PORTÁL NÚKIB

Manuál pro poskytovatele regulovaných služeb v režimu nižších povinností

TLP:CLEAR

2. června 2026

Verze 1.1

Národní úřad pro kybernetickou a informační bezpečnost

Obsah

1 Co se dozvím v tomto dokumentu?

Předmětem tohoto podpůrného materiálu je popis povinností s příklady jejich aplikace v oblasti kybernetické bezpečnosti vyplývajících ze zákona č. 264/2025 Sb., o kybernetické bezpečnosti (dále jen „zákon“), a především z jeho prováděcí **vyhlášky č. 410/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností** (dále jen „VBO-N“).

Pokud máte jakékoliv další otázky, podívejte se na www.portal.nukib.gov.cz nebo nám napište na regulace@nukib.gov.cz.

Tento dokument slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů. Právo změny tohoto dokumentu vyhrazeno.

Informace obsažené v dokumentu se vztahují k právní úpravě účinné ke dni platnosti publikované verze dokumentu.

1.1 Jak pracovat s podpůrným materiálem

Informace uvedené v přílohách a v příkladech níže jsou pouze jedním z mnoha možných řešení. Například bezpečnostní opatření *systém zajištění minimální kybernetické bezpečnosti* nebo *řízení přístupu* mohou být implementována v jednotlivých organizacích individuálně a jiným způsobem, než jak je uvedeno v tomto podpůrném materiálu.

Tento materiál také úzce souvisí s materiálem Přiměřenost při zavádění bezpečnostních opatření v režimu nižších povinností.

Pro zvýšení přehlednosti dokumentu jsou využívány následující symboly:

	**Upozornění** Důležitá informace, na kterou je třeba upozornit, protože má zásadní význam.
	**Informace** Doplňující vysvětlení nebo podrobnosti, které pomohou lépe porozumět tématu.
	**Poznámka** Doplňující informace, které mohou být užitečné, ale nejsou nezbytné pro hlavní obsah dokumentu.

2 Bezpečnostní opatření

Bezpečnostní opatření stanovená VBO-N mají být zaváděna v rámci **stanoveného rozsahu řízení kybernetické bezpečnosti** (dle § 12 zákona).

Jak stanovit rozsah řízení kybernetické bezpečnosti a co ho definuje?

Rozsah řízení kybernetické bezpečnosti definuje oblasti, kde je potřeba řešit zavádění bezpečnostních opatření. Podrobně je tato problematika popsána v materiálu Stanovení rozsahu řízení kybernetické bezpečnosti.

Bezpečnostní opatření by měla být v souladu s požadavky zákona **zaváděna v nezbytné míře** a v souladu s VBO-N **přiměřená bezpečnostním potřebám** konkrétní organizace. To znamená, že u všech bezpečnostních opatření lze rozhodnout o míře jejich zavedení.

Další informace k aplikaci přiměřenosti při zavádění bezpečnostních opatření najdete v materiálu Přiměřenost při zavádění bezpečnostních opatření v režimu nižších povinností na Portálu Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „Úřad").

*Dle § 13 zákona je poskytovatel regulované služby v režimu nižších povinností (dále jen „poskytovatel regulované služby") povinen bezpečnostní opatření stanovená VBO-N zavést **do jednoho roku ode dne doručení rozhodnutí o registraci regulované služby**.*

Bezpečnostní opatření, která je poskytovatel regulované služby povinen v souladu se zákonem zavést, se dělí na bezpečnostní opatření organizační a technická. Jsou jimi:

- systém zajišťování minimální kybernetické bezpečnosti,
- požadavky na vrcholné vedení,
- řízení aktiv,
- řízení rizik,
- bezpečnost lidských zdrojů,
- řízení kontinuity činností,
- řízení přístupu,
- řízení identit a jejich oprávnění,
- detekce a zaznamenávání kybernetických bezpečnostních událostí,
- řešení kybernetických bezpečnostních incidentů,
- bezpečnost komunikačních sítí,
- aplikační bezpečnost a
- kryptografické algoritmy.

Hlavním účelem a výstupem procesu řízení rizik, který je zachován i v režimu nižších povinností, je určení přiměřených bezpečnostních opatření, která mají být zavedena. V režimu nižších povinností pro tento účel slouží tzv. **přehled bezpečnostních opatření dle § 3 odst. 2 VBO-N.**

2.1 Neopominutelná vs. vyhodnotitelná bezpečnostní opatření

Zákon je postaven na tzv. performativních pravidlech, která dávají poskytovatelům regulované služby prostor pro individuální posouzení a přizpůsobení bezpečnostních opatření podle jejich konkrétního provozního, technického a organizačního kontextu.

To znamená, že všechna stanovená bezpečnostní opatření jsou povinná, ale u tzv**. vyhodnotitelných bezpečnostních opatření** poskytovatel regulované služby vyhodnotí, zda jsou pro něj relevantní. Pokud poskytovatel regulované služby nazná, že pro něj některé z vyhodnotitelných bezpečnostních opatření relevantní není, nemusí jej zavádět. Jeho nezavedení však musí být poskytovatelem regulované služby odůvodněno. Veškerá odůvodnění nezavedení či omezení konkrétního vyhodnotitelného bezpečnostního opatření pak musí být uvedena v **přehledu bezpečnostních opatření** (viz kapitola Systém zajišťování minimální kybernetické bezpečnosti).

Bezpečnostní opatření v rámečku se řadí do tzv. **neopominutelných bezpečnostních opatření**, která jsou **nepodkročitelným minimem**. To znamená, že tato bezpečnostní opatření je nutné zavést vždy. Míru jejich zavedení však již lze přizpůsobit provoznímu, technickému a organizačnímu kontextu konkrétního poskytovatele regulované služby.

§ 3 Systém zajišťování minimální kybernetické bezpečnosti

Zajištění minimální úrovně kybernetické bezpečnosti zavedením základních bezpečnostních opatření, která zohledňují bezpečnostní potřeby poskytovatele regulované služby.

§ 4 Požadavky na vrcholné vedení

Aktivní zapojení vrcholného vedení a jeho podpora k zajištění kybernetické bezpečnosti v organizaci.

