevného disku škodlivým programem Ransomware). Určení rozsahu technických aktiv, u kterých bude zaznamenávání prováděno, je v této vyhlášce z důvodu, že není nutné bezpečnostní a provozní události sledovat na všech technických aktivech, protože by to poskytovatele regulované služby 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 v této vyhlášce požadavek na jeho aktualizaci v pravidelném intervalu a při významných změnách (jako např. při pořízení nového technického aktiva, ze kterého by mohlo být důležité záznamy o bezpečnostních událostech sledovat).

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. Zejména z důvodů správného vyhodnocování bezpečnostních a provozních událostí pro případy vyšetřování kybernetických bezpečnostních incidentů. Příkladem je předcházení situacím jako např. použití nástroje typu "web application firewall" (dále jen „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). Doba uchovávání záznamů je nastavena na 18 měsíců, a to zejména na základě zkušeností úřadu a skutečnosti, že střední doba detekce kybernetického bezpečnostního incidentu v regionu EMEA (z anglického 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 kybernetický bezpečnostní incident stal. Při vyšetřování takového incidentu je pak zcela klíčové, zda jsou tyto záznamy k dispozici nebo nikoliv. Hodnotou 18 měsíců se zvyšuje šance na zajištění potřebných důkazů k případnému šetření a analyzování kybernetických bezpečnostních 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 poskytovatele regulované služby by mělo dojít mimo určení rozsahu technických aktiv a jejich bezpečnostních a relevantních provozních událostí i k posouzení toho, jaké logy budou podle § 22 vyhlášky uchovávány a po jakou dobu. Zejména je tak na místě učinit např. vzhledem k použitelnosti (informační hodnotě) konkrétního typu logů v čase, kdy u některých typů logů postrádá smysl jejich uchovávání a jsou relevantní pouze v řádech hodin nebo dní a vlastním zdrojům pro vyhodnocování kybernetických bezpečnostních událostí, přičemž 18 měsíců je výchozí hodnota, která když bude nastavena jinak, vyžaduje řádné odůvodnění na základě výstupů systému řízení bezpečnosti informací a bezpečnostních potřeb poskytovatele regulované služby.

Novým požadavkem v oblasti zaznamenávání událostí oproti původní vyhlášce je povinnost používat centrální nástroj (s ohledem na vazbu mezi aktivy, viz odůvodnění k § 20) pro uchovávání záznamů (např. nástroj pro správu logů, syslog server), který by měl zajišťovat i plnění předchozích požadavků pro zajištění důvěrnosti, integrity a dostupnosti ukládaných záznamů. Vyhláška si neklade za cíl stav, ve kterém bude tento nástroj pro centrální uchovávání záznamů absentovat a všechny záznamy budou uchovávány (např. i nad rámec vhodné doby retence) v nástroji pro vyhodnocování kybernetických bezpečnostních událostí (např. SIEM). Jelikož účinnost a ekonomičnost tohoto nástroje je naopak snížena při zahlcení nadměrným množstvím záznamů. Nicméně je na místě v praxi určit, jaký objem záznamů je technicky možné aktivně využívat a mít připraven k vyhodnocování, zatímco aktivně nevyužívané záznamy je vhodné přemístit na jiné úložiště, na kterém sice nejsou tyto záznamy okamžitě připraveny, ale jsou dostupné po nějakém čase např. pro potřeby zpětné analýzy (tzv. long-term nebo cold storage).

K § 23 (Vyhodnocování kybernetických bezpečnostních událostí)

Toto ustanovení cílí na to, aby poskytovatelé regulované služby disponovali nástroji umožňujícími provádět kontinuální a centralizované vyhodnocování kybernetických bezpečnostních událostí z bezpečnostních a relevantních provozních záznamů. Pod tímto názvem jsou např. vnímány nástroje typu SIEM nebo SOAR, které v praxi mohou být využívány i tzv. dohledovými centry SOC (z anglického Security Operations Center), a další bezpečnostní opatření, která plní tento úkol. Mezi sbíranými záznamy 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 kontrolovat 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 v původní vyhlášce nedošlo k zásadním změnám, pouze byly reflektovány změny ve zněních ostatních ustanovení a byla zpřehledněna jeho struktura.

K § 24 (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 (např. aktivní komunitou v případě tzv. „open-source software“). V této oblasti je nově požadavek na aplikování schválených bezpečnostních aktualizací, jelikož nestačí mít pouze podporovaná technická aktiva, pokud nemají tyto aktualizace aplikovány. V takovém případě mohou být tato technická aktiva zranitelná vůči již známým zranitelnostem, pro které již může existovat záplata. Schválenými bezpečnostními aktualizacemi jsou myšleny ve většině případů aktualizace přímo od výrobce nebo smluvního dodavatele daného technického aktiva, kdy u těchto aktualizací je na místě ověřovat, že daná aktualizace opravdu pochází z důvěryhodného zdroje a nebyla např. během stahování podvržena (lze např. ověřovat hashové otisky), jelikož i tyto aktualizace mohou být vektorem útoku. Nicméně u některých technických

aktiv může být na místě i ověřovat funkčnost a bezpečnost aktualizací před jejich nasazením do provozního prostředí (např. že daná aktualizace nezpůsobí nefunkčnost daného technického aktiva), a proto je také možnost tyto schválené bezpečnostní aktualizace vnímat jako schválené až po jejich otestování v rámci např. testovacího/předprodukčního prostředí poskytovatele regulované služby a jejich schválení pro nasazení do provozního prostředí. Obecně by pod pojmem schválené bezpečnostní aktualizace měly být vnímány např. ty aktualizace, které jsou schváleny podle nastavených postupů a procesů poskytovatele regulované služby v rámci řádného řízení změn a zranitelností (relevantními oblastmi jsou zejména tzv. change management, vulnerability management, patch management atd.).

