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. 410/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností

Bezpečnostní opatření pro poskytovatele regulované služby v režimu nižších povinností jsou vyjmenována v § 14 odst. 2 *[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. 410/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností (dále jen „vyhláška“) odpovídají ustanovení § 3 a následující. Ačkoliv je výčet bezpečnostních opatření poskytovatelů regulované služby v režimu nižších povinností ve většině případů stejný s názvem bezpečnostních opatření pro poskytovatele regulované služby v režimu vyšších povinností, jsou u poskytovatelů regulované služby v režimu nižších povinností kladeny nižší nároky na úroveň a komplexnost jednotlivých bezpečnostních opatření.

§ 14 odst. 2 *[Seznam bezpečnostních opatření]* zákona – organizační a technická opatření
a) systém zajišťování minimální kybernetické bezpečnosti
b) požadavky na vrcholné vedení
c) řízení aktiv
d) řízení rizik (poznámka: vyhláškou neupraveno)
e) bezpečnost lidských zdrojů
f) řízení kontinuity činností
g) řízení přístupu
h) řízení identit a jejich oprávnění
i) detekce a zaznamenávání kybernetických bezpečnostních událostí
j) řešení kybernetických bezpečnostních incidentů
k) bezpečnost komunikačních sítí
l) aplikační bezpečnost
m) kryptografické algoritmy

K § 1 (Předmět úpravy)

Vyhláška navazuje na zákonem stanovená zmocnění. Jedná se především o stanovení a zavedení přiměřených bezpečnostních opatření a rozsahu, v jakém jsou poskytovatelé regulované služby v režimu nižších povinností povinni zavést a provádět jednotlivá bezpečnostní opatření. S cílem zajištění bezpečnosti regulované služby a aktiv v míře nezbytné pro zajištění kybernetické bezpečnosti regulované služby.

Vyhláška dále stanovuje způsob stanovení významnosti dopadu kybernetického bezpečnostního incidentu pro potřeby hlášení kybernetického bezpečnostního incidentu poskytovatelem regulované služby v režimu nižších povinností, jak plyne ze zákona. Vyhláškou, jejíž předmět úpravy je vymezen v § 1, realizuje Národní úřad pro kybernetickou a informační bezpečnost (dále jen „úřad“) zmocnění, které je mu svěřeno na základě § 13 odst. 3 a § 15 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 i pojmy jako primární aktivum, podpůrné aktivum, technické aktivum a poskytovatel regulované služby podle zákona. 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 účtem lokálního administrátora na své koncové stanici 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 uživatelským účtem tato oprávnění nemá.

Administrátorem se rozumí privilegovaný uživatel nebo osoba, která zajišťuje mj. 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). Privilegovaného uživatele je potřeba chápat jako někoho, 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 tedy není zajišťovat správu, provoz, použití, údržbu a bezpečnost technického aktiva, což je náplní práce a odpovědností administrátora, přičemž administrátor k této činnosti vyžaduje privilegovaná oprávnění, tudíž musí být zároveň i privilegovaným uživatelem. V praxi může 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 následně záleží na kontextu organizace daného poskytovatele regulované služby, zavedených organizačních a technických opatření atd.

Pojem **bezpečnostní politika** v obecném slova smyslu cílí na zajištění bezpečnostních opatření vedoucích k eliminaci rizik. Jejím cílem je zajištění kybernetické bezpečnosti prostřednictvím stanovení zásad, práv a povinností. Je ve vlastním zájmu poskytovatele regulované služby mít vytvořenou a schválenou bezpečnostní politiku, jelikož jen tak lze zaručit její vymáhání.

K § 3 (Systém zajišťování minimální kybernetické bezpečnosti)

Systémem zajišťování minimální kybernetické bezpečnosti je myšleno zajištění minimální úrovně kybernetické bezpečnosti aktiv poskytovatele regulované služby založené na zavedení bezpečnostních opatření. Základem je, že poskytovatel regulované služby při zajišťování kybernetické bezpečnosti zavádí a provádí přiměřená bezpečnostní opatření zohledňující jeho bezpečnostní potřeby. Bezpečnostní opatření jsou definována v § 3 až 13 vyhlášky. V rámci zavádění bezpečnostních opatření musí poskytovatel regulované služby zavést alespoň bezpečnostní opatření podle § 3 odst. 2 až 6 (Systém zajišťování minimální kybernetické bezpečnosti), § 4 (Požadavky na vrcholné vedení), § 5 (Bezpečnost lidských zdrojů), § 6 (Řízení kontinuity činností) a § 10 (Řešení kybernetických bezpečnostních incidentů). Tato bezpečnostní opatření představují naprosté minimum, bez jejichž zavedení není možné naplnit legislativní cíl, kterým je transpozice směrnice NIS 2, jejímž cílem je zvýšení kybernetické bezpečnosti. V rámci § 3 se jedná o stanovení rámce systému zajišťování minimální úrovně kybernetické bezpečnosti a promítnutí kybernetické bezpečnosti do základních procesů organizace, včetně zpracování přehledu bezpečnostních opatření, který je klíčovým dokumentem popisující přístup poskytovatele regulované služby k zavádění bezpečnostních opatření nebo stanovení osoby pověřené za řízení, rozvoj a koordinaci kybernetické bezpečnosti a komunikaci s vrcholným vedením.

Ustanovení § 4 klade vyžaduje aktivní zapojení vrcholného vedení do zajišťování kybernetické bezpečnosti, jelikož podpora vrcholného vedení je zcela klíčová. Častým cílem hackerských útoků jsou uživatelé, proto je v § 5 kladen důraz na rozvoj bezpečnostního povědomí všech zainteresovaných osob. Aby byla organizace schopna zajistit obnovu svojí infrastruktury související se zajišťování kybernetické bezpečnosti regulované služby, je v § 6 stanovena povinnost provádět činnosti související s řízením kontinuity činností. Požadavky § 10 pokrývají oblast řešení kybernetických bezpečnostních incidentů, zejména v souladu se směrnicí NIS 2 určování kybernetických bezpečnostních incidentů s významným dopadem, jejich řešení a hlášení. Vybrané povinné paragrafy dále obsahují provazby do ostatních (tzv. nepovinných) bezpečnostních opatření. U ostatních bezpečnostních opatření uvedených v § 7 až 9 a § 11 až 13 se může poskytovatel regulované služby rozhodnout, že některá z uvedených bezpečnostních opatření aktuálně není možné z relevantních důvodů zavést, avšak toto nezavedení musí řádně zdůvodnit v přehledu bezpečnostních opatřeních, včetně termínů jejich plánovaného zavedení, určení priority a odpovědné osoby. Pokud některé

z bezpečnostních opatření není trvale možné zavést (např. není relevantní), je nutné toto nezavedení rovněž řádně zdůvodnit v přehledu bezpečnostních opatření.

Poskytovateli regulované služby je dále v odstavci 2 tohoto ustanovení uložena povinnost zpracovat přehled bezpečnostních opatření požadovaných touto vyhláškou obsahující alespoň **(i)** přehled všech zavedených bezpečnostních opatření, včetně popisu jejich zavedení, **(ii)** přehled všech bezpečnostních opatření, která budou zavedena, včetně termínů pro jejich zavedení, priority a určení odpovědné osoby, **(iii)** přehled všech nezavedených bezpečnostních opatření, včetně odůvodnění jejich nezavedení. Cílem přehledu je tedy nejen popsat aktuální stav organizace ve vztahu k zákonu a vyhlášce, ale také stanovení systematického a řízeného přístupu k implementaci bezpečnostních opatření. Poskytovatel regulované služby nemusí zavádět všechna bezpečnostní opatření (musí však zavést alespoň bezpečnostní opatření podle § 3 odst. 2 až 6, § 4 až 6 a § 10, jejichž zavedení musí poskytovatel regulované služby v souladu s tímto ustanovením rozplánovat v rámci přehledu bezpečnostních opatření), u ostatních bezpečnostních opatření je nutné rozplánovat jejich zavedení do budoucna, případně zdůvodnit, proč je poskytovatel regulované služby nezavedl. Přehled bezpečnostních opatření může mít podobu dokumentu jak v listinné, tak elektronické podobě a při jeho tvorbě je nutné vycházet z přílohy č. 1 k této vyhlášce. Úřad se při definování minimálních náležitostí a obsahu tohoto dokumentu inspiroval prováděcím předpisem pro poskytovatele regulované služby v režimu vyšších povinností. Poskytovatelé režimu vyšších povinností mají povinnost zpracovat plán zvládání rizik a prohlášení o aplikovatelnosti. Cílem této vyhlášky bylo nastavit pro poskytovatele regulované služby v režimu nižších povinností základní bezpečnostní opatření, jejichž zavádění funguje na jiném principu oproti režimu vyšších povinností. U poskytovatele v režimu nižších povinností se jedná pouze o minimální náležitosti, kdy obsah přehledu bezpečnostních opatření je oproti výše uvedeným dokumentům pro režim vyšších povinností přiměřeně zredukován a jsou vybrány pouze relevantní části.