§ 5 Bezpečnost lidských zdrojů

Rozvoj bezpečnostního povědomí pro uživatele, vrcholné vedení a administrátory a jejich rozvoj v oblasti kybernetické bezpečnosti.

§ 6 Řízení kontinuity činností

Stanovení postupů a odpovědností souvisejících s řízením kontinuity činností, které je nezbytné pro zajištění rychlé, efektivní a účinné reakce na nepříznivé či mimořádné situace.

§ 10 Řešení kybernetických bezpečnostních incidentů

Nastavení procesu řešení kybernetických bezpečnostních incidentů, včetně těch s významným dopadem.

Zbývající bezpečnostní opatření dle VBO-N, která nejsou zahrnuta ve výše uvedeném výčtu, představují již zmiňovanou skupinu tzv. vyhodnotitelných bezpečnostních opatření.

S nepominutelnými, stejně jako vyhodnotitelnými bezpečnostními opatřeními se blíže seznámíme v následujících dvou kapitolách.

3 Neopominutelná bezpečnostní opatření

Bezpečnostní opatření, která jsou uvedena v této kapitole, **je nezbytné** u regulované služby **přiměřeným způsobem zavést vždy**.

Tato bezpečnostní opatření mají převážně organizační charakter. Jejich implementací by měl poskytovatel regulované služby zajistit nastavení základních procesů v oblasti kybernetické bezpečnosti a vypracování potřebné bezpečnostní dokumentace.

3.1 Systém zajišťování minimální kybernetické bezpečnosti

Ustanovení VBO-N: § 3 odst. 2 až 6 VBO-N, příloha č. 1 a 2 VBO-N

Cíl bezpečnostního opatření: Zajištění minimální úrovně kybernetické bezpečnosti zavedením základních bezpečnostních opatření, která zohledňují bezpečnostní potřeby poskytovatele regulované služby.

Přehled bezpečnostních opatření

Poskytovatel regulované služby je povinen vést **přehled bezpečnostních opatření**, který slouží jako přehled stavu zavedení všech bezpečnostních opatření uvedených ve VBO-N. Přehled bezpečnostních opatření má konkrétně obsahovat:

- přehled všech **zavedených** bezpečnostních opatření, včetně popisu jejich zavedení;
- přehled všech bezpečnostních opatření, která **budou zavedena, a to včetně:**
  - termínu jejich zavedení,
  - priority jejich zavedení, a
  - určení osoby odpovědné za jejich zavedení;
- přehled všech **nezavedených** bezpečnostních opatření, včetně odůvodnění jejich nezavedení.

Jak správně vést tento přehled? Hlavními body jsou:

- listinná nebo elektronická podoba,
- pravidelná **aktualizace a přezkum** daného přehledu alespoň **jednou za rok** a
- **uchování** jednotlivých verzí přehledů alespoň **po dobu 4 let**.

Příklad vedení přehledu bezpečnostních opatření lze nalézt v příloze tohoto dokumentu.

Příklady plnění:

- Organizace má vytvořený přehled bezpečnostních opatření v excelové tabulce, za který nese odpovědnost osoba pověřená kybernetickou bezpečností.
- Tento přehled je pravidelně jednou ročně aktualizován.
- Vrcholné vedení je s tímto přehledem vždy na začátku nového roku seznámeno.

Bezpečnostní politika a bezpečnostní dokumentace

Dalším požadavkem je vytvoření bezpečnostní politiky a bezpečnostní dokumentace, které by měly pokrývat všechna relevantní bezpečnostní opatření, tedy ta, která jsou nebo budou zaváděna. Důležité je, aby byly bezpečnostní politika a bezpečnostní dokumentace platné a účinné a aby docházelo k **vynucování dodržování stanovených povinností a pravidel**.

Bezpečnostní politika a bezpečnostní dokumentace musí být **pravidelně aktualizovány**. Interval pravidelné aktualizace není stanoven, ale v souladu s dobrou praxí by k přezkoumání a případné aktualizaci mělo dojít jednou za rok a v případě prováděných změn, které mají vliv na informace uvedené v dokumentech, klidně dle potřeby i dříve.

Z pohledu VBO-N není podstatné pojmenování dokumentů, případně v kolika dokumentech jsou jednotlivé oblasti řešeny. Důležitá je obsahová **úplnost, čitelnost, snadná identifikovatelnost, vyhledatelnost** (samotných dokumentů i informací v nich obsažených) a uspořádání s ohledem na organizační prostředí a zavedené zvyklosti v oblasti řízení dokumentů poskytovatele regulované služby.

Příklady plnění:

- Organizace vytvořila jednu hlavní bezpečnostní politiku, která obsahuje základní oblasti kybernetické bezpečnosti a k tomu je vytvářena postupně potřebná bezpečnostní dokumentace.
- Všechny dokumenty jsou pravidelně aktualizovány v pravidelném intervalu jednou ročně.
- Jakoukoliv změnu v bezpečnostní politice a bezpečnostní dokumentaci schvaluje vrcholného vedení.
- V případě změny v bezpečnostní politice a bezpečnostní dokumentaci jsou relevantní zaměstnanci o této změně informováni.

Bližší informace k vedení bezpečnostní politiky a bezpečnostní dokumentace lze nalézt v podpůrném materiálu Řízení bezpečnostní politiky a dokumentace: režim nižších povinností.

Pravidla pro používání a manipulaci technických aktiv

Pro technická aktiva ve stanoveném rozsahu řízení kybernetické bezpečnosti je nutné stanovit pravidla pro jejich používání a manipulaci s nimi.

Oblasti, ve kterých je vhodné stanovit pravidla a postupy, jsou například:

- používání technických aktiv (například koncových stanic zaměstnanců, technických postupů administrátorů, SW prostředků v organizaci),
- manipulace s aktivy – v elektronické i fyzické podobě (například zařízení zaměstnanců) a
- likvidace aktiv – nastavení pravidel pro likvidaci technických aktiv (blíže viz Příloha č. 2 – Likvidace informací a dat).

Co si představit pod pojmem technické aktivum?