Oproti tomu u nepodporovaných technických aktiv není možné zaručit jistou úroveň bezpečnosti formou vydávání bezpečnostních záplat a aktualizací. Z tohoto důvodu je novou povinností v tomto ustanovení, oproti původnímu vyhlášce, vést evidenci technických aktiv, která již nejsou podporována a zavádět bezpečnostní opatření, která tuto problematiku reflektují a poskytnou vyšší nebo obdobnou úroveň zabezpečení (např. prostřednictvím segmentace komunikační sítě, kdy jsou nepodporovaná technická aktiva oddělena ve vlastním segmentu, který není považován za zabezpečený). Stejně tak je v této oblasti nově zaveden požadavek evidovat i technická aktiva, která sice jsou podporovaná, ale u kterých není možné zavést poslední schválenou bezpečnostní aktualizaci (např. z toho důvodu, že aplikování této aktualizace způsobí nefunkčnost daného technického aktiva, aktivum nemá dostatečnou hardwarovou výbavu nebo by třeba aplikování mohlo mít negativní vliv na jiná aktiva).

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 např. kompromitace, což může být případ, kdy mezi interní komunikaci dvou osob nebo technických aktiv vstupuje třetí strana, která tuto komunikaci kompromituje či modifikace transakce (sloužící pro provedení změny v databázi) neoprávněnou osobou. 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 bezpečnostní 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 původnímu znění vyhlášky je v tomto ustanovení uvedena povinnost provádět skenování zranitelností technických aktiv, a to z interní a externí komunikační sítě např. formou veřejně dostupných nástrojů pro skenování zranitelností IP rozsahu vystavených vůči veřejnému internetu, kdy tyto nástroje mohou poskytovateli regulované služby poskytnout informaci, 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 její provádění v pravidelném intervalu jednoho roku, jelikož je v praxi provádění skenování zranitelností finančně nenáročný proces realizovatelný pomocí veřejně dostupných nástrojů je doporučeno tento interval naopak snížit a zavést skenování zranitelností jako součást běžných procesů.

Obdobně jako u skenování zranitelností, musí poskytovatel regulované služby na základě tohoto ustanovení periodicky provádět penetrační testování u technických aktiv s ohledem na hodnocení těchto aktiv a hodnocení rizik, přičemž i zde je nutné postupovat přiměřeně podle § 3 písm. c) vyhlášky. V praxi se může např. jednat o tzv. „core“ část, v některých případech se může jednat o všechna technická aktiva tvořící interní komunikační síť. Je tedy nezbytné si správně tato technická aktiva vydefinovat, jelikož absence penetračního testování u těchto

aktiv by mohla mít za následek zanesení případné zranitelnosti do produkčního prostředí, které může následně využít potenciální útočník. Penetrační testování je podle tohoto ustanovení nezbytné provádět z interní i externí komunikační sítě, před jejich uvedením do provozu a v souvislosti s významnou změnou. Pokud dané aktivum není dostupné z externí sítě např. z důvodu ostrovního režimu, bude se aplikovat pouze penetrační testování ze sítě interní. Pokud by vedla potenciální cesta mezi externí a interní sítí i k takto vyčleněným aktivům, je vhodné otestovat i tyto prostupy, aby bylo prověřeno, že jsou případná bezpečností opatření nastavena správně. Penetrační testování je nutné provádět za účelem nalezení případných slabých míst (zranitelností) z pohledu kybernetické bezpečnosti a tato slabá místa ošetřit nebo rovnou odstranit, aby nemohla být ohrožena bezpečnost regulované služby. Oproti původním vyhlášce musí poskytovatel regulované služby provádět penetrační testování z interní a externí komunikační sítě alespoň jednou za dva roky. V odůvodněných případech (např. vysoké komplexnosti prováděného testu) je možné rozdělit toto testování do systematických celků a provést ho nejpozději do pěti let. Tento interval je nastaven tak, aby vhodně pokryl drtivou většinu poskytovatelů regulovaných služeb, a to za cílem zvýšení úrovně kybernetické bezpečnosti v České republice. Jestliže je tento interval s ohledem na § 3 písm. c) vyhlášky nepřiměřený pro konkrétního specifického poskytovatele regulované služby, může na základě řízení rizik přizpůsobit způsob plnění tohoto bezpečnostního opatření a náležitě to odůvodnit v dokumentu prohlášení o aplikovatelnosti.

U každého provedeného penetračního testování je také nově povinnost evidovat osobu nebo osoby, které penetrační testování vykonaly a v jakém časovém rozmezí (datum provedení) bylo toto testování realizováno. Tento požadavek vznikl na základě potřeby zpětné přezkoumatelnosti a získání uceleného pohledu nad prováděnými penetračními testy z pohledu poskytovatele regulované služby.