Aby bylo zajištěno kontinuální zlepšování systému zajišťování minimální kybernetické bezpečnosti, je kladen důraz na provedení každoroční aktualizace přehledu bezpečnostních opatření, včetně vyhodnocení účinnosti zavedených bezpečnostních opatření, které musí být řádně zdokumentováno. V rámci aktualizace přehledu je žádoucí vyhodnotit, zda se v daném období podařilo zavést plánovaná bezpečnostní opatření nebo nikoliv, plány v případě potřeby upravit, a rovněž přezkoumat, zda nepominuly důvody pro nezavedení vybraných bezpečnostních opatření. V souladu s nejlepší praxí je doporučeno, aby v rámci vyhodnocení účinnosti bezpečnostních opatření byly zohledněny mj. i výsledky kontrol v oblasti kybernetické bezpečnosti, výsledky předchozích vyhodnocení účinnosti a posouzení dopadů kybernetických bezpečnostních incidentů na regulované služby. Aby tento přehled plnil svůj účel, měl by obsahovat aktuální informace, vzhledem k tomu, že cílem vyhlášky je mj. snížit administrativní zátěž poskytovatele regulované služby, je stanovena minimální perioda jednoho roku pro jeho aktualizaci.

Za účelem zpětné přezkoumatelnosti (auditovatelnosti) plnění povinností je nutno přehledy bezpečnostních opatření uchovávat alespoň po dobu 4 let, přičemž povinnost se vztahuje na uchovávání těch verzí přehledů, se kterými bylo prokazatelně seznámeno vrcholné vedení.

Základní povinností v odstavci 3 je stanovení bezpečnostní politiky a bezpečnostní dokumentace, která obsahově pokryje oblasti upravené touto vyhláškou. Z pohledu vyhlášky není kladen důraz na to, jak se který dokument jmenuje a v kolika dokumentech jsou dané oblasti řešeny, ale důležitá je obsahová úplnost, čitelnost, snadná identifikovatelnost, vyhledatelnost a logické uspořádání s ohledem na prostředí organizace a zavedené zvyklosti v oblasti řízení dokumentů u poskytovatele regulované služby. Aby bezpečnostní politika

a bezpečnostní dokumentace plnila svůj účel, klade toto ustanovení dále důraz na dodržování stanovených pravidel a postupů a jejich pravidelnou aktualizaci. Pravidelnou aktualizací se rozumí interval, ve kterém dochází k přezkoumání bezpečnostní politiky a bezpečnostní dokumentace a případné revizi. Interval pro pravidelnou aktualizaci bezpečnostní politiky a bezpečnostní dokumentace není stanoven, avšak v souladu s nejlepší praxí by tento interval neměl přesáhnout 1 rok a měla by být prováděna rovněž v souvislosti s prováděnými změnami.

V rámci ustanovení odstavce 3 písm. c) je stanovena povinnost pravidla a postupy uvedené v bezpečnostní politice a bezpečnostní dokumentaci dodržovat a jejich dodržování vynucovat. V případě, že by pravidla a postupy stanovené v bezpečnostní politice a bezpečnostní dokumentaci nebyly v praxi používány, ztratilo by bezpečnostní opatření svůj smysl a ke zvýšení kybernetické bezpečnosti by nedošlo.

Povinnost provést určení primárních a podpůrných aktiv, včetně vazeb mezi nimi je stanovena nově na úrovni zákona. Ustanovení odstavce 4 navazuje dalším procesem, a to stanovením pravidel pro používání a manipulaci s technickými aktivy. Tato pravidla a způsoby je nutno definovat přiměřeně s ohledem na určená aktiva. Těmito pravidly a postupy se rozumí nejen označování technických aktiv, jako příklad lze uvést označování pomocí protokolu TLP („Traffic Light Protocol“), ale i pravidla pro manipulaci s technickými aktivy jak v elektronické podobě, tak fyzické podobě, nebo pravidla pro likvidaci technických aktiv.

V rámci ustanovení odstavce 5 je stanovena povinnost promítnout vhodné požadavky uvedené v příloze č. 2 k této vyhlášce do smluv se všemi dodavateli, jejichž předmět plnění souvisí se zajišťováním kybernetické bezpečnosti, a to na základě zohlednění hrozeb a zranitelností, celkové kvality produktů a postupů v oblasti kybernetické bezpečnosti, včetně postupů bezpečného vývoje spojených s daným dodavatelem. Tato povinnost dopadá nejen na budoucí smlouvy s dodavateli, ale i na uzavřené smlouvy, jejichž obsah je nutné přezkoumat a zohlednit v nich nové povinnosti, které na ně dopadají při zajišťování minimální kybernetické bezpečnosti. Cílem ustanovení je zajistit, aby poskytovatelé regulované služby vyžadovali plnění požadavků zajišťování kybernetické bezpečnosti i po svých dodavatelích. Je žádoucí vyhodnotit možné hrozby a zranitelnosti spojené s tímto dodavatelem, celkovou kvalitu produktů a postupů v oblasti kybernetické bezpečnosti tohoto dodavatele, včetně postupů bezpečného vývoje. Výčet požadavků na smluvní ujednání, který je uveden v příloze č. 2 k této vyhlášce, představuje minimum, které musí být při uzavírání smlouvy přiměřeně zohledněno a posouzeno. Smluvní ujednání vyhodnocená jako relevantní poskytovatel regulované služby zakomponuje do smluv. Jedná se např. o ustanovení zajišťující bezpečnost informací, sankce za porušení smlouvy, ustanovení upravující povinnost dodavatele dodržovat pravidla pro dodavatele stanovená poskytovatelem regulované služby, řízení změn nebo ustanovení o kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy. Je doporučeno požadovat při uzavírání smluv i další ujednání zohledňující specifické požadavky plynoucí ze zajištění provozních a bezpečnostních potřeb souvisejících s regulovanou službou a systémem zajišťování minimální kybernetické bezpečnosti.

Ustanovení v odstavci 6 stanovuje povinnost v oblasti akvizice, vývoje a údržby technických aktiv spadajících do stanoveného rozsahu řízení kybernetické bezpečnosti. Je nutné, aby byly tyto oblasti podpořeny jasnými požadavky na zajištění kybernetické bezpečnosti, jako nedílné součásti jejich rozvoje a bylo vymáháno jejich dodržování. Poskytovatel regulované služby při stanovování bezpečnostních požadavků vychází zejména z požadavků vyhlášky a jejich promítnutí je nezbytné v rámci vývoje i provozu dodávaných produktů.

K § 4 (Požadavky na vrcholné vedení)

Pro prosazování požadavků zajišťování kybernetické bezpečnosti je klíčová podpora vrcholného vedení ve vztahu k systému zajišťování minimální kybernetické bezpečnosti. Potřebu zapojení vrcholného vedení do řízení kybernetické bezpečnosti zdůrazňuje také směrnice NIS 2, která ukotvuje vetší 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 směrnice NIS 2, ale zajistit praktickou vykonatelnost – tedy popsat, jak má vrcholné vedení plnit svoji roli v rámci systému zajišťování minimální kybernetické bezpečnosti, jak má být zapojeno a jaké výstupy má znát či schvalovat, včetně zajištění kontrolovatelnosti tohoto požadavku.

Vrcholné vedení je podle tohoto ustanovení povinno určit osobu pověřenou kybernetickou bezpečností, která v organizaci koordinuje systém zajišťování minimální kybernetické bezpečnosti, dohlíží na jeho stav a rozvoj a komunikuje v této oblasti s vrcholným vedením. Výkonem této činnosti může být pověřena osoba, která prokáže odbornou znalost v oblasti kybernetické bezpečnosti. Za odbornou znalost v oblasti kybernetické bezpečnosti nemusí být považována pouze akademická znalost kybernetické bezpečnosti, ale může se jednat o zisk certifikátu ze školení týkajícího se oblasti kybernetické bezpečnosti nebo doložení znalostí obdobného charakteru. Roli osoby pověřené kybernetickou bezpečností může zastávat také osoba, která nemá odbornou znalost, avšak bez zbytečného odkladu absolvuje odborné školení zaměřené na problematiku kybernetické bezpečnosti. Pro řádný výkon činností by měla být tato osoba vhodně zařazena v organizační struktuře a rovněž disponovat dostatečnými pravomocemi.