Podle zákonné definice se jedná o prostředky a vybavení technického či programového charakteru, které podporují provoz regulované služby, jako jsou například servery, koncové stanice a firewall.

Příklady plnění:

- Při předávání pracovní koncové stanice (například počítač) či mobilních zařízení (například laptop, mobil či tablet) jsou zaměstnanci seznámeni s tím, že tato technická aktiva je možné využívat pouze k pracovním účelům. Nemají na nich být například instalovány vlastní aplikace či stahovány filmy apod. Současně jsou zaměstnanci poučení o tom, jak s těmito technickými aktivy pracovat, jaké externí zařízení k nim mohou připojovat, zdali je mohou odnášet z pracoviště apod.
- Zaměstnanci jsou poučeni o tom, jak zacházet s citlivými dokumenty a jak využívat šifrování pro jejich bezpečný přenos, pokud je potřeba je sdílet. Organizace pro klasifikaci citlivých dokumentů používá tzv. Traffic Light Protokol (neboli „TLP“), jehož používání je doporučováno Úřadem. Zavedení tohoto systému označování aktiv zajišťuje v organizaci jednotná a srozumitelná pravidla pro sdílení citlivých informací jak interně, tak směrem k externím subjektům.

Smlouvy s dodavateli

Na úrovni smluvních ujednání je důležité myslet i na kybernetickou bezpečnost. Ve smlouvách by proto měly být zohledněny **relevantní** minimální požadavky uvedené v příloze č. 2 VBO-N. Ne každá smlouva musí vždy obsahovat všechny požadavky uvedené v příloze č. 2 VBO-N.

V závislosti na specifikách regulované služby je vhodné doplnit také další specifická ustanovení, vyplývající z individuálního posouzení rizik a potřeb regulované služby.

Tyto požadavky se nevztahují pouze na nově uzavírané smlouvy. Je nezbytné podívat se i na ty stávající a pokud je to možné, pokusit se (například dodatkem) zajistit, aby obsahovaly relevantní požadavky z uvedené přílohy VBO-N.

Pokud se například smlouva týká pouze dodávek hardwaru nebude ve všech smlouvách relevantní řešit softwarové licence. To samé lze aplikovat pro ujednání o úrovni poskytovaných služeb (SLA), které nebude třeba zahrnovat do uzavíraných smluv, pokud to není pro danou dodávku relevantní.

Příklady plnění:

- Smlouvy s jednotlivými dodavateli jsou postupně kontrolovány a následně dojde k jednání s dodavateli o možnostech doplnění jednotlivých požadavků dle přílohy č. 2 VBO-N do smluv.
- V případě uzavírání nových smluv budou již požadavky na kybernetickou bezpečnost (příloha č. 2 VBO-N) implementovány do smluv.

Akvizice, vývoj a údržba

Při akvizici, vývoji a údržbě technických aktiv spadajících do stanoveného rozsahu řízení kybernetické bezpečnosti je třeba, aby došlo ke stanovení požadavků na zajištění kybernetické bezpečnosti (tedy například při nákupu hardwaru či softwaru). Účelem je, aby v organizaci nedocházelo k pořizování či vývoji technických aktiv, které neumožňují plnit požadavky VBO-N. Obdobně je u údržby třeba dbát na pravidelné aktualizace či rozsah oprávnění a přístupů dodavatelů.

Příklady plnění:

- Organizace stanovila bezpečnostní požadavky v oblasti kybernetické bezpečnosti v souvislosti s plánovanou akvizicí, vývojem a údržbou.
- Bezpečnostní požadavky jsou v souladu s VBO-N. Zároveň budou tyto bezpečnostní požadavky zaváděny i do smluv s dodavateli, tak aby bylo zajištěno jejich dodržování a případné vymáhání.
- Bezpečnostními požadavky, které mohou být zohledněny jsou například:
  - vícefaktorová autentizace,
  - bezpečné komunikační protokoly a aktuální kryptografické algoritmy,
  - řízení vzdáleného přístupu dodavatelů,
  - zajištění bezpečnostních aktualizací u technických aktiv apod.

3.2 Požadavky na vrcholné vedení

Ustanovení VBO-N: § 4 VBO-N

Cíl bezpečnostního opatření: Zapojení vrcholného vedení do řízení kybernetické bezpečnosti.

Kybernetickou bezpečnost je nezbytné budovat od nejvyšší úrovně – vrcholného vedení. To je odpovědné za strategické řízení organizace, a jeho role je tedy klíčová pro vytvoření bezpečného a odolného prostředí. Je nutné, aby vrcholné vedení kybernetickou bezpečnost dané organizace podporovalo a aktivně ji prosazovalo. Vrcholné vedení totiž:

- ovlivňuje celkovou kulturu bezpečnosti v organizaci,
- pomáhá při budování důvěry u zaměstnanců, partnerů i zákazníků,
- ukazuje, že kybernetická bezpečnost je prioritou, a ne pouze administrativní povinností,
- poskytuje potřebné zdroje na zajištění kybernetické bezpečnosti organizace a
- svojí angažovaností zvyšuje šanci organizace na úspěšné zvládnutí bezpečnostních výzev.

VBO-N přitom specifikuje několik základních požadavků, které musí vrcholné vedení plnit:

Určení osoby pověřené kybernetickou bezpečností

Vrcholné vedení určí osobu, které svěří pravomoci potřebné k řízení a rozvoji kybernetické bezpečnosti, dohledu nad jejím stavem a pravidelnou komunikací s vrcholným vedením organizace.

Osoba pověřená kybernetickou bezpečností musí splňovat určité kvalifikační předpoklady. Zejména musí mít odpovídající odborné znalosti v oblasti kybernetické bezpečnosti, což lze doložit například:

- absolvováním odborného teoretického i praktického školení v souladu s její pracovní náplní, a to bez zbytečného odkladu, nebo
- jiným způsobem prokázanou odbornou způsobilostí (například certifikace, doložitelná odbornost, praxe).

Zákon ani VBO-N žádné konkrétnější kvalifikační požadavky neobsahují.