Po dokončeném skenování zranitelností nebo penetračním testování je nezbytné, aby bylo provedeno ověření funkčnosti a bezpečnosti zavedeného bezpečnostního opatření, které vedlo k nápravě zjištěné zranitelnosti, aby bylo prokázáno, že potenciální útočník nemůže této zranitelnosti nadále zneužít.

K § 25 (Kryptografické algoritmy)

Zabezpečení komunikace a bezpečnost technických aktiv využívajících kryptografii (např. síťové komunikační protokoly, kryptografické klíče a certifikáty) jsou podmíněny využíváním aktuálně odolných kryptografických algoritmů. Dále je nezbytné, aby poskytovatelé regulované služby prosazovali bezpečné nakládání s kryptografickými algoritmy, např. stanovením pravidel a postupů pro užívání kryptografických algoritmů a vzděláváním uživatelů formou školení. Toto ustanovení dále odkazuje na doporučení v oblasti kryptografických algoritmů vydávaná úřadem (např. dokument Minimální požadavky na kryptografické algoritmy), která zveřejňuje na svých webových stránkách a podle vývoje v této oblasti je na základě odborné výzkumné činnosti aktualizuje. Tato doporučení nejsou vzhledem k dynamickému vývoji této problematiky zahrnuta ve vyhlášce, ani jejích přílohách, a to právě z důvodu potřeby četnějších aktualizací a doplnění o relevantní informace.

Oproti původní vyhlášce, která tuto povinnost neukládala, je nově stanoven požadavek, aby poskytovatel regulované služby zajistil 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 poskytovatele regulované služby. Její zabezpečení bývá často opomíjeno, zejména pak zachování její důvěrnosti a integrity. V obecnosti se jedná o zabezpečení zejména důvěrnosti a integrity formou různých bezpečnostních opatření, které aplikuje poskytovatel regulované služby, aby v případech, kdy využívá některou ze zmíněných forem komunikace pro přenášení informací nebo dat, nedošlo

k narušení bezpečnosti regulované služby. Mohlo by se např. jednat o nasazení S/MIME či jiného šifrování obsahu e-mailu, pokud jsou v něm obsaženy citlivé informace, využití nějakého nástroje zajišťujícího šifrovanou audiovizuální nebo hlasovou komunikaci, pokud by v rámci daného hovoru mělo být probíráno nastavení interních bezpečnostních nástrojů, výsledky z penetračního testování nebo jiné citlivé informace.

V případě, kdy poskytovatel regulované služby využívá kryptografické klíče nebo certifikáty, musí zajistit jejich potřebnou kvalitu, nezbytnou ochranu a správu. Dále je v tomto usnesení uvedeno, jaké minimální parametry musí být v souvislosti s kryptografickými klíči a certifikáty zajištěny. Je to z důvodu jejich praktické implementace a možné přezkoumatelnosti ze strany poskytovatele regulované služby, kdy je cílem zajištění efektivnosti tohoto bezpečnostního opatření.

K § 26 (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 bezpečné architektury, architektury komunikační sítě, umístění jednotlivých technických aktiv atd.

Je nezbytné, aby poskytovatel regulované služby vyhodnotil, jaké hrozby a zranitelnosti mohou dostupnost jeho regulované služby, a to včetně jednotlivých aktiv, ohrozit a současně podle potřeb organizace zavedl bezpečnostní opatření, aby se snížil 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 (např. UPS nebo diesel-agregát), ale také např. držením jistých skladových zásob technických aktiv nebo dostatečným smluvním ošetřením dodávky služeb souvisejících s dostupností u třetích stran (např. připojení k internetu).

V oblasti technických aktiv je také nutné s ohledem na hodnocení těchto aktiv a výsledky řízení rizik dbát na bezpečné konfigurace a jejich správu (tzv. Security Configuration Management). Podle nejlepší praxe v oblasti kybernetické bezpečnosti a provozu je na místě nakládat s konfiguracemi bezpečně, jelikož i v rámci běžných provozních změn lze skrze např. lidské pochybení způsobit implementaci špatné konfigurace a narušit dostupnost regulované služby nebo povolení neřízených prostupů a vznik kybernetické bezpečnostní události či incidentu.

V neposlední řadě se toto ustanovení věnuje problematice zálohování, která v původní vyhlášce nebyla zcela pokryta, 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 za dopad např. zašifrování, a tedy nepoužitelnost aktiv regulovaných služeb (např. ransomware). Poskytovatel regulované služby je tak povinen 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 jedním ze spolehlivých způsobů pro zajištění kontinuity a dostupnosti (případně obnovení) regulované služby (např. 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 § 27 (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 zejména u technických aktiv regulované služby, slouží

toto ustanovení pro zdůraznění specifických potřeb nad rámec předchozích ustanovení, a to pro průmyslová, řídicí nebo jiná obdobná specifická technická aktiva.