Pro prosazování požadavků zajišťování minimální kybernetické bezpečnosti je klíčová podpora vrcholného vedení směrem k osobě pověřené kybernetickou bezpečností a dalším relevantním osobám ve vztahu k systému zajišťování minimální kybernetické bezpečnosti. Proto je zcela na místě klást v tomto ustanovení důraz na zapojení vrcholného vedení, jak prokazatelným poučením o jeho povinnostech a rozsahu odpovědností, tak prokazatelným dohledem nad stavem kybernetické bezpečnosti v organizaci formou seznámení se s přehledem bezpečnostních opatření. Toto ustanovení také zdůrazňuje povinnost na prokazatelné absolvování školení podle § 5 odst. 2 písm. a) vyhlášky. Dále je kladen důraz na podporu vrcholného vedení formou poskytnutí dostatečných zdrojů (zejména finančních nebo personálních). Bez dostatečných zdrojů není možné naplnit požadavky vyhlášky a zajistit kybernetickou bezpečnost v organizaci. Požadavky na potřebné zdroje by měly vycházet zejména z přehledu bezpečnostních opatření. Toto ustanovení dále ukládá vrcholnému vedení povinnost zapojit se do procesu řízení kontinuity činností. Konkrétně se jedná o stanovení priority obnovy primárních aktiv, o kterých by mělo mít vrcholné vedení nejlepší přehled z hlediska jejich dopadu na předmět podnikání poskytovatele regulované služby.

Jelikož režim nižších povinností dopadá na nově regulované orgány a osoby, je velmi důležité, aby si vrcholné vedení bylo vědomo své odpovědnosti plynoucí z legislativy kybernetické bezpečnosti a vytvářelo u poskytovatele regulované služby vhodné prostředí pro kontinuální zlepšování kybernetické bezpečnosti. Ustanovení přiměřeně upravuje požadavky na povinnosti, které dopadají na vrcholné vedení tak, aby bylo schopno informovaně a vědomě rozhodovat o účelném přístupu k zajištění kybernetické bezpečnosti, uvědomovalo si svoji odpovědnost a disponovalo všemi relevantními informacemi pro manažerské rozhodování, nejen o tom, jaké investice jsou účelné a efektivní, ale jak má poskytovatel regulované služby celkově přistupovat k zajištění kybernetické bezpečnosti regulované služby.

K § 5 (Bezpečnost lidských zdrojů)

Podstatou tohoto ustanovení je řízení bezpečnosti lidských zdrojů. Jedná se zejména o průběžné vzdělávání v oblasti kybernetické bezpečnosti a udržování potřebné úrovně bezpečnostního povědomí. Důvodem pro tento požadavek je zejména skutečnost, že velká část kybernetických bezpečnostních incidentů je způsobená vlivem nedostatečného bezpečnostního povědomí uživatelů obecně. Proto se zde cílí nejen na osobu pověřenou kybernetickou bezpečností a administrátory, ale i na zaměstnance.

Politika bezpečného chování uživatelů podle odst. 1 písm. a) tohoto ustanovení je výchozím dokumentem pro řízení bezpečnosti lidských zdrojů. Tato politika by měla reflektovat všechny relevantní body z přílohy č. 3 k této vyhlášce, která obsahuje doporučená témata pro rozvoj bezpečnostního povědomí. Úřad si uvědomuje, že informovaný a proškolený uživatel je jedním z nejefektivnějších způsobů, jak z pohledu kybernetické bezpečnosti eliminovat rizikové chování uživatele, které může mít negativní dopad na celou organizaci. Proto byla vytvořena příloha č. 3 k této vyhlášce obsahující doporučená témata pro rozvoj bezpečnostního povědomí, na kterou je odkazováno v rámci ustanovení odst. 1 písm. a).

Dalším požadavkem je stanovení pravidel rozvoje bezpečnostního povědomí vrcholného vedení, uživatelů, administrátorů a osoby pověřené kybernetickou bezpečností včetně pravidel pro tvorbu hesel, reflektující požadavky stanovené v § 8 vyhlášky. Bezpečnostním povědomím jsou v této vyhlášce myšleny nejen znalosti v oblasti kybernetické bezpečnosti, ale také obecné povědomí ve vztahu k zajišťování kybernetické bezpečnosti konkrétní regulované služby. Pravidla rozvoje bezpečnostního povědomí by měla odrážet specifické prostředí poskytovatele regulované služby a stanovovat, např. typy školení z oblasti kybernetické bezpečnosti, periodu pro jejich absolvování a kdo je povinen se školení účastnit. Toto ustanovení dále požaduje, aby v souladu se stanovenými pravidly byla prováděna vstupní a pravidelná školení v oblasti kybernetické bezpečnosti, která svým obsahem zohlední relevantní témata uvedená v příloze č. 3 k této vyhlášce a bezpečnostní potřeby poskytovatele regulované služby. Do množiny osob, které jsou povinny absolvovat vstupní a pravidelná školení, která zajistí poučení o povinnostech a bezpečnostní politice, je nutné zahrnout také vrcholné vedení. Obsah školení by měl odpovídat cílové skupině (mělo by být zohledněno, zda se jedná např. o běžné uživatele, administrátory nebo o osobu pověřenou kybernetickou bezpečností). Způsob provádění školení, ani cyklus pro jeho opakování není vyhláškou upraven. Měl by být přizpůsoben potřebám dané organizace a zároveň by měl vyplývat z odlišných potřeb jednotlivých skupin uživatelů, administrátorů nebo osoby pověřené kybernetickou bezpečností. Důležitým parametrem je efektivita takového školení. V souladu s nejlepší praxi je doporučené provádět pravidelná školení v oblasti kybernetické bezpečnosti alespoň jedenkrát ročně.

O provedených vstupních a pravidelných školeních v oblasti kybernetické bezpečnosti je nutné vést přehledy. Konkrétní podoba těchto přehledů není vyhláškou stanovena, je však žádoucí, aby bylo patrné kdo, jaké školení a kdy absolvoval. Může jím být např. prezenční listina ze školení, osvědčení o absolvování nebo certifikát. Vyhláškou také není stanoveno, kdo v rámci organizace musí tyto přehledy vést. V praxi tyto přehledy vede zpravidla personální oddělení obdobně jako přehledy o účasti na školeních bezpečnosti a ochrany zdraví při práci nebo požární ochrany.

Další nezbytnou součástí je zajistit administrátorům a osobě pověřené kybernetickou bezpečností dostatečná odborná teoretická i praktická školení. Vzhledem k dynamickému vývoji technologií ICT a požadavkům na zajištění kybernetické bezpečnosti, které v současnosti nabývají stále většího významu, je naprosto nezbytné, aby tyto osoby rozšiřovaly své znalosti a udržovaly si aktuální přehled.

Součástí bezpečnosti lidských zdrojů je v souladu s odst. 1 písm. c) a d) i kontrola dodržování bezpečnostní politiky a stanovení pravidel a postupů pro řešení případů porušení bezpečnostní politiky ze strany uživatelů, administrátorů a osoby pověřené kybernetickou bezpečností (např. disciplinární řízení). Kontrolou dodržování bezpečnostní politiky může být v praxi provádění nahodilého ověřování dodržování stanovených pravidel, např. dodržování zásady čistého stolu a obrazovky, bezpečné nakládání s hesly a odhlašování uživatelů od pracovních stanic. Kontrola dodržování bezpečnostní politiky může být také součástí jiných procesů, jako např. auditní činnosti nejen v oblasti kybernetické bezpečnosti.

Zajištěním výše zmíněných činností by mělo být docíleno dostatečného bezpečnostního povědomí uživatelů a potřebné úrovně znalostí administrátorů a osoby pověřené kybernetickou bezpečností za účelem minimalizace četnosti případných kybernetických bezpečnostních incidentů způsobených zejména lidských faktorem.

K § 6 (Řízení kontinuity činností)

Toto bezpečnostní opatření cílí na schopnost organizace rychle a účinně reagovat na situace související s nepříznivými vlivy, např. přírodními katastrofami nebo kybernetickými bezpečnostními incidenty. V případě nepřipravenosti na takové situace by hrozilo úplné nebo částečné přerušení poskytování regulované služby na nepřijatelně dlouhou dobu. Řízení kontinuity činností je jak proaktivním, tak i reaktivním opatřením pro mimořádné situace.

Základem efektivního řízení kontinuity je stanovení priorit v rámci technických aktiv, které současně s pořadím obnovy a připravenými postupy slouží k co nejrychlejší obnově v případě mimořádné situace. V rámci stanovení priority technických aktiv je nutné přihlédnout také k prioritě relevantního primárního aktiva ve vztahu k danému technickému aktivu, která byla stanovena vrcholným vedením. Pro rychlé a efektivní zvládnutí mimořádné situace je nutné jasně stanovit odpovědnosti a povinnosti konkrétních osob při obnově. Postupy obnovy tvoří zejména plány obnovy, jejichž doporučeným obsahem jsou detailní postupy pro obnovení dat včetně pořadí činností, potřebného času a zdrojů, způsobu ověření úspěšného obnovení dat ze záloh a umístění a popisu záloh. Do plánů obnovy je rovněž doporučeno zahrnout kontakty na odpovědné osoby, včetně kontaktů na dodavatele, kteří jsou pro obnovu potřební. Doporučeno je také tyto plány pravidelně testovat a aktualizovat, jelikož pokud budou postupy a kontaktní informace v těchto plánech neaktuální, nebude možné je v případě mimořádné situace plně využít. V rámci těchto kontaktních údajů je nutné stanovit i dílčí odpovědnosti a povinnosti relevantních osob při obnově daných primárních aktiv.