Mezi povinnosti pověřené osoby patří mimo jiné i pravidelná komunikace s vrcholným vedením, kterému podává relevantní informace o stavu a potřebách kybernetické bezpečnosti v dané organizaci. Je naopak již povinností vrcholného vedení udělit osobě pověřené kybernetickou bezpečností potřebné pravomoci, které jí umožní efektivně řídit bezpečnostní procesy v organizaci.

Na osobu pověřenou výkonem této role nejsou kladeny takové nároky jako na manažera kybernetické bezpečnosti dle vyhlášky č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností. To znamená, že pověřená osoba nemusí mít předchozí znalosti a zkušenosti se zajišťováním kybernetické bezpečnosti, ale je to samozřejmě výhodou

Příklady plnění:

- Pověřenou osobou je interní zaměstnanec s dostatečným přehledem o fungování organizace.
  - Například jako osoba pověřená kybernetickou bezpečností může být určen jeden ze zaměstnanců IT.
- Pokud organizace vhodným zaměstnancem nedisponuje, je možné tuto roli řešit i dodavatelsky (doporučujeme zvážit, zda dodavatelské řešení bude opravdu přínosné)
- Klíčové je, aby tato osoba měla dostatečnou podporu vrcholného vedení a mohla aktivně ovlivňovat bezpečnostní strategii organizace.
- Požadavek na určení osoby pověřené kybernetickou bezpečností může být ukotven například v bezpečnostní politice, kde jsou stanoveny také práva a povinnosti této osoby.

Absolvování školení

Každý člen vrcholného vedení absolvuje vstupní a následná i pravidelná školení v oblasti kybernetické bezpečnosti, a to s důrazem na:

- odpovědnosti a povinnosti vrcholného vedení,
- hlavní rizika spojená s kybernetickými hrozbami a
- strategické kroky, které mohou být podniknuty k omezení bezpečnostních hrozeb.

Školení zaměřující se primárně na kybernetickou bezpečnost je nezbytné pro to, aby vrcholné vedení mohlo informovaně rozhodovat mimo jiné o investicích do bezpečnostních opatření a zároveň rozumělo důsledkům neplnění povinností vyplývajících ze zákona a VBO-N. Je možné například využít bezplatné školení kybernetické bezpečnosti dostupné na: https://osveta.nukib.gov.cz/.

Příklady plnění:

- Členové vrcholného vedení pravidelně absolvují školení zaměřené na kybernetickou bezpečnost, která jsou přizpůsobená jejich roli.
- Školení zahrnují témata jako role vrcholného vedení, hlavní rizika spojená s kybernetickými hrozbami a strategické kroky pro jejich omezení.
- Dále kromě základních témat řeší také aktuální hrozby a trendy v kybernetické bezpečnosti.
- Dochází k využití kurzů:
  - organizovaných Úřadem, které jsou zdarma, nebo
  - školení od specializovaných společností.

Zajištění zdrojů

Vrcholné vedení by mělo zajistit zdroje (finanční, personální a technické) nezbytné k dosažení požadované úrovně kybernetické bezpečnosti v souladu s přehledem bezpečnostních opatření.

Může se jednat například o:

- financování nutných bezpečnostních technologií (firewally, antiviry, systémy pro detekci narušení),
- nastavení a přizpůsobení procesů organizace s ohledem na kybernetickou bezpečnost a
- zavedení pravidelného školení pro zaměstnance.

Bez zajištění dostatečných zdrojů nemohou být požadovaná bezpečnostní opatření účinně implementována. Vynaložení daných zdrojů by mělo být vždy řádně odůvodněno a také by mělo být přiměřené k hodnotě aktiva (blíže viz materiál Přiměřenost při zavádění bezpečnostních opatření v režimu nižších povinností).

Příklady plnění:

Vrcholné vedení:

- zajišťuje dostatečné finanční, personální a technické zdroje potřebné k dosažení požadované úrovně kybernetické bezpečnosti,
- alokuje rozpočty na nákup bezpečnostních technologií jako jsou firewally, systémy pro detekci narušení nebo antivirové programy,
- zajišťuje financování školení zaměstnanců,
- podporuje najímání odborníků, kteří se věnují zabezpečení kritických systémů,
- umožňuje investice nejen do moderních technologií, ale také do testování bezpečnostních opatření.

Pravidelné sledování stavu zavádění bezpečnostních opatření

Vrcholné vedení má povinnost pravidelně se seznamovat se stavem kybernetické bezpečnosti organizace. To zahrnuje:

- seznamování se se stavem zavádění bezpečnostních opatření a
- seznamování se s nedostatky v oblasti zavádění bezpečnostních opatření.

Tento přehled umožňuje vrcholnému vedení lépe pochopit situaci a učinit strategická rozhodnutí, například při rozdělování zdrojů.

Klíčovým dokumentem je v tomto směru „Přehled bezpečnostních opatření“ (viz kapitola Systém zajišťování minimální kybernetické bezpečnosti).

Příklady plnění:

Vrcholné vedení:

- aktivně se zajímá o stav kybernetické bezpečnosti a má přehled o všech zavedených bezpečnostních opatření, včetně jejich aktuálního stavu a účinnosti,
- identifikuje nedostatky a oblasti vyžadující zlepšení,
- tento proces zahrnuje do pravidelné porady vrcholného vedení s osobou odpovědnou za kybernetickou bezpečnost a seznamuje se s dokumenty, jako je „Přehled bezpečnostních opatření“,
- každý měsíc dostává reporty a v případě potřeby se účastní porad s bezpečnostním týmem.

Podpora neustálého zlepšování zajišťování kybernetické bezpečnosti

Kybernetické hrozby se neustále vyvíjejí, a proto je důležité, aby vrcholné vedení aktivně podporovalo neustálé zlepšování systému kybernetické bezpečnosti. To zahrnuje především:

- podporu osoby pověřené kybernetickou bezpečností, například poskytováním dostatečných pravomocí a podpory při prosazování změn a
- motivování zaměstnanců k dodržování pravidel kybernetické bezpečnosti.