Název tohoto ustanovení byl změněn na základě zkušeností expertů věnujícím se těmto aktivům a také z prováděných kontrol úřadu, kdy např. poskytovatelé regulované služby disponovali technickými aktivy, která byla atypická od běžných koncových stanic a serverů, avšak nejednalo se přímo o průmyslová nebo řídicí technická aktiva v běžném slova smyslu. Přestože tato technická aktiva s nimi sdílela obdobné vlastnosti, jako je např. zastaralost operačních systémů, používání nezabezpečených komunikačních protokolů specifických pro dané prostředí, závislost na dodavateli a vzdálené správě tohoto technického aktiva, nebyla pro ně zavedena vhodná bezpečnostní opatření jako např. přísnější řízení v rámci segmentace sítě u těchto technických aktiv, dostatečná redundance pro případy obnovy při nedostupnosti těchto technických aktiv nebo vyšší bezpečnostní požadavky na zabezpečení vzdáleného připojení a správy. S těmito specifickými technickými aktivy nebylo nakládáno jako s průmyslovými a řídicími technickými aktivy a ani jako s běžnými technickými aktivy, jelikož tak nebyly vnímány, přestože se z pohledu kybernetické bezpečnosti jedná o podpůrná technická aktiva.

Textace úvodu tohoto ustanovení byla záměrně změněna, aby si poskytovatelé regulované služby byli vědomi toho, že i tato oblast a tato specifická technická aktiva mohou být součástí rozsahu řízení kybernetické bezpečnosti a je tedy i v této oblasti na místě zavádět bezpečnostní opatření jako u ostatních aktiv, jen na tato aktiva musí poskytovatelé regulované služby aplikovat opatření tohoto paragrafu nad rámec všech předchozích. Na základě kontrolní činnosti úřadu v praxi často dochází k nevhodnému oddělení tzv. informačních a operačních technologií (IT a OT) z pohledu systému řízení bezpečnosti informací a dochází k neřízenému zavádění bezpečnostních opatření a jejich opomenutí, kdy se např. správci nebo garanti OT prvků mylně domnívají, že se na tato průmyslová nebo jiná specifická aktiva aplikuje pouze tento paragraf. Je však nezbytné zavádět celý rozsah požadavků vyhlášky v souladu s konceptem řízení rizik.

Při formulování těchto doplňujících požadavků byla také využita doporučení NIST, mezinárodní normy např. IEC 62443, standardy, poznatky z mezinárodních jednání a nejlepší praxe z této oblasti. Oproti původní vyhlášce došlo také k narovnání a sjednocení využívané terminologie.

Hlavními požadavky tohoto ustanovení zůstaly požadavky na omezení, ať už fyzického přístupu, vzdáleného přístupu a správy a nově také omezení oprávnění k přístupu k těmto aktivům. Jak již bylo výše zmíněno, u těchto aktiv je očekáváno, že mohou mít např. delší životní cyklus, jelikož mohou být příliš specifická a vytvářena na míru pro dané prostředí. Proto nejen z těchto důvodů, oproti např. bezpečnostním požadavkům v § 17, které se sice obecně věnují řízení fyzické bezpečnosti, je specifikován požadavek tohoto ustanovení čistě na omezení tohoto fyzického přístupu k těmto aktivům. Poskytovatel regulované služby tak musí fyzický přístup k těmto specifickým technickým aktivům více limitovat a omezit, než jak je tomu požadováno u běžnějších technických aktiv. Stejně tak musí nakládat i v oblasti vzdáleného přístupu a správy, jelikož v případě, kdy by nebyl poskytovatel regulované služby schopen zajistit aktuálnost software (často firmware) těchto specifických technických aktiv, nemuselo by být možné zaručit odolnost u těchto aktiv z důvodů jejich zastaralosti. Je tedy nezbytné, aby vzdálený přístup a správa byla co nejvíce omezena, včetně omezení této komunikace mimo komunikační síť poskytovatele regulované služby (např. veřejný internet), a potenciální útočník nemohl využít zranitelností, které za životní cyklus těchto aktiv již mohou být veřejně známy. Jedna z možností, jak zajistit vyšší úroveň bezpečnosti vzdáleného přístupu je prostřednictvím k tomu určených specifických koncových technických aktiv (tzv. jump serverů, nebo např. řešení PAM), které přináší další vrstvu oddělení komunikační sítě

při administrátorském přístupů v rámci vzdálené správy a vzdáleného přístupu k těmto specifickým aktivům a jejich kontrolu.

Dále je v tomto ustanovení uveden požadavek na oddělení prostředí specifických technických aktiv a požadavek na segmentaci komunikační sítě v rámci tohoto prostředí. Pro zajištění lepšího oddělení mezi jednotlivými prostředími, segmenty komunikačních sítí (např. s ohledem na důležitost daných aktiv v segmentu) nebo pro další ochranu při vzdáleném přístupu nebo vzdálené správě nejen zmíněných specifických technických aktiv, lze implementovat např. bezpečnostní opatření v rámci tzv. Purdue modelu (jinak angl. Purdue Enterprise Reference Architecture), demilitarizovanou zónu (DMZ), která umožní granulárnější řízení a kontrolu komunikace mezi jednotlivými segmenty a mohou tak být minimalizována rizika vyplývající z přímé komunikace těchto aktiv. Mimo jiné ve vyhlášce také zůstal požadavek pro zajištění dostupnosti, kdy např. u těchto specifických aktiv by kromě připravených plánů obnovy, zabezpečených pravidelných záloh a schválených aktuálních konfigurací mohl poskytovatel regulované služby disponovat skladovými zásobami s ohledem na specifičnost těchto aktiv.