V neposlední řadě se toto ustanovení věnuje problematice zálohování. Tato oblast 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 následek např. zašifrování (ransomware), tedy nepoužitelnost aktiv. Poskytovatel regulované služby tak musí vytvářet pravidelné zálohy informací, dat, konfigurací a nastavení technických aktiv pro účely případné obnovy nejen po kybernetickém bezpečnostním incidentu. Tyto zálohy mohou být vytvářeny v off-line, on-line nebo hybridním režimu podle potřeb poskytovatele regulované služby, avšak je nutné mít na paměti, že různé metody mají svá rizika. V souladu s nejlepší praxí jsou zálohy často šifrovány, a to z důvodu eliminace rizika spočívajícího v přístupu k informacím organizace, např. v případě odcizení záloh. Je také nutné zajistit oddělení tohoto zálohovacího prostředí od jiných, např. od běžného provozního prostředí, jak je následně uvedeno v § 12 této vyhlášky, který se věnuje bezpečnosti komunikačních sítí.

K § 7 (Řízení přístupu)

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

V souladu s ustanovením odstavce 1 a s nejlepší praxí (např. normy ISO/IEC 27002) musí být přístupová práva a oprávnění uživatelům a administrátorům přistupujícím k aktivům přidělována pouze v rozsahu nezbytně nutném pro výkon činností vyplývajících z popisu pracovního místa nebo smluvního ujednání. Důležité je neudělovat neopodstatněné výjimky a případné výjimky řádně řídit. Nezbytná je i pravidelná kontrola přidělených identit a přístupových oprávnění a bezodkladné odebírání nebo změna přístupových oprávnění při změně pracovní pozice nebo zařazení uživatelů a administrátorů. Obdobný požadavek je v ustanovení uveden i pro případ ukončení nebo změny smluvního vztahu, kdy je důvodem ochrana aktiv před jejich kompromitací a zneužitím. V tomto případě je ovšem požadavek upřesněn na deaktivaci daného účtu a bezodkladné odebrání/změnu přístupových práv a oprávnění, jelikož není na místě uživatelské účty kompletně mazat z důvodu možné zpětné přezkoumatelnosti. Je tak zamezeno dalšímu užívání daného uživatelského účtu a zároveň lze dohledávat, např. v bezpečnostních záznamech o událostech, případné činnosti provedené daným účtem.

Poskytovatel regulované služby musí pro řízení přístupu k aktivům všem uživatelům, administrátorům a technickým aktivům přidělit v souladu s odst. 1 písm. a) jedinečné identifikátory z důvodu jednoznačného stanovení vykonavatele činnosti. Jedinou výjimku z tohoto pravidla mohou tvořit tzv. sdílené technické účty. Jejich použití by však mělo podléhat přísné regulaci a být možné jen ve zcela výjimečných situacích. Dále 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 snižuje např. riziko kompromitace sítě v případě zneužití jeho identity. Tedy když dojde ke kompromitaci uživatelského účtu, zatímco privilegovaný (např. administrátorský) účet též osoby je oddělen v souladu s nejlepší praxí, tak nemůže dojít k zneužití privilegovaných oprávnění daného účtu.

V rámci řízení přístupu technických aktiv musí být řízeny identifikátory, přístupová práva a oprávnění účtů těchto technických aktiv. Obdobně vůči uživatelským a administrátorským účtům musí být i zaváděna bezpečnostní opatření pro řízení přístupů těchto 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 není zavedena heslová politika, 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 (z anglického Mobile Device Management). V případě, že se v rámci organizace využívají technická aktiva, která nemá poskytovatel regulované služby ve své správě, je nezbytné přijmout vhodná bezpečnostní opatření spojená s jejich využíváním (např. tato zařízení umístit do jiného síťového segmentu nebo vynucovat/vyžadovat po uživatelích jejich pravidelnou aktualizaci).

V rámci ustanovení odstavce 2 musí poskytovatel regulované služby v oblasti fyzické bezpečnosti nastavit a vymáhat pravidla a postupy, kterými budou všeobecně chráněna aktiva. Tato pravidla musí být prosazována a dodržována. Poskytovatel regulované služby použije relevantní prostředky fyzické bezpečnosti a zavede adekvátní bezpečnostní opatření, kterými zajistí fyzickou bezpečnost. Prostředky fyzické bezpečnosti se rozumí zejména mechanické zábranné prostředky, zařízení elektrické zabezpečovací signalizace, prostředky omezující působení požárů, prostředky omezující působení projevů živelných událostí nebo systémy pro kontrolu vstupu. Součástí fyzické bezpečnosti je zvážení všech bezpečnostních aspektů jednotlivých lokalit, ve kterých je regulovaná služba provozována. Je klíčové si uvědomit, že k zajišťování kybernetické bezpečnosti je nutné přistupovat komplexně a že bez dostatečného fyzického zabezpečení aktiv může být mnohdy kontraproduktivní investovat do zabezpečení např. na aplikační nebo síťové úrovni.

K § 8 (Řízení identit a jejich oprávnění)

Tyto požadavky stanovují minimální úroveň pro správu a ověření identit, kterou by měli poskytovatelé regulované služby prosazovat. Tento paragraf vychází zejména z kontrolní a metodické činnosti úřadu, doporučení partnerských organizací, standardů publikovaných organizací NIST (např. 800-63B) a nejlepší praxe v oblasti kryptografie a zabezpečení správy a ověřování identit.

U nástroje pro řízení identit, přístupových práv a oprávnění (uživatelů, administrátorů a technických aktiv) je nezbytné, aby jednotlivé identity byly jmenné (jednoznačné i v případě technických účtů) a dalo se rozlišit mezi jednotlivými účty, zejména v případě zpětného dohledání činnosti uživatele, administrátora nebo dodavatele. Je také zapotřebí, aby v rámci tohoto nástroje byly takto vytvořeným jednotlivým identitám přidělena relevantní přístupová práva a oprávnění. V rámci řízení přístupových práv a oprávnění je nutné zajištění řízení práv pro přístup k jednotlivým aktivům a oprávnění pro čtení dat, zápis informací a dat nebo změnu oprávnění (např. známé také z anglického read, write, modify a execute). V praxi se tedy může jednat např. o právo přístupu k datovému úložišti, do konkrétní adresářové složky nebo ke konkrétnímu rozhraní. Toto řízení je důležité zejména za účelem omezení práv a oprávnění u osob bez potřebného need-to-know nebo pracovnímu zařazení. Dále je v tomto ustanovení pro zvýšení úrovně zabezpečení požadováno, aby v případě neúspěšných pokusů o přihlášení byly tyto pokusy řízeny, např. pomocí časového omezení, kdy účet bude po daném počtu neúspěšných pokusů o přihlášení na určitou dobu zablokován, zablokován úplně (např. do odblokování administrátorem) nebo bude jen navýšen časový interval umožňující další pokus. Výběr konkrétního bezpečnostního opatření je na poskytovateli regulované služby v souladu s jeho potřebami. Mezi další požadavky patří také zajištění, že nástroj po stanovené době nečinnosti vyzve, např. uživatele, k opětovnému zadání svých přihlašovacích údajů, aby nedošlo k případné kompromitaci jeho stanice v době, kdy uživatel nebude u své koncové stanice, ale nechal ji omylem odemčenou.

Dále je také stanoven požadavek na odolnost ukládaných a přenášených autentizačních údajů v tomto nástroji, přičemž tento požadavek míří mimo jiné i na tzv. odolnost proti off-line útokům. Pojmem off-line útok je myšlen např. útok, při kterém útočník odcizí databázi hesel a následně má možnost s touto databází manipulovat ve svém zařízení (obecně v jiném prostředí). V případě, kdy k tomuto odcizení dojde a databáze hesel není dostatečně zabezpečena (např. pomocí aktuálně odolných šifrovacích nebo hašovacích funkcí kryptografických algoritmů), se může útočník dostat rovnou ke konkrétním heslům jednotlivých účtů. Proto je v tomto ustanovení uveden požadavek, aby byla zajištěna i odolnost ukládaných autentizačních údajů, tedy aby tyto údaje byly zašifrovány dostatečně silnou šifrou.

Útočník, i když odcizí tuto databázi hesel, se dostane pouze k zašifrovaným údajům (zde je samozřejmě nutné zvolit odolnou kryptografii). Tento požadavek významným způsobem může zvýšit zabezpečení autentizačních údajů.

Z pohledu kybernetické bezpečnosti lze v ustanovení shledat tři úrovně nastavení správy a ověřování identit. V první řadě je zakotveno úsilí směřující k využívání autentizačního mechanismu založeného na vícefaktorové autentizaci s nejméně dvěma různými typy faktorů. Různými typy autentizačních faktorů je myšleno ověření identity na základě něčeho, co daný uživatel zná (např. heslo, PIN), čím je (např. biometrický údaj) nebo co vlastní (např. token). Tento způsob je z pohledu kybernetické bezpečnosti v současné době nejvhodnější a používání pouze jednoho autentizačního faktoru v podobě identifikátoru účtu a hesla se v jeho porovnání nepovažuje za dostatečně bezpečné např. při možné kompromitaci nebo úniku hesel. 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 systému v případech kdy by potenciální útočník dokázal překonat autentizační mechanismus sloužící pro prvotní ověření identity.