Příklady plnění:

Vrcholné vedení:

- aktivně podporuje zlepšování systému kybernetické bezpečnosti tím, že zajišťuje dostatek pravomocí pro osobu odpovědnou za kybernetickou bezpečnost,
- motivuje zaměstnance k dodržování pravidel a zajišťuje implementaci nových bezpečnostních opatření, jako je vícefaktorová autentizace nebo segmentace sítě.
- zaměřuje se na budování kultury kybernetické bezpečnosti v organizaci,
- podporuje testování nových přístupů a technologií (například AI pro detekci hrozeb).

Stanovení priorit obnovy

V případě kybernetického bezpečnostního incidentu je klíčové mít jasně stanoveny priority obnovy. Vrcholné vedení určuje, která primární aktiva (služby a informace) musí být obnovena přednostně, aby organizace mohla co nejdříve obnovit své klíčové služby.

Jako priority obnovy v případě kybernetického bezpečnostního incidentu tak mohou být stanoveny například:

- zajištění funkčnosti systémů pro zákazníky a
- obnovení kritických interních systémů (například účetní a personální systémy).

Příklady plnění:

Vrcholné vedení

- definuje jasné priority pro obnovu informací a služeb v případě kybernetického bezpečnostního incidentu,
- stanovuje, že nejdříve budou obnoveny systémy kritické pro zákaznické služby, následně interní systémy, jako jsou účetní a personální databáze (dle kontextu organizace),
- ověřuje, že plány obnovy jsou pravidelně aktualizovány a v ideálním případě otestovány například formou cvičení.

3.3 Bezpečnost lidských zdrojů

Ustanovení VBO-N: § 5 VBO-N, příloha č. 3 VBO-N

Cíl bezpečnostního opatření: Zajištění vzdělávání uživatelů, administrátorů, osoby pověřené kybernetickou bezpečností a vrcholného vedení v oblasti kybernetické bezpečnosti a udržování povědomí o důležitosti dodržování naučených bezpečnostních postupů a pravidel v této oblasti.

Jednou z nejčastějších příčin kybernetických bezpečnostních incidentů je **nedostatečné bezpečnostní povědomí uživatelů** informačních a komunikačních technologií. Zvýšenou pozornost je proto třeba věnovat nejen poučení a průběžnému vzdělávání běžných uživatelů, ale také cílené osvětě administrátorů, osoby pověřené kybernetickou bezpečností a vrcholného vedení, a to v rámci komplexního přístupu k bezpečnosti lidských zdrojů.

Politika bezpečného chování uživatelů

Poskytovatel regulované služby má dokumentovanou formou stanovit požadavky na bezpečné chování uživatelů a tyto požadavky vymáhat. V příloze č. 3 VBO-N je uveden seznam témat, která má poskytovatel regulované služby zohlednit. Pro něj relevantní témata je poskytovatel regulované služby povinen dále rozpracovat v politice bezpečného chování uživatelů, a to dle svých konkrétních bezpečnostních potřeb.

Pravidla rozvoje bezpečnostního povědomí

V souladu se stanovenou politikou bezpečného chování uživatelů je nutné stanovit pravidla rozvoje bezpečnostního povědomí pro vrcholné vedení, uživatele, administrátory a osobu pověřenou kybernetickou bezpečností, a to včetně pravidel pro tvorbu hesel, reflektující požadavky § 8 VBO-N.

Pravidla rozvoje bezpečnostního povědomí je nutné přizpůsobit prostředí organizace. Součástí těchto pravidel má být stanovení požadavků na vstupní a pravidelná školení v oblasti kybernetické bezpečnosti. Rozsah a frekvence účasti na školeních musí odpovídat potřebám jednotlivých skupin osob.

Příklady plnění:

Stanovení pravidel rozvoje bezpečnostního povědomí

- Organizace má zpracovánu politiku bezpečného chování uživatelů.
- Byla zhodnocena všechna témata přílohy č. 3 VBO-N a vybrány a rozpracovány relevantní oblasti pro organizaci.
- Má stanovena pravidla pro rozvoj bezpečnostního povědomí přizpůsobená pro jednotlivé role – vrcholné vedení, uživatelé, administrátoři a osoba pověřená kybernetickou bezpečností.
- Dále jsou stanovena pravidla pro tvorbu hesel.

Vstupní a pravidelná školení

- Každý nový zaměstnanec absolvuje vstupní školení v oblasti kybernetické bezpečnosti.
- Jednou za rok probíhají prezenční průběžná školení kybernetické bezpečnost uzpůsobena na míru organizaci.
- Administrátoři a osoba pověřená kybernetickou bezpečností mají vlastní rozpočet na školení a několikrát ročně absolvují odborná školení v oblasti kybernetické bezpečnosti, jež mají teoretickou i praktickou náplň.

Způsobů, jak zajistit vstupní a průběžná školení v organizaci, je více. Je možné tato školení zajistit například interními zdroji či absolvovat školení, jež bezplatně nabízí Úřad v rámci šíření osvěty o kybernetické bezpečnosti. Viz https://osveta.nukib.gov.cz/.

Kontrola dodržování stanovených pravidel

V souvislosti se stanovenými bezpečnostními politikami a bezpečnostní dokumentací je potřeba zajistit kontrolu jejich dodržování ze strany uživatelů, administrátorů a osoby pověřené kybernetickou bezpečností. Stejně tak je nutné stanovit pravidla a postupy pro řešení případů porušení bezpečnostní politiky a bezpečnostní dokumentace.

Příklady plnění:

Dodržování stanovených pravidel

- Kontrola dodržování bezpečnostní politiky a bezpečnostní dokumentace je jednou z povinností vedoucích zaměstnanců a probíhá v předem neoznámeném termínu jednou do roka.
- Je důsledně vyžadováno dodržování bezpečnostní politiky a bezpečnostní dokumentace.
- Jsou stanovena pravidla a postupy pro řešení případů porušení bezpečnostní politiky a bezpečnostní dokumentace.

Vedení přehledů o školení

- Jsou vedeny přehledy o školeních a seznamy osob, které tyto školení absolvovaly.

3.4 Řízení kontinuity

Ustanovení VBO-N: § 6 VBO-N

Cíl bezpečnostního opatření: Schopnost poskytovatele regulované služby rychle a účinně reagovat na mimořádnou situaci (úmyslnou i neúmyslnou, přírodní událost apod.), která může regulovanou službu nepříznivým způsobem ovlivnit a narušit její provoz.