K § 28 (Přechodná ustanovení)

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

K § 29 (Účinnost)

Zákon a návrh vyhlášky jsou vzájemně komplementární. Je v zájmu jak normotvůrce, tak adresátů prováděcího právního předpisu, aby zákon a návrh vyhlášky vstoupily v účinnost ve stejný okamžik.

K příloze č. 1 (Hodnocení aktiv)

Cílem této přílohy je představit jeden z možných způsobů hodnocení aktiv. Tato příloha obsahuje stupnice pro hodnocení důvěrnosti, integrity a dostupnosti stejně jako tomu bylo v původní vyhlášce, jen s drobnými textovými úpravami. Příloha byla doplněna o popis procesu hodnocení aktiv, který by měl poskytovateli regulované služby usnadnit aplikaci tohoto bezpečnostního opatření a slouží především ke zvýšení návodnosti. Jednotlivé tabulky definují čtyři základní úrovně pro hodnocení aktiv, jejich popis, základní formy ochrany, sdílení s třetími stranami podle TLP protokolu a požadavky na způsob jejich likvidace (odkazem na přílohu č. 2 k vyhlášce). Jednotlivé úrovně byly stanoveny na základě nejlepší praxe. Při tvorbě metodiky hodnocení aktiv má poskytovatel regulované služby vycházet z této přílohy. To však není podmínkou, poskytovatel regulované služby může používat odlišný počet úrovní pro hodnocení aktiv, alespoň o čtyřech úrovních, než jaký je uveden v této příloze, dodrží-li jednoznačné vazby mezi jimi používaným způsobem hodnocení aktiv a stupnicemi a úrovněmi pro hodnocení aktiv, které jsou uvedeny v příloze. Dále byly do přílohy přesunuty oblasti pro hodnocení primárních aktiv, které byly doplněny o další příklady z důvodu zvýšení přehlednosti a návodnosti.

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

K příloze č. 2 (Likvidace informací a dat)

Příloha popisuje možnosti, jak přistoupit k mazání a likvidaci technických nosičů informací a dat, včetně provozních údajů a jejich kopií. Pravidla a postupy pro likvidaci musí být stanovena přiměřeně tak, aby neúměrně nezatížila poskytovatele regulované služby, ale zároveň, aby byly dodrženy popsané postupy s ohledem na úroveň aktiv a další aspekty.

Stanovené postupy v této příloze jsou formulovány tak, aby bylo zajištěno, že dojde ke správnému posouzení a následnému využití odpovídajícího způsobu likvidace. V další části této přílohy jsou popsány samotné způsoby likvidace technických nosičů informací a dat, včetně provozních údajů a jejich kopií v závislosti na úrovni aktiv. V této příloze byly provedeny úpravy textu za účelem zvýšení přehlednosti a s ohledem na dynamiku vývoje technologií a nástrojů došlo k vypuštění dříve vypsaných možných příkladů likvidace, jelikož rigidnost legislativních předpisů by neumožňovala v dostatečné míře tento trend reflektovat.

K příloze č. 3 (Zranitelnosti a hrozby)

V této příloze je poskytovateli 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. norma ISO/IEC 27005) a současně je nezbytné zohlednit hrozby a zranitelnosti podle vlastní zkušenosti poskytovatele regulované služby.

Oproti původní vyhlášce došlo k úpravě a doplnění několika nových hrozeb a zranitelností, které byly identifikovány v rámci činnosti úřadu a spolupráce úřadu se soukromým i veřejným sektorem a odbornou veřejností, kdy např. zranitelnosti 15 a 16 a hrozby 7, 13, 17, 19 a 20 reagují na získané zkušenosti s problematikou v oblastech cloud computingu. Hrozby 7, 14 a 18 pak reagují na neustále se rozšiřující využívaní družicových (satelitních) služeb jako aktiv nezbytných pro poskytování regulovaných služeb. Mezi družicové služby patří např. družicové navigace, resp. služby globálních navigačních družicových systémů GNSS (určených zejména pro navigaci a přesnou synchronizaci času) a družicová komunikace. Družicové služby mohou být ze své technické a fyzikální povahy náchylné na specifické hrozby (např. rušení či podvržení).

K příloze č. 4 (Hodnocení rizik)

Příloha obsahuje doporučení pro výpočet rizik a jednotlivé stupnice pro hodnocení hrozeb, zranitelností i rizik. Každá stupnice pracuje se čtyřmi úrovněmi možného hodnocení. Jednotlivé úrovně byly stanoveny na základě nejlepší 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 č. 1 týkající se hodnocení aktiv došlo i zde k drobným úpravám textu za účelem zvýšení přehlednosti a návodnosti. Nově byly doplněny způsoby zvládání rizik pro snižování nebo eliminaci rizik a zajišťování požadované úrovně důvěrnosti, integrity a dostupnosti.

K příloze č. 5 (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. To znamená, že pokud na základě výstupů z provedeného 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 prohlášení o aplikovatelnosti.

Správné a dostatečné ošetření smluvních vztahů z pohledu kybernetické bezpečnosti je základním předpokladem k zajištění bezpečnosti aktiv regulované služby, kde hrají významnou roli dodavatelé. V této příloze je popsán příkladný výčet ustanovení, která by měla obsahovat každá smlouva uzavřená s dodavatelem.