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

Dále jsou ve vyhlášce pro případy, kdy není možné použít z určitého důvodu ani autentizaci pomocí kryptografických klíčů a certifikátů stanovena pravidla, která je nutné vynucovat v případě autentizace za pomocí pouze identifikátoru účtu (např. přihlašovacího jména) a hesla. Tento způsob z bezpečnostního hlediska není ideální, protože je ve velké míře závislý na samotných uživatelích, kteří heslo vytváří a nakládají s ním. Z těchto důvodů jsou stanoveny požadavky, které je nutné dodržet a technicky vynucovat. Jde zejména o minimální délku hesla, skladbu hesla, pravidla pro tvorbu a životnost hesel atp. Minimální délka hesla byla pro uživatele stanovena na 12 znaků z toho důvodu, že při výpočetním výkonu 1,5 Th/s a typu hashe NTLM (NT Lan Manager, který je dnes běžně využívaný) s délkou hesla 8 znaků a využití komplexity, bude trvat prolomení tohoto hashe 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. K těmto příkladům je však nutné uvést ještě několik 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 „každé dva roky dojde ke zdvojnásobení počtu tranzistorů na čipu“, z toho plyne, že se doba prolomení hashe bude i nadále zkracovat. Tato varianta výpočtu taktéž nepočítá s tím, že by útočník využil např. slovník, který může také výrazně snížit dobu prolomení hashe. Vzhledem k faktům popsaným výše je u administrátorů stanoven požadavek na délku hesla na 17 znaků a pro účty technických aktiv na 22 znaků, což při dodržení komplexity odpovídá entropii na úrovni zhruba 128 bitů. Za účelem zvýšení komplexity hesel a tím i ztížení využití např. slovníkových útoků je dalším požadavkem, aby nástroj, který je využíván k ověření identity umožnil uživateli při tvorbě hesla možnost vybírat nejen malá a velká písmena, číslice, ale i běžné speciální znaky. Je nezbytné, aby změna hesla byla prováděna pravidelně, a to nejpozději do 18 měsíců

z důvodu možné kompromitace, které si poskytovatel regulované služby nemusí být vědom. 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 vícefaktorové autentizace a implementují se bezpečnostní opatření postavená na principu nulové důvěry neboli 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.

Toto ustanovení dále požaduje, aby výchozí hesla technických aktiv byla bezodkladně změněna a jejich nové heslo bylo v případě autentizace pomocí identifikátoru účtu a hesla tvořeno náhodným řetězcem složeným z malých a velkých písmen, číslic a speciálních znaků. Zejména z důvodu, kdy výchozí hesla technických aktiv jsou součástí veřejné dokumentace aktiva výrobce a lze je tak snadno dohledat. Dále je požadavek na komplexitu, zejména v délce, důležitý, jelikož u hesel technických aktiv nejsou často aplikovatelné požadavky např. na znovu ověření účtu při stanovené době nečinnosti nebo se často tyto účty nezablokují při neúspěšných pokusech o přihlášení.

Nastavení by mělo být tedy takové, že čím je větší počet možných změn hesla, tím by měl být počet hesel, která budou „uložena v paměti“ větší. Další požadované pravidlo je, aby uživatelům a administrátorům nebylo umožněno zvolit si jednoduchá a často používaná hesla. Tento požadavek je ve vyhlášce uveden z toho důvodu, aby se předešlo používání hesel, která jsou zveřejněna ve slovnících často používaných hesel (mezi těmito hesly jsou např. „admin“, „heslo1234“, „123456“, „123123“, „P@$$w0rd“). Dále je zde ze stejných důvodů požadavek i na neumožnění použití hesel na základě mnohonásobně opakujících se znaků, přihlašovacího jména, e-mailu nebo názvu systému. V rámci tohoto ustanovení je uveden požadavek na znemožnění použití dříve používaných hesel s pamětí alespoň 12 předchozích hesel.

Další část tohoto ustanovení požaduje, aby byla dodržena důvěrnost při vytváření výchozích autentizačních údajů a při obnově přístupu. Např. při vytváření přístupových údajů pro nové zaměstnance, pověřená osoba vytvoří a předá jejich prvotní hesla např. pomocí SMS, e-mailu nebo na papíře, tím je ale narušena důvěrnost těchto „nových“ hesel. Pokud navíc nedochází k technicky vynucené změně těchto hesel, můžou takto vytvořená hesla být platná po celou dobu jejich životnosti a může je znát pověřená osoba, která je vytvořila. Dalším požadavkem je změna výchozích hesel, která je důležitá k zajištění důvěrnosti používaných hesel, jelikož existují zdroje, ze kterých lze zjistit výchozí hesla některých technických aktiv. 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 nebo identifikátoru sloužícího k obnově přístupu nebo pro zřízení přístupu po jeho prvním použití nebo po uplynutí 24 hodin je zde z toho důvodu, aby heslo nebo identifikátor nebyl zneužitelný např. pokud by se útočník dostal k e-mailu, ve kterém by toto heslo nebo identifikátor ve formě odkazu byl uveden.

Dalším požadavkem v rámci tohoto ustanovení je povinnost bezodkladné změny přístupového hesla při podezření na jeho kompromitaci, kdy se jedná o standardní bezpečnostní opatření zamezující zneužití potenciálně kompromitovaných hesel.

V neposlední řadě se toto ustanovení věnuje zabezpečení administrátorských účtů určených zejména pro případ obnovy po kybernetickém bezpečnostním incidentu, tedy např. „super admin“ nebo „root“. Tyto účty by měly být používány pouze v nezbytně nutných případech, pro velmi omezený rozsah činností a nemělo by s nimi být za jiných okolností nadbytečně manipulováno. Při nadměrném využívání se zvyšuje riziko možné kompromitace účtu, což s takto vysokým stupněm oprávnění může představovat riziko pro celou komunikační síť nebo i celou infrastrukturu organizace.

K § 9 (Detekce a zaznamenávání kybernetických bezpečnostních událostí)

V rámci tohoto ustanovení je požadováno nasazení nástrojů, které jsou schopny detekovat kybernetické bezpečnostní události, které mohou vést ke kybernetickým bezpečnostním incidentům a tyto události umí tyto nástroje buď jen detekovat nebo jim současně mohou účinně čelit.

Z hlediska kategorizace je možné využít tyto nástroje na úrovni komunikačních sítí, kdy je požadavkem tohoto ustanovení, aby bylo zajištěno ověření a kontrola přenášených dat (tedy schopnost ověřit a kontrolovat příchozí a odchozí komunikaci) zejména na perimetru komunikační sítě a současně docházelo k blokování nežádoucí komunikace. Typickými příklady nástrojů a prostředků pro zajištění tohoto požadavku jsou např. různé síťové sondy, nástroje pro síťovou analýzu, moduly a nástroje pro detekci/prevenci průniku (IDS/IPS) a firewally. Nicméně je doporučeno obdobně postupovat nejen na perimetru sítě, ale také v komunikační síti, jelikož kybernetická bezpečnostní událost, potažmo i případný kybernetický bezpečnostní incident, se může vyskytnout i pouze v interní síti např. když by byly server nebo koncová stanice uvnitř sítě kompromitovány ještě před zveřejněním signatury nebo pravidla, která by jeho přítomnost na perimetru sítě odhalila nebo v případě, kdy na perimetru nebylo vůbec možné nežádoucí komunikaci detekovat z důvodu šifrování této komunikace během přenosu. Tato kompromitace pak může být neaktivní několik týdnů a až poté se začne v komunikační síti šířit. Je tedy v zájmu poskytovatele regulované služby tyto události detekovat v rámci celé komunikační sítě regulované služby a náležitě s nimi dále pracovat v rámci zvyšování své úrovně kybernetické bezpečnosti.

Další kategorií nástrojů jsou ty, které jsou nasazené v rámci technických aktiv, zejména na serverech a koncových stanicích za účelem nepřetržité a automatické ochrany před škodlivým kódem. Do této kategorie patří např. nástroje pro detekci škodlivého kódu, antivirové programy, EDR, XDR, nástroje pro detekci anomálií, nástroje pro behaviorální analýzu. Úřad současně doporučuje provádět tuto detekci a zavést tuto ochranu i na jiná relevantní technická aktiva např. na mobilní zařízení, pokud jsou využívána v rámci poskytování regulované služby.

Dalším požadavkem tohoto ustanovení je udržování aktuálnosti u všech výše zmíněných detekčních a ochranných nástrojů zajištěním jejich pravidelné aktualizace, a to včetně detekčních pravidel.