Stanovení priorit obnovy technických aktiv

V návaznosti na stanovenou prioritu obnovy primárních aktiv vrcholným vedením (viz kapitola Požadavky na vrcholné vedení) je dále nutné v rámci Plánu obnovy stanovit:

- která technická aktiva musí být obnovena prioritně,
- v jakém pořadí budou konkrétní technická aktiva obnovována a
- postup obnovy vybraných technických aktiv.

Příklady plnění:

- Vrcholné vedení definuje jasné priority pro obnovu informací a služeb v případě kybernetického bezpečnostního incidentu.
- Stanovuje, že nejdříve budou obnoveny systémy kritické pro zákaznické služby, následně interní systémy, jako jsou například účetní a personální databáze.
- Plány obnovy jsou pravidelně aktualizovány a testovány prostřednictvím simulací.

Stanovení povinností a odpovědností konkrétních osob

V souvislosti se stanovením priorit, pořadí a postupů obnovy musí dojít také ke stanovení odpovědností a povinností osob, které zajistí rychlé a efektivní zvládnutí nastalé mimořádné situace. Podrobnosti ke stanovení odpovědností a povinností v rámci dokumentace naleznete v materiálu *Řízení bezpečnostní politiky a dokumentace: režim nižších povinností*.

Příklady plnění:

- Vedení definuje, kdo je odpovědný za proces obnovy v případě mimořádné události.
- Dále je definováno, kde provádí samotné kroky k obnově technických aktiv.
- Tyto role a jejich povinnosti a odpovědnosti jsou popsány i písemně (formou řízené dokumentace).

Pravidelné zálohování

Součástí tohoto bezpečnostního opatření je také proces zálohování. Poskytovatel regulované služby musí v pravidelných intervalech vytvářet zálohy informací, dat, konfigurací a nastavení technických aktiv, a to zejména v návaznosti na stanovené priority obnovy technických aktiv.

Příklady plnění:

- Jsou prováděny zálohy informací, dat, konfigurací a nastavení technických aktiv nezbytných zejména pro účely obnovy regulované služby.
- Postupně jsou do procesu záloh přidávána další technická aktiva dle priority.

3.5 Řešení kybernetických bezpečnostních incidentů

Ustanovení VBO-N: § 10 VBO-N

Cíl bezpečnostního opatření: Nastavení procesů pro řešení kybernetických bezpečnostních incidentů.

Oznámení kybernetického bezpečnostního incidentu

Nejdůležitějším předpokladem pro řešení kybernetických bezpečnostních incidentů je, aby se o nich poskytovatel regulované služby včas dozvěděl. Je proto třeba zajistit, aby neobvyklé chování technických aktiv a podezření na jakékoliv zranitelnosti byly poskytovateli regulované služby oznamovány všemi relevantními osobami (například uživateli či dodavateli).

Způsob, jakým dojde k oznámení, je na samotném poskytovateli regulované služby. Příkladem může být oznámení uživatelem prostřednictvím SMS, e-mailu či prostřednictvím systému technické podpory. Vybraný způsob (případně více možných způsobů) by měl být součástí bezpečnostní politiky a všechny relevantní osoby by s tímto způsobem oznamování měly být seznámeny tak, aby věděly, na koho a jakým způsobem se mají obracet.

Co je kybernetická bezpečnostní událost a co kybernetický bezpečnostní incident?

Kybernetická bezpečnostní událost je událost, která může vyústit v kybernetický bezpečnostní incident.

Kybernetický bezpečnostní incident je narušení bezpečnosti informací v kybernetickém prostoru.

Detailní informace k hlášení kybernetických bezpečnostních incidentů lze nalézt v podpůrném materiálu Hlášení kybernetických bezpečnostních incidentů.

Metodika pro posuzování kybernetických bezpečnostních událostí a incidentů

Dále je třeba vytvořit metodiku pro posuzování kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů, která by měla obsahovat i posuzování významnosti dopadu kybernetických bezpečnostních incidentů v souladu s § 14 VBO-N. Podrobnosti jsou obsaženy v materiálu Významnost incidentu v režimu nižších povinností.

Příklady plnění:

- Uživatelé, administrátoři, osoby pověřené kybernetickou bezpečností a další zaměstnanci mohou nahlašovat neobvyklé chování technických aktiv a podezření na možné zranitelnosti například přes:
  - e-mail,
  - telefonicky,
  - osobně,
  - pomocí service desku nebo
  - ticketovacího nástroje.
- Všichni uživatelé, administrátoři i další zaměstnanci organizace jsou poučení o povinnosti nahlašování neobvyklého chování technických aktiv a podezření na zranitelnosti. Toto poučení je součástí vstupního a pravidelného školení.
- Dodavatelům vzniká povinnost nahlašování kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů na základě smluvního vztahu s poskytovatelem regulované služby.

Detekce a posuzování kybernetických bezpečnostních událostí

Další povinností je zajistit detekci kybernetických bezpečnostních událostí a jejich posuzování v souladu se stanovenou metodikou, neboť kybernetické bezpečnostní události mohou vést ke kybernetickému bezpečnostnímu incidentu. V případě, kdy byl zjištěn kybernetický bezpečnostní incident, je třeba zajistit jeho řešení, tedy provedení kroků směřujících k obnovení poskytování regulované služby.

Příklady plnění:

- Metodiku pro posuzování kybernetických bezpečnostních událostí a incidentů včetně posuzování významnosti dopadu kybernetických bezpečnostních incidentů má organizace stanovenou jako samostatný dokument.
- Organizace má zajištěnu detekci kybernetických bezpečnostních událostí, jejich posouzení a řešení nastalých kybernetických bezpečnostních incidentů.

Hlášení incidentů dle § 15 zákona

U kybernetických bezpečnostních incidentů s významným dopadem (viz materiál Významnost incidentu v režimu nižších povinností) ukládá zákon poskytovateli regulované služby povinnost hlásit jej Úřadu.