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

Ustanovení o oprávnění užívat data upravuje, kdo a za jakých podmínek je oprávněn přistupovat a využívat data obsahující informace související s poskytováním regulované služby (osobní data a jiné pro poskytovatele regulované služby citlivé údaje, provozní data jako jsou logy a specifická systémová nastavení). Je vhodné jasně definovat účel užívání dat, kdo k nim má přístup a kdo je odpovědný za jejich případné neoprávněné užití nebo zveřejnění.

Ustanovení o autorství programového kódu, popřípadě o programových licencích je vhodné do smluv zahrnout nejen v případech, kdy je předmětem dodavatelského vztahu vývoj softwaru. Je v zájmu všech zainteresovaných stran mít od začátku jasně vymezeno, kdo je vlastníkem zdrojového, resp. programového kódu a kdo rozhoduje o způsobu jeho použití, případném prodeji nebo dalším vývoji; zda se jedná z pohledu problematiky autorských práv o společné autorství či nikoliv nebo jen o licenční ujednání, ve kterém dochází k převodu autorských práv; zda může být kód zpřístupněn třetím stranám apod. Toto ustanovení je důležité vnímat také jako klíčový prvek ochrany před tzv. vendor lock-in.

Ustanovení o kontrole zavedených bezpečnostních opatření je nutné zahrnout v rámci smluvních ustanovení z důvodu, aby poskytovatel regulované služby, který odebírá službu nebo produkt od dodavatele, měl možnost provést zákaznický audit u tohoto dodavatele. Toto ustanovení je důležité zejména v tom případě, kdy si chce poskytovatel regulované služby ověřit, zda dodavatel opravdu v praxi dodržuje stanovené podmínky a pravidla.

Ustanovení upravující řetězení dodavatelů je ve smlouvách důležité z toho důvodu, že poskytovatel regulované služby vybírá dodavatele např. podle určitých kritérií, která kladou jisté nároky např. i na kybernetickou 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 kybernetickou bezpečnost a pro správné řízení dodavatelů. Poddodavatel by navíc měl být zavázán samozřejmě dodržovat v plném rozsahu i ujednání mezi dodavatelem a poskytovatelem regulované služby, což je velice důležité pro celý systém řízení bezpečnosti informací.

Ustanovení, které je vhodné zahrnout do obsahu smlouvy s dodavatelem je ustanovení o povinnosti dodavatele dodržovat bezpečnostní politiky a bezpečnostní dokumentace poskytovatele regulované služby nebo ustanovení o odsouhlasení bezpečnostní politiky a bezpečnostní dokumentace dodavatele (nebo odsouhlasení pro dodavatelský vztah relevantních částí bezpečnostní politiky a bezpečnostní dokumentace) poskytovatelem regulované služby. V případě, že se dodavatel podílí na ochraně dat nebo správě systémů souvisejících s regulovanou službou, je vhodné vyhodnotit rizika s tímto spojená. Pokud se dodavatel smluvně nezaváže dodržovat pro předmět dodávky relevantní bezpečnostní politiky a bezpečnostní dokumentace a z toho plynoucí povinnosti, poskytovatel regulované služby se vystavuje riziku snížení svých vlastních zavedených bezpečnostních standardů. Toto ustanovení kromě toho, že zvyšuje odpovědnost samotných dodavatelů, zároveň snižuje rizika plynoucí z dodavatelských vztahů.

Ustanovení o řízení změn je bohužel jedním z podceňovaných smluvních ustanovení. Cílem tohoto ustanovení je, aby byly od začátku nastaveny jasné požadavky na řízení změn relevantních pro dodávku týkající se regulované služby (např. povinnost dodavatele hlásit s předstihem plánované změny, vyžadovat souhlas s provedením změny, vést dokumentaci

o všech provedených změnách a testování změn). Odpovědný přístup k řízení změn má pozitivní vliv na dostupnost regulované služby a její zabezpečení.

Mezi další klíčové ustanovení, které je vhodné v souvislosti s řízením dodavatelů zohlednit, patří také soulad smluv s obecně závaznými právními předpisy. Díky tomu by mělo být zajištěno, že smluvní vztahy podporují zákonné požadavky na bezpečnost a provozní stabilitu. Toto ustanovení vytváří právní základ pro kontrolu a dohled nad dodavatelem a umožňuje sankcionovat porušení obecně závazných zákonných povinností. Současně toto ustanovení zajišťuje, že dodavatel aktivně přizpůsobuje svou činnost platné legislativě a není možné tolerovat jeho neznalost souvisejících právních povinností.