Poskytovatel regulované služby také musí řídit automatické spouštění obsahu, ať už např. při připojení vyměnitelného zařízení, datových nosičů nebo také spouštění maker při otevírání souborů nebo jiného druhu spustitelného kódu. Jedná se např. o ochranu, která může zabránit případnému kompromitovanému souboru, který by se mohl automaticky spustit a rozšířit svůj škodlivý kód na dané koncové stanici. Může taktéž sloužit k ochraně při manipulaci s datovými nosiči (např. flash disk, velkokapacitní paměťová zařízení nebo paměťové karty), kdy může být např. nedopatřením uživatele zavedeno kompromitované médium do koncové stanice, což by mohlo ohrozit interní síť regulované služby. V případě vyměnitelných zařízení (např. myš, klávesnice, tiskárna nebo externí Wi-Fi karta) je nutné brát v potaz, že i tato zařízení mohou obsahovat paměťové médium (např. pro uložení uživatelských profilů) nebo se může jednat o kompromitovaná zařízení, jež umožní např. navázat vzdálenou komunikaci s potenciálním útočníkem a poskytovat mu záznam činnosti koncové stanice. Obecné doporučení a praxe je omezení uživatelů, kteří smí vyměnitelná zařízení, spouštění maker a jiných spustitelných kódů využívat, nasazení nástrojů, které zakazují nebo alespoň omezují jejich spuštění. Dále je také doporučeno v případě četné potřeby využívání flash disků nebo

jiných paměťových médií, které nemá organizace ve své správě využívat tzv. antivirové pračky (koncová stanice s několika nástroji, které slouží k detekci škodlivého kódu) a taková média podrobit testu, než jsou zapojena do koncové stanice uživatele. Lze také přímo v nastavení nástroje pro nepřetržitou automatickou ochranu před škodlivým kódem nastavit automatickou kontrolu připojovaných vyměnitelných zařízení. Zavedením tohoto bezpečnostního opatření se může mimo jiné snížit i riziko plynoucí ze situací, kdy by bylo kompromitované vyměnitelné zařízení fyzicky zavedeno do koncové stanice přímo útočníkem.

Dále je požadováno, aby byly informace o relevantních detekovaných kybernetických bezpečnostních událostech, např. z detekčních nástrojů, nepřetržitě poskytovány relevantním osobám a včasně je varovaly, aby mohla být zaručena dostatečně rychlá reakce na tyto události. Může se jednat např. o modelovou situaci, kdy detekční nástroj EDR zahlásí varování na detekovanou událost, jelikož byl zachycen škodlivý kód nebo virus a relevantní osobě přijde upozornění; z helpdesku přijde e-mail určené osobě, že nástroj nebo uživatel zaznamenal podezřelé chování koncové stanice. V případě opožděné reakce by mohlo dojít ke vzniku kybernetického bezpečnostního incidentu, který by měl dopad na kybernetickou bezpečnost regulované služby nebo by mohlo dojít k rozšíření dané kompromitace na další technická aktiva v rámci interní sítě.

V rámci tohoto ustanovení je také v souladu s předchozími požadavky na detekci kybernetických bezpečnostních událostí zapotřebí zaznamenávat jak bezpečnostní, tak relevantní provozní události. Ačkoliv by detekce kybernetických bezpečnostních událostí měla být podle tohoto ustanovení prováděna zejména na serverech a koncových stanicích, poskytovatel regulované služby může na základě svých bezpečnostních potřeb zaznamenávat bezpečnostní a relevantní provozní události i u takových technických aktiv, která mohou významně ovlivnit bezpečnost regulované služby (např. páteřní switche). Tyto záznamy musí obsahovat podle požadavků tohoto ustanovení datum a čas, včetně specifikace časového pásma (někdy se stává, že technická aktiva automaticky nepřevádí mezi letním a zimním časem, proto je nutný jednoznačný identifikátor). Dále je nutno, aby ze záznamu bylo jasné, o jaký typ činnosti se jedná, zdali tato činnost byla úspěšná a ze kterého technického aktiva a účtu pochází. U případů, kdy je identita dynamicky měněna, je nutné zajistit její jednoznačnost pro případy zpětného přezkumu. Tyto záznamy je poskytovatel regulované služby povinen uchovávat po dobu, kterou si na základě svých bezpečnostních potřeb stanoví. Důvod, proč je nutné zaznamenávat i relevantní provozní události je, že např. v případě vzniku kybernetického bezpečnostního incidentu mohou tyto záznamy představovat zásadní důkazy pro forenzní analýzu. Mezi relevantní bezpečnostní události se mohou řadit např. výpadek konektivity, abnormální zatížení linky nebo výrazně zvýšená teplota technických aktiv.

K § 10 (Řešení kybernetických bezpečnostních incidentů)

Základním požadavkem tohoto ustanovení je nastavení procesu řešení kybernetických bezpečnostních incidentů. Toto ustanovení doplňuje problematiku kybernetických bezpečnostních incidentů popsanou v zákoně, konkrétně v § 15, 16 a 17. Základním předpokladem pro to, aby mohly být kybernetické bezpečností události a incidenty vůbec řešeny je, aby o nich poskytovatel regulované služby věděl. Je tedy nutné, aby podle požadavku písmene a) bylo zajištěno, že všechny zainteresované strany (uživatelé, administrátoři, osoba pověřená kybernetickou bezpečností a dalších zaměstnanci, včetně relevantních dodavatelů) oznamují neobvyklé chování technických aktiv a podezření na jakékoliv zranitelnosti. Cílem tohoto ustanovení je zajistit informovanost osob odpovědných za řešení kybernetických bezpečnostních incidentů, a tedy zajištění jejich praktického řešení. Jedná se o nastavení procesu a stanovení povinností v rámci bezpečnostní politiky nebo smluvního vztahu a poučení

zainteresovaných stran o těchto procesech a povinnostech, které z nich plynou. Způsob a forma oznamování podezřelého chování zainteresovanými stranami směrem k odpovědným osobám a samotné řešení je ponecháno na poskytovateli regulované služby. V praxi může být realizováno prostřednictvím nejrůznější kanálů např. telefonicky, osobně, e-mailem nebo pomocí service desk.

Dále se zde rozlišují kybernetické bezpečnostní incidenty a kybernetické bezpečnostní incidenty s významným dopadem, přičemž jednotlivé povinnosti jsou ve vztahu k těmto dvěma skupinám rozdílné, a to z důvodu snížení zátěže na poskytovatele regulované služby. Vzhledem k této skutečnosti je nezbytné, aby poskytovatel regulované služby vytvořil podle písmene b) tohoto ustanovení metodiku pro posuzování kybernetických bezpečnostních incidentů v souladu s požadavky § 14 této vyhlášky a zajistil posuzování detekovaných kybernetických bezpečnostních událostí a incidentů v souladu s touto metodikou. Poskytovatel regulované služby zajistí řešení všech kybernetických bezpečnostních incidentů, přičemž řešením kybernetického bezpečnostního incidentu se rozumí zejména kroky směřující k obnově poskytování regulovaných služeb narušených kybernetickým bezpečnostním incidentem. Avšak pouze kybernetické bezpečnostní incidenty s významným dopadem je poskytovatel regulované služby povinen podle § 15 zákona hlásit Národnímu CERT. U kybernetických bezpečnostních incidentů s významným dopadem je poskytovatel regulované služby rovněž v souladu s písmenem f) tohoto ustanovení povinen vytvořit závěrečnou zprávu o kybernetickém bezpečnostním incidentu, včetně popisu jeho příčiny vzniku, pokud je známá.

Aby mohly být kybernetické bezpečnostní incidenty řešeny, musí být nejprve podle písmene c) tohoto ustanovení zajištěna detekce kybernetických bezpečnostních událostí. Povinnost detekce je blíže specifikována v § 9 této vyhlášky.

K § 11 (Bezpečnost komunikačních sítí)

Se zajištěním kybernetické bezpečnosti aktiv úzce souvisí zabezpečení komunikační sítě, která je tvořena technickými aktivy regulované služby a využívá se zejména k provozování regulované služby a práci s ní. Tato oblast je upravena na základě standardů v oblasti síťových komunikací a nejlepších praktik (např. normy ISO/IEC 27002). V tomto paragrafu jsou popsány obecné a nezbytné základy pro zajištění minimální bezpečnosti komunikace jako takové a komunikačních sítí.

Podle tohoto ustanovení je požadováno zajištění segmentace komunikační sítě, což znamená její rozdělení do jednotlivých síťových segmentů např. na základě důvěryhodnosti (např. řízený segment s přímým přístupem do veřejného internetu tzv. DMZ, 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. oddělením provozního prostředí od zálohovacího (nebo také vývojové a testovací 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). 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 na jejím perimetru (potažmo s externí komunikační sítí), současně také i mezi jednotlivými prostředími.