Detailní informace k hlášení kybernetických bezpečnostních incidentů lze nalézt v podpůrném materiálu Hlášení kybernetických bezpečnostních incidentů.

Vytvoření závěrečné zprávy v souladu s § 16 zákona

V souladu s požadavkem § 16 zákona musí poskytovatel regulované služby vytvořit závěrečnou zprávu o vyřešení kybernetického bezpečnostního incidentu s významným dopadem. Pokud je přitom známa, musí být v závěrečné zprávě popsána i příčina jeho vzniku. Je současně nutné, aby poskytovatel regulované služby v této souvislosti dodržel postupy a lhůty uvedené v § 16 zákona.

Příklady plnění:

- Hlášení kybernetických bezpečnostních incidentů s významným dopadem přes Portál Úřadu má na starost osoba pověřená kybernetickou bezpečností.
- Organizace má připravenu šablonu pro závěrečnou zprávu včetně popisu příčiny kybernetického bezpečnostního incidentu (pokud je známa), kterou osoba pověřená kybernetickou bezpečností spolu s relevantními osobami vyplní v případě vzniklého kybernetického bezpečnostního incidentu s významným dopadem.

4 Vyhodnotitelná bezpečnostní opatření

Poskytovatel regulované služby u níže uvedených vyhodnotitelných bezpečnostních opatření zváží, v jaké míře (popř. zda vůbec) bude daná bezpečnostní opatření s ohledem na bezpečnostní potřeby jeho organizace zavádět.

4.1 Řízení přístupu

Ustanovení VBO-N: § 7 VBO-N

Cíl bezpečnostního opatření: Zajistit jednoznačnou identifikaci osob a zařízení přistupujících k aktivům a řízení práv a oprávnění s ohledem na vykonávanou činnost s aktivem, včetně řešení fyzické bezpečnosti aktiv.

Přístupová práva a oprávnění

Každému uživateli a administrátorovi přistupujícímu k aktivu musí být přidělena odpovídající přístupová práva, a to s takovým stupněm oprávnění, jaký je nezbytný pro povahu jím vykonávané práce s aktivem. Každý uživatelský a administrátorský účet by měl být:

- jedinečný,
- jednoznačně identifikovatelný (spojitelný s konkrétní osobou) a
- řízený.

Má-li být uživateli přiděleno i administrátorské oprávnění, musí být tento **administrátorský účet od uživatelského účtu oddělen** a využíván výhradně k privilegovaným činnostem.

Příklady plnění:

- Je vypracovaná politika zabývající se problematikou uživatelských účtů, zohledňující specifické potřeby organizačních jednotek a jejich povinnosti.
- Jsou přidělována ta nejnižší možná uživatelská oprávnění, která jsou pro vykonávanou práci zaměstnanců nezbytná.
- Je vedena evidence zaměstnanců a jejich přidělených přístupových oprávnění.
- Administrátoři technických aktiv využívají pro jejich administraci výhradně administrátorské účty vázané k danému technickému aktivu, které jsou v rámci organizace unikátní. Pro práci nevyžadující administrátorská oprávnění využívají běžný uživatelský účet.
- Je prováděna periodická kontrola nastavení přidělených uživatelských práv.
- V případě, že je potřeba zajistit pro uživatele vyšší míru oprávnění (například v souvislosti s využíváním určitého SW), je tato potřeba formálně popsána a práva jsou přidělena pouze na nezbytně nutnou úroveň postačující k pracovním úkonům.
- Jsou důsledně vedeny informace o účtech dodavatelů a správců nakupovaných online služeb.
- U dodavatelů online služeb je periodicky prováděn audit, zda jsou používané administrátorské účty unikátní pro danou osobu a organizaci.
- Speciálně je kontrolována evidence uživatelských účtů přidělovaných pro externí pracovníky a důsledně je kontrolována deaktivace účtu po ukončení pracovně právního vztahu.
- Pokud organizace využívá množství specifických aktiv, kde u některých z nich není možné k řízení uživatelských účtů komplexně přistupovat, tak pro jednotlivá aktiva s odlišným způsobem řízení uživatelských oprávnění, je vedena speciální evidence, obsahující informace a politiky technických účtů.

Řízení účtů technických aktiv

Pokud se používají účty, které nejsou přiřazené konkrétní osobě (například systémové nebo technické účty používané konkrétním technickým aktivem či aplikací), musí se i tyto účty řídit stejnými pravidly správy a kontroly jako běžné uživatelské účty.

Mobilní zařízení

Jsou-li využívána mobilní zařízení či obdobná technická aktiva anebo zařízení, včetně těch, která nejsou přímo spravována poskytovatelem regulované služby, je pro tato zařízení nutné zavést odpovídající bezpečnostní opatření zajišťující jejich bezpečný provoz. Jedná se například o mobilní telefony či notebooky dodavatelů, přes které uživatelé přistupují do interní sítě organizace.

Příklady plnění:

- Organizace všechny zaměstnance vybavila pracovními mobilními telefony, na které pomocí centrálního nástroje dohlíží a jsou v její správě.
- Pro mobilní aktiva je nastavena organizační bezpečnostní politika, která specifikuje, jak s nimi smí a nesmí být zacházeno.
- Zaměstnanci mohou aktiva využívat i pro soukromé účely, ale s jistými restrikcemi jako je znemožnění instalace libovolného SW, je zakázáno „kopírování obsahu schránky“ mezi okolními a firemními aplikacemi, na aktivu je vynucen požadavek na délku hesla pro odemknutí obrazovky.

Pravidelná kontrola přidělených práv a oprávnění

U přidělených práv a oprávnění je nutné pravidelně hodnotit, zda neuplynula doba či legitimní důvody, pro které měla být příslušná práva a oprávnění uživateli přidělena. Pro výše uvedená hodnocení je důležité v rámci organizace zavést procesy vedoucí k pravidelné kontrole přidělených práv a oprávnění.

Příklady plnění:

- Organizace periodicky kontroluje relevantnost přidělených práv.
- Organizace poskytuje nadřízeným zaměstnancům přehledy o přidělených právech podřízených osob, která jsou revidována na základě zpětné vazby.