Další část této přílohy se věnuje povinnosti dodavatele informovat poskytovatele regulované služby o kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy, o způsobu řízení rizik na straně dodavatele a o zbytkových rizicích souvisejících s plněním smlouvy, 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 poskytovatele regulované služby z hlediska kybernetické bezpečnosti důležité. U takto ošetřených smluv se zamezí případům, kdy dodavatel zatají kybernetické bezpečnostní 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. Zahrnout do smluv s dodavateli ustanovení o povinnosti dodavatele informovat poskytovatele regulované služby o žádosti cizozemského orgánu o zpřístupnění nebo předání dat je klíčové pro ochranu dat před neoprávněným přístupem ze strany zahraničních subjektů a pro zachování kontroly nad datovými toky. Povinnost dodavatele informovat poskytovatele regulované služby pomáhá předcházet situacím, kdy by data mohla být předána bez vědomí vlastníka dat. Absence tohoto ustanovení ve smlouvě by mohla vést k neoprávněnému zpřístupnění citlivých dat a závažným bezpečnostním a právním rizikům. Ustanovení o povinnosti dodavatele informovat poskytovatele regulované služby o fyzických osobách přicházejících do kontaktu s důvěrnými informacemi je vhodné zahrnout do smluvních ujednání z důvodu zajištění transparentnosti, řízení rizik a odpovědnosti za přístup k citlivým datům. Cílem tohoto ustanovení je zabránit neautorizovanému přístupu, omezit riziko úmyslného zneužití informací nebo útoku z vnitřního prostředí (např. únik dat, kompromitace systémů) a umožnit rychlou reakci na kybernetické bezpečnostní incidenty. Toto ustanovení dále umožňuje poskytovateli regulované služby prověřit přístupy k citlivým informacím ze strany dodavatele. Toto ustanovení je tedy stěžejní pro zajištění transparentnosti, kontroly a řízení přístupu k důvěrným informacím. Jeho absence by mohla vést k nekontrolovanému přístupu neoprávněných osob k citlivým datům a oslabení aplikovaných bezpečnostních opatření.

Ustanovení o specifikaci podmínek z pohledu bezpečnosti při ukončení smlouvy (tzv. exit strategie) je v této příloze zahrnuto z důvodu zajištění minimalizace rizik (jež by mohly vzniknout při přechodu na nové řešení), ochrany dat a kontinuity služeb. Pokud dojde k ukončení smluvního vztahu (např. z důvodu ukončení poskytování služeb pro něž byla smlouva sjednána, nemožnosti dodavatele plnit smluvní závazky, podstatné změny ve vlastnické struktuře dodavatele, které by mohly mít vliv na kybernetickou bezpečnost) je nutné, aby byl vymezen jasný plán pro kontrolované předání činností, migraci dat, ochranu informací a zajištění provozní kontinuity. Jasně stanovený postup minimalizuje riziko narušení dostupnosti regulované služby, bezpečnostních incidentů a právních komplikací. Pokud tento požadavek nebude ve smluvním ujednání zahrnut může to pro poskytovatele regulované služby znamenat riziko v podobě ztráty kontroly nad daty nebo nefunkčnost klíčových služeb. Důvodem pro zakomponování tohoto ustanovení do smluv je rovněž zajištění kontinuity

regulované služby, ochrany dat a citlivých informací, minimalizaci bezpečnostních rizik, zajištění odpovědnosti a právní ochrany a řízení dodavatelů v rámci přechodného období.

Ustanovení o řízení kontinuity činností v souvislosti s řízením dodavatelů 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.

Ustanovení o specifikaci náležitostí o úrovni poskytovaných služeb (SLA) a bezpečnostních opatření ve smlouvě je součástí této přílohy z důvodu zajištění dostupnosti a kontinuity služby, zabezpečení dat a systémů, rychlé reakce na kybernetické bezpečnostní incidenty a stanovení odpovědností. Toto ustanovení má definovat povinnosti dodavatele, parametry kvality služby a mechanismy pro řešení vzniklých kybernetických bezpečnostních incidentů. Absence těchto specifikací by mohla vést k právním a bezpečnostním rizikům, nejasnostem v odpovědnosti nebo narušení provozu regulované služby.

Dalším ustanovením, které je vhodné zohlednit v souvislosti s řízením dodavatelů je dodržování pravidel bezpečného vývoje. Toto ustanovení má za cíl minimalizovat bezpečnostní rizika již ve fázi vývoje a zabránit zranitelnostem, které by mohly být zneužity ke kybernetickým útokům. Zakotvení tohoto ustanovení do smlouvy s dodavatelem je vhodné zejména tehdy, pokud se jedná o součást regulované služby, kde by jakákoliv zranitelnost mohla způsobit výpadek, narušení integrity dat, neoprávněný přístup nebo obdobné ohrožení poskytování regulované služby. Správně nastavené bezpečnostní postupy ve vývoji minimalizují bezpečnostní rizika a zabraňují vzniku zranitelností, snižují náklady na dodatečné bezpečnostní opravy, chrání důvěrnost, integritu a dostupnost regulované služby, zajišťují odpovědnost dodavatele a jeho závazky k bezpečnosti softwaru.

Ustanovení, které je v rámci smluvního vztahu nezbytné zohlednit, je specifikace podmínek pro formát předání dat a informací, a to včetně technických, bezpečnostních a procesních požadavků na jejich zpřístupnění poskytovateli regulované služby. Zakomponování tohoto ustanovení do smluv zajistí právní jistotu, efektivní interoperabilitu a zajištění kontinuity regulované služby, přičemž současně minimalizuje provozní a bezpečnostní rizika spojená s přenosem dat mezi subjekty.