S tím je spojen další požadavek, kdy odchozí a příchozí komunikace na perimetru komunikační sítě musí být omezena na nezbytnou pro řádné zajištění poskytování regulované služby. Jedním z vektorů útoku může být případ, kdy si např. uživatel stáhne škodlivý kód z veřejného

internetu. Omezení komunikace na pouze schválenou a nezbytně nutnou pro provoz regulované služby, tak může vést ke značné redukci např. případného nechtěného načtení závadné webové stránky nebo omezení nežádoucí vnější komunikace do interní sítě. Byť je požadavek pro poskytovatele regulované služby v režimu nižších povinností omezen na perimetr komunikační sítě, úřad doporučuje toto bezpečnostní opatření aplikovat také pro interní komunikační síť, jelikož se jedná o běžně využívaný postup a nejlepší praxi v oblasti při zabezpečení síťové komunikace, který je také v souladu např. s principy nulové důvěry neboli tzv. zero-trust. Navíc toto bezpečnostní opatření slouží ke zvýšení úrovně kybernetické bezpečnosti u poskytovatele regulované služby, jelikož dojde k omezení případného šíření nebezpečného kódu nebo útočníka v komunikační síti.

Dalším požadavkem je využití aktuálních a odolných síťových protokolů, potažmo aktuálních a odolných kryptografických algoritmů, zejména k zajištění důvěrnosti a integrity síťové komunikace. Jsou tím myšleny především různé zabezpečené síťové protokoly nebo šifrování síťové komunikace, aby např. nemohlo dojít k odposlechnutí komunikace v rámci autentizace, tedy kompromitaci přístupových hesel uživatele nebo administrátora. Takto získaná hesla by mohla být následně zneužitá útočníkem k získání kontroly nad daným aktivem, případně nad celou interní sítí.

Vzdálený přístup (např. VPN vzdálené připojení do interní komunikační sítě) a vzdálená správa technických aktiv (např. prostřednictvím vzdálené plochy, terminálového SSH připojení na server) musí být omezena na nezbytně nutnou míru. Další požadavek tohoto ustanovení opět zdůrazňuje nutnost, aby poskytovatel regulované služby také zabezpečil (zejména důvěrnost a integritu) vzdálené připojení a vzdálenou správu technických aktiv. Na závěr také požaduje vést přehled o uživatelích a administrátorech, kteří tato vzdálená připojení nebo vzdálenou správu využívají, např. mít aktuální jmenný přehled o jednotlivých dodavatelích spravujících servery nebo o uživatelích, kteří např. disponují VPN klientem a vzdáleně se přihlašují do interní sítě, jelikož mohou mít povolenou práci z domů.

K § 12 (Aplikační bezpečnost)

Jedním z požadavků tohoto ustanovení je bezodkladné aplikování schválených bezpečnostních aktualizací, kdy např. v rámci vydaných bezpečnostních záplat je výrobcem nebo dodavatelem ošetřena zjištěná zranitelnost. Za schválenou aktualizaci lze považovat takovou, která např. pochází od výrobce nebo smluvního dodavatele daného aktiva a poskytovatel regulované služby po otestování jeho funkčnosti a bezpečnosti schválil jeho nasazení v provozním prostředí. Je vhodné také ověřovat jejich tzv. hash „otisk“ (např. MD5), kdy po stažení může poskytovatel regulované služby ověřit, že nedošlo k podvržení nebo narušení integrity aktualizačního balíčku.

Aplikační bezpečnost se dotýká oblastí jak software, tak i hardware (technické a programové prostředky a vybavení), u kterých je nutné, aby technická aktiva byla podporována, ať už výrobcem, dodavatelem nebo jinou osobu (např. aktivní komunitou v případě open-source licence). U nepodporovaných technických aktiv totiž není možné zaručit jistou úroveň bezpečnosti, jelikož pro ně nejsou vydávány bezpečnostních záplaty a aktualizace. Z tohoto důvodu je povinností poskytovatele regulované služby, v rámci tohoto ustanovení, vést evidenci technických aktiv, která již nejsou podporována a zavádět u nich bezpečnostní opatření, která se na tuto problematiku zaměřují, např. omezením přístupů k danému technickému aktivu a současně prostřednictvím segmentace komunikační sítě, kdy jsou nepodporovaná technická aktiva oddělena ve vlastním segmentu, který není považován za zabezpečený. Obecně musí poskytovatel regulované služby zavést taková bezpečnostní

opatření, aby zajistil obdobnou nebo vyšší úroveň bezpečnosti, pokud nemůže zajistit aktuálnost a podporu těchto aktiv, která tak mohou být zranitelná. Dále je pak požadováno v navazujícím ustanovení, aby poskytovatel regulované služby omezil komunikaci těchto nepodporovaných technických aktiv na nezbytně nutnou a omezil tak zbytečné síťové prostupy, které mohou případní útočníci zneužít k jejich kompromitaci.

Dále je v tomto ustanovení podle písmene c) uvedena povinnost provádět skenování zranitelností relevantních technických aktiv, a to např. v interní síti nebo z externí komunikační sítě, což lze provést i formou veřejně dostupných nástrojů pro skenování zranitelností konkrétních IP rozsahů, kdy tyto nástroje mohou poskytovateli regulované služby říct, jak jsou jeho technická aktiva zranitelná z pohledu běžného útočníka (např. otevřené porty, zranitelné operační systémy, nezabezpečené vzdálené přístupy nebo zranitelná aktiva vystavená do veřejného internetu). U této povinnosti není stanoven požadavek na pravidelný interval, ovšem v praxi je provádění skenování zranitelností finančně nenáročný proces realizovatelný pomocí veřejně dostupných nástrojů, tudíž je doporučeno si tento interval stanovit (např. na týdenní, měsíční nebo kvartální bázi) a zavést skenování zranitelností jako součást běžných procesů, a to včetně následného zavádění přiměřených bezpečnostních opatření na základě zjištěných výsledků.

K § 13 (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 bylo prosazováno bezpečné nakládání s kryptografickými algoritmy, např. stanovením pravidel a postupů pro užívání kryptografických algoritmů a působením na uživatele cestou vzdělávání v této oblasti. Toto ustanovení dále odkazuje na doporučení úřadu v oblasti kryptografických algoritmů (např. dokument Minimální požadavky na kryptografické algoritmy), které úřad zveřejňuje na svých webových stránkách a podle vývoje v této oblasti je na základě odborné výzkumné činnosti aktualizuje. Vzhledem k dynamickému vývoji této problematiky nejsou tato doporučení zahrnuta ve vyhlášce, ani jejích přílohách, právě z důvodu potřeby četnějších aktualizací a doplnění o relevantní informace. V této souvislosti platí, že poskytovatelé regulovaných služeb by měli mít přehled o využívaných kryptografických algoritmech ve své organizaci, adekvátně reagovat na nové hrozby a zranitelnosti, a současně zohledňovat doporučení a metodiky vydané úřadem.

Dále je stanovena povinnost zajistit zabezpečení hlasové, audiovizuální a textové komunikace. Toto ustanovení explicitně zahrnuje e-mailovou komunikaci, která je velice často využívána pro předávání informací nejen v rámci poskytovatele regulované služby a její zabezpečení bývá opomíjeno, zejména pak zachování její důvěrnosti a integrity. Poskytovatel regulované služby musí současně zajistit i bezpečnou nouzovou komunikaci v rámci své organizace. 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. Jedná se např. o nasazení S/MIME či jiné 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 kupříkladu nastavení interních bezpečnostních nástrojů, výsledky z penetračních testů nebo jiné citlivé informace.

K § 14 (Stanovení významnosti dopadu kybernetického bezpečnostního incidentu)

Ustanovení zakotvuje způsob určení významnosti dopadu kybernetického bezpečnostního incidentu na poskytování regulované služby. Určení významnosti dopadu je stěžejní pro případnou aktivaci dalších povinností v procesu hlášení kybernetických bezpečnostních incidentů. Pravidla a postupy pro identifikaci a klasifikaci kybernetických bezpečnostních incidentů s významným dopadem jsou součástí politiky zvládání kybernetických bezpečnostních incidentů. Poskytovatel regulované služby má podle § 10 této vyhlášky pro posuzování kybernetických bezpečnostních událostí a incidentů povinnost vypracovat metodiku, jejíž součástí je i stanovení významnosti dopadu kybernetického bezpečnostního incidentu.

Pro potřeby vyhodnocení významnosti dopadu kybernetického bezpečnostního incidentu na poskytování regulované služby je nejprve nutné stanovit únosnou míru újmy způsobenou kybernetickým bezpečnostním incidentem. Únosná míra újmy je souhrn nejvyšší škody a nemajetkové újmy vzniklé v souvislosti s kybernetickým bezpečnostním incidentem. Nejvyšší škodu v tomto případě představuje celková finanční ztráta nebo náklady, které vzniknou v důsledku kybernetického bezpečnostního incidentu. Nemajetková újma představuje nepřímou finanční ztrátu. Jde tedy o škody, které mohou zahrnovat poškození reputace, ztrátu důvěry zákazníků nebo jiné formy nehmotných ztrát.

Následuje stanovení oblastí pro posouzení významnosti dopadu kybernetických bezpečnostních incidentů na organizaci zohledňující provozní dopad, množství zasažených osob, zdroje potřebné pro obnovu, typ a umístění dotčených aktiv (které mohou být ovlivněny kybernetickým bezpečnostních incidentem, ale nebyly přímo zasaženy), citlivost zasažených informací a dat a přímou příčinu kybernetického bezpečnostního incidentu, je-li poskytovateli regulované služby známa.