Deaktivace účtů

Dojde-li ke změně nebo ukončení smluvního vztahu (se zaměstnancem, dodavatelem), je třeba z pohledu správy uživatelských a administrátorských účtů na tento stav adekvátně reagovat a například při rozvázání pracovního poměru v adekvátním časovém horizontu příslušné účty deaktivovat či upravit úroveň jejich oprávnění, aby nemohlo dojít ke zneužití těchto účtů.

Příklady plnění:

- Organizace do politiky řízení přístupu zapracovala požadavek na bezodkladné odstavení uživatelských účtů odcházejících zaměstnanců. Před ukončením pracovního poměru zaměstnance může dojít i k dřívějšímu vypnutí některých služeb, jako například VPN připojení či izolace síťových disků.
- Informační systém personální agendy byl doplněn o technologii zajišťující informování relevantních pracovníků IT oddělení s technickou kontrolou činností, zda byly provedeny kroky dle schválených politik.

Fyzická bezpečnost

Musí být zajištěno zabezpečení přístupu k aktivům a ochrana aktiv před možností jejich odcizení či poškození. Aktiva musí být chráněna takovým způsobem, aby u nich nedošlo k neoprávněným zásahům a zneužití.

Příklady plnění:

- Organizace si vymezila místa na základě hodnoty umístěných aktiv a zohledněním dopadu na celkový chod organizace, do kterých mají přístup jen relevantní zaměstnanci a dodavatelé, jako je například serverovna nebo jiný prostor s důležitými aktivy.
- Areál organizace je střežen kamerovým systémem a technologií EZS, dohled může být zajištěn i v mimopracovní dobu bezpečnostní agenturou.
- Relevantní mobilní aktiva jsou vhodným způsobem opatřena pečetí, zajišťující identifikaci manipulace s aktivem.
- Technická aktiva, u kterých je bezpečnost zajišťována primárně prostřednictvím fyzické bezpečnosti, mají garantovaného správce, který je za ně odpovědný a vhodným způsobem dochází k evidování osob, které k aktivům přistupují.
- Stav zajištění fyzické bezpečnosti je popsán v bezpečnostní dokumentaci. Pro uvedené dokumenty je bezpečnostní politikou stanoveno periodické přezkoumání a povinnost aktualizovat bezpečnostní opatření.

4.2 Řízení identit a jejich oprávnění

Ustanovení VBO-N: § 8 VBO-N

Cíl bezpečnostního opatření: Stanovení minimální úrovně pro správu a ověření identit, kterou by poskytovatel regulované služby měl v organizaci prosazovat.

Nástroj pro řízení identit, přístupových práv a oprávnění

Poskytovatel regulované služby zavede nástroj pro řízení identit, přístupových práv a oprávnění, který musí umožnit:

- **Řízení počtu možných neúspěšných pokusů o přihlášení**. Toto bezpečnostní opatření je podstatné zejména u přístupů z veřejného internetu. Tyto přístupy jsou rizikové z pohledu možnosti jejich zneužití potenciálním útočníkem například při jeho pokusu o průnik do systému nebo zablokování dostupnosti tohoto přístupu.
- **Opětovné ověření identity po stanovené době nečinnosti**. Zavedením tohoto bezpečnostního opatření může poskytovatel regulované služby předejít například kompromitaci koncové stanice v době, kdy u ní uživatel není fyzicky přítomen a omylem ji ponechá odemčenou.

- **Řízení přístupových práv, oprávnění pro čtení a zápis informací a dat a změnu oprávnění**. Zavedení tohoto bezpečnostního opatření musí být v souladu s pracovní náplní jednotlivých zaměstnanců, tak aby byla dodržena zásada need-to-know (tj. každý zaměstnanec má jen taková oprávnění a přístup pouze k těm informacím, které bezprostředně potřebuje pro výkon své práce).
- **Odolnost uložených a přenášených autentizačních údajů**. Při přenášení či ukládání autentizačních údajů je nutné využít aktuální kryptografii (aktuální šifrovací či hašovací funkce), tak aby nedošlo k jejich odposlechu a následnému zneužití.

Autentizační mechanismus

V rámci nastavení správy a ověření identit lze ve VBO-N najít tři úrovně nastavení autentizačního mechanismu. Jedná se o:

- **Vícefaktorovou autentizaci s nejméně dvěma různými typy faktorů** (například heslo a kód z ověřovací aplikace v telefonu).
- **Autentizaci pomocí kryptografických klíčů a certifikátů.** V případě, kdy nelze vyhovět požadavku na zavedení vícefaktorové autentizace s nejméně dvěma různými typy faktorů, je třeba, aby nástroj pro ověřování identit uživatelů, administrátorů a technických aktiv využíval alespoň autentizaci pomocí kryptografických klíčů a certifikátů.
    - Může se jednat například o autentizaci pomocí SSH klíčů.
- **Autentizaci pomocí pouze identifikátorů účtu a hesla.** V případě, kdy poskytovatel regulované služby nemůže zajistit zavedení ani vícefaktorové autentizace s nejméně dvěma různými typy faktorů, ani autentizace pomocí kryptografických klíčů a certifikátů, musí při využívání autentizace pomocí identifikátorů účtu a hesla technicky zajistit vynucení následujících pravidel:
    - **Minimální délka hesla:**
        - 12 znaků pro účty uživatelů,
        - 17 znaků pro účty administrátorů a
        - 22 znaků pro účty technických aktiv.
    - **Skladba hesla:**
        - Umožnění uživateli používat nejenom malá a velká písmena, číslice, ale i speciální znaky.
        - Nesmí být používána jednoduchá a často používaná hesla.
        - Nesmí být tvořena hesla na základě mnohonásobně opakujících se znaků, přihlašovacího jména, e-mailu, názvu systému nebo obdobným způsobem.
        - Nesmí docházet k opětovnému použití dříve použitých hesel s pamětí alespoň 12 předchozích hesel.
    - **Životnost hesla:**
        - Změna hesla musí být prováděna v pravidelných intervalech, nejpozději po 18 měsících.

Co si lze představit pod faktory autentizace kybernetické bezpečnosti