Ustanovení o pravidlech pro likvidaci dat ukládá dodavatelům povinnost zajistit ochranu důvěrnosti, integrity a dostupnosti dat poskytovatele regulované služby, což zahrnuje i bezpečnou likvidaci dat po ukončení jejich využívání. Je proto nezbytné jasně definovat pravidla a postupy likvidace dat, aby bylo zabráněno jejich neoprávněnému zpřístupnění, zneužití nebo narušení bezpečnosti informačních systémů. Implementace tohoto ustanovení přispívá k minimalizaci rizika neoprávněného přístupu nebo zneužití dat, čímž se zajišťuje jejich důvěrnost i po ukončení smluvního vztahu. Smluvně stanovené podmínky prokazatelné likvidace dat zároveň posilují právní jistotu a odpovědnost dodavatele, což zajišťuje soulad s regulatorními a bezpečnostními požadavky poskytovatele regulované služby.

Ustanovení o právu jednostranně odstoupit od smlouvy nebo smlouvu vypovědět bez výpovědní doby v případě významné změny kontroly nad dodavatelem nebo změny kontroly nad zásadními aktivy využívanými dodavatelem k plnění podle smlouvy je dalším bodem, které je nutné při vzniku smluvního vztahu zohlednit. Povinnost poskytovatele regulované služby na zajištění kontinuity a bezpečnosti regulovaných služeb, je jedním z klíčových aspektů řízení kybernetické bezpečnosti, k čemuž se úzce váže i ochrana poskytovatele regulované služby před nečekanými změnami v dodavatelském řetězci. V kontextu smlouvy s dodavatelem je proto vhodné zakotvit ustanovení umožňující okamžité

ukončení smlouvy v případě významné změny kontroly nad dodavatelem nebo jeho zásadními aktivy. Zakotvením tohoto ustanovení do smluv je eliminována možnost, že by poskytovatel regulované služby byl nucen setrvat ve smluvním vztahu s novým subjektem, jehož vlastnická struktura, bezpečnostní standardy nebo regulatorní požadavky by mohly být neslučitelné s požadavky na kybernetickou bezpečnost a ochranu kritické infrastruktury u poskytovatele regulované služby.

Ustanovení o sankcích za porušení povinností do smluv zajišťuje poskytovali regulované služby vymahatelnost smluvních závazků a odpovědnost dodavatele za bezpečnost poskytovaných služeb. Sankční mechanismy představují účinný nástroj ke snížení bezpečnostních rizik, zajištění provozní stability a ochranu poskytovatele regulované služby před důsledky nesplnění zákonných požadavků. Jasně definované sankce zároveň motivují dodavatele k plnění smluvních povinností a zajišťují regulatorní soulad v oblasti kybernetické bezpečnosti.

Ustanovení o zpřístupnění nebo předání dat na základě žádosti cizozemského orgánu pouze po provedení přezkoumání zákonnosti žádosti zajišťuje ochranu dat, minimalizuje právní rizika a zajišťuje soulad s českým i evropským právním řádem. Zároveň toto ustanovení přispívá k transparentnosti a odpovědnosti při nakládání s citlivými informacemi v rámci regulovaných služeb. Při poskytování regulovaných služeb může dojít k situaci, kdy zahraniční orgán požádá o přístup k datům zpracovávaným mimo území České republiky. Aby se předešlo neoprávněnému nebo nezákonnému přenosu informací, je nutné smluvně stanovit, že jakékoliv zpřístupnění dat bude provedeno až po důkladném přezkoumání zákonnosti žádosti. Do smluvních ujednání je dále vhodné zakomponovat požadavek na ustanovení o zpřístupnění nebo předání dat cizozemskému orgánu až po vynaložení úsilí o zabránění zpřístupnění nebo předání dat v rámci možností daných právním řádem. Toto bezpečnostní opatření zajišťuje ochranu citlivých informací, právní jistotu poskytovatele regulované služby a minimalizaci bezpečnostních rizik. Zároveň posiluje odpovědnost dodavatele za aktivní obranu proti neoprávněným požadavkům a umožňuje efektivní řízení rizik při zpracování dat v zahraniční jurisdikci. V případě, že zahraniční orgán požádá o zpřístupnění dat, existuje riziko neoprávněného přenosu nebo zneužití informací, které by mohlo vést k narušení bezpečnosti, porušení právních předpisů (např. GDPR) nebo kompromitaci důvěrných údajů. Smluvní ustanovení zajišťuje, že i v situaci, kdy je povinnost zpřístupnit citlivá data nevyhnutelná, bude rozsah předání minimalizován, a tím dojde ke snížení možných negativních dopadů. Je tedy nezbytné, aby smlouva obsahovala ustanovení o zpřístupnění nebo předání dat na základě žádosti cizozemského orgánu pouze v nezbytném rozsahu. Toto opatření minimalizuje bezpečnostní rizika, zajišťuje ochranu citlivých informací a podporuje soulad s právním rámcem v oblasti ochrany dat. Současně může být díky tomuto ustanovení nastaven kontrolní mechanismus, který umožňuje poskytovateli regulované služby dohlížet na rozsah a důvodnost předání dat a omezit potenciální negativní dopad.

Tato příloha vychází z přílohy č. 7 k původní vyhlášce a doplňuje ji na základě zkušeností úřadu např. z oblasti cloud computingu.

K příloze č. 6 (Témata pro rozvoj bezpečnostního povědomí)

Na tuto přílohu odkazuje § 10 vyhlášky. Cílem této přílohy je snaha úřadu předat nejlepší praxi získanou vzdělávací činností, vytvořením výčtu nejzásadnějších tematických 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 poskytovatelům regulované služby.