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

Uvedené požadavky na stanovení oblastí pro posouzení významnosti incidentu vycházejí ze systému americké Agentury pro kybernetickou bezpečnost a infrastrukturu (CISA). Jedná se o mezinárodně uznávaný model, jehož funkčnost je ověřena v praxi. Únosná míra újmy v kombinaci s oblastmi pro posouzení významnosti naplňuje požadavky směrnice NIS 2 na stanovení významnosti kybernetického bezpečnostního incidentu.

K § 15 (Účinnost)

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

K příloze č. 1 (Přehled bezpečnostních opatření)

Tato příloha představuje přehled bezpečnostních opatření ve formě tabulky (Tab. č. 1), která má poskytovateli regulované služby sloužit jako nástroj k vyhodnocení účinnosti zavedených bezpečnostních opatření za stanovené období. Přehled bezpečnostních opatření má být každoročně aktualizován, aby byl zajištěn princip neustálého zlepšování a aby měl poskytovatel regulované služby přehled o aktuální situaci v rámci zajišťování kybernetické bezpečnosti. Interval aktualizace je možné zkrátit podle potřeb povinné osoby.

První sloupec tabulky „Přehled bezpečnostních opatření“ slouží pro zápis bezpečnostních opatření požadovaných touto vyhláškou a je nezbytné do něj zanést všechna bezpečnostní opatření formou odkazu do vyhlášky. Druhý sloupec slouží k uvedení stavu zavedení bezpečnostního opatření. V tomto sloupci poskytovatel regulované služby na základě

posouzení skutečného stavu uvede, zda bylo dané bezpečnostní opatření zavedeno, nezavedeno nebo zda je v procesu implementace. Následuje sloupec s popisem bezpečnostního opatření. V případě, že je dané bezpečnostní opatření označeno jako zavedeno, bude v tomto sloupci popsán způsob jeho zavedení. Způsob zavedení lze popsat také prostřednictvím odkazu do příslušné bezpečnostní politiky nebo bezpečnostní dokumentace. V případě, že dané bezpečnostní opatření zavedeno není, je nutné tuto skutečnost v tomto sloupci řádně zdůvodnit. Pokud je bezpečnostní opatření označeno jako „v procesu“, je nutné popsat např. v jaké fázi se poskytovatel regulované služby v daném procesu nachází. Následující tři sloupce přehledu bezpečnostních opatření jsou relevantní pouze v případě, že je zavádění daného bezpečnostního opatření v procesu. V takové situaci je pak nutné uvést plánovaný termín zavedení bezpečnostního opatření, prioritu zavedení bezpečnostního opatření a osobu odpovědnou za zavedení bezpečnostního opatření. Způsob prioritizace je na uvážení poskytovatele regulované služby, je však nutné, aby byl pro danou organizaci funkční a podporoval efektivitu zajišťování kybernetické bezpečnosti. Jednou z možností je využití prioritizace na základě důležitosti daného aktiva nebo využití číselné škály např. v rozmezí 1-10, případně jiný způsob, který bude dané organizaci vyhovovat. Osoby pověřené za zavedení jednotlivých bezpečnostních opatření by měly být zahrnuty jak do procesu pravidelného vyhodnocení účinnosti zavedených bezpečnostních opatření, tak také do aktualizace přehledu bezpečnostních opatření.

Přehled bezpečnostních opatření – VZOR

Vyhodnocení účinnosti zajišťování kybernetické bezpečnosti					2025
Bezpečnostní opatření podle vyhlášky	**Stav bezpečnostního opatření**	**Popis bezpečnostního opatření**	**Termín zavedení bezpečnostního opatření**	**Priorita zavedení bezpečnostního opatření**	**Odpovědnost za bezpečnostního opatření**
§ 5 písm. a)	Zavedeno	Politika bezpečného chování uživatelů je v dokumentu BP04_Bezp_lidskych_zdroju v kapitole „1 - Politika bezpečného chování uživatelů“ a jsou v ní zohledněna relevantní témata z přílohy č. 3.	-	-	-

§ 5 písm. b)	Zavedeno	Pravidla rozvoje bezpečnostního povědomí jsou stanovena v dokumentu Bezp_lidskych_zdroju v kapitole „2 - Rozvoj bezpečnostního povědomí“, kde jsou také pravidla pro tvorbu hesel, konkrétně v podkapitole „2.1. Pravidla pro tvorbu hesel“.	-	-	-
§ 8 odst. 2	V procesu	V současnosti společnost zavádí vícefaktorovou autentizaci.	Q2 2025	1	Petr Horák (IT oddělení)
§ 8 odst. 4 písm. a) bod 2	Nezavedeno	Starší SCADA ve výrobě neumožňuje zadání hesla o délce více než 12 znaků.	-	-	-
§ 9 odst. 1 písm. c)	Zavedeno	Spouštění obsahu z vyměnitelných zařízení je na všech noteboocích zakázáno, a to podle dokumentu XXX.	-	-	-

K příloze č. 2 (Požadavky na smluvní ujednání s dodavateli)

Obsahem této přílohy je přehled základních bezpečnostních opatření pro smluvní vztahy jejichž předmět plnění souvisí se zajišťováním kybernetické bezpečnosti.

Tato příloha vznikla na základě nejlepší praxe. V příloze je popsán příkladný výčet ustanovení, která by měla obsahovat každá dodavatelská smlouva jejíž předmět plnění spadá do stanoveného rozsahu řízení kybernetické bezpečnosti určeného postupem podle § 12 zákona.

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 jeho dodavatelem při sdílení dokumentů a informací získaných v průběhu plnění smlouvy.

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

Ustanovení upravující řetězení dodavatelů je ve smlouvách důležité z toho důvodu, že poskytovatel regulované služby vybírá dodavatele např. podle určitých kritérií, která kladou jisté nároky 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 zajišťování minimální kybernetické bezpečnosti.

Ustanovení o specifikaci podmínek z pohledu bezpečnosti informací 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 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, kybernetických 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, zajištění odpovědnosti a právní ochrany a řízení dodavatelů v rámci přechodného období.

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 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 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 důvěrnosti smluvního vztahu je vhodné zahrnout do smluv uzavíraných s dodavateli za účelem vytvoření právně závazného rámce, jenž posílí právní jistotu obou smluvních stran a zároveň omezí riziko úniku nebo zneužití důvěrných informací souvisejících s poskytováním regulované služby. Zajištění důvěrnosti je klíčové zejména v kontextu ochrany informací o bezpečnostních opatřeních, technických řešeních, provozních datech nebo strategických procesech, jejichž zveřejnění by mohlo mít negativní dopad na plynulý a bezpečný chod regulované služby.

Ustanovení, které je vhodné zahrnout do obsahu smlouvy s dodavatelem, je také ustanovení o povinnosti dodavatele dodržovat bezpečnostní politiky povinné osoby nebo ustanovení o odsouhlasení bezpečnostních politik dodavatele (nebo odsouhlasení částí bezpečnostních politik relevantních pro dodavatelský vztah) povinnou osobou. V případě, že se dodavatel podílí na ochraně dat nebo správě systémů souvisejících s regulovanou službou, je vhodné vnímat rizika s tímto spojená. Pokud se dodavatel smluvně nezaváže dodržovat pro předmět dodávky relevantní bezpečnostní politiky 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.

Další část tohoto ustanovení se věnuje povinnosti dodavatele informovat poskytovatele regulované služby o kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy. Tato informace je pro odběratele z hlediska zajišťování kybernetické bezpečnosti důležitá. U takto ošetřených smluv se zamezí případům, kdy dodavatel zatají kybernetické bezpečnostní incidenty svému odběrateli.

Ustanovení o řízení kontinuity činností v souvislosti s dodavateli je zmíněno v této příloze proto, aby i ve smlouvách bylo jasně uvedeno, jak bude dodavatel zapojený a jaké na něj budou kladeny požadavky, v případě nutnosti aktivovat postupy obnovy.

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

Dalším ustanovením, které je vhodné zohlednit v souvislosti s řízením dodavatelů, je dodržování pravidel bezpečného vývoje. Toto ustanovení má za cíl minimalizovat 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 nastavená pravidla ve vývoji minimalizují rizika a zabraňují vzniku zranitelností, snižují náklady na dodatečné bezpečnostní opravy, chrání důvěrnost, integritu a dostupnost poskytované služby, zajišťují odpovědnost dodavatele a jeho závazky k bezpečnosti softwaru.

K příloze č. 3 (Témata pro rozvoj bezpečnostního povědomí)

Na tuto přílohu nově odkazuje § 5 této vyhlášky. Cílem této přílohy je snaha úřadu předat nejlepší praxi získanou vzdělávací činností vytvořením výčtu nejzásadnějších tematických oblastí, které je dobré zohlednit v pravidlech rozvoje bezpečnostního povědomí. 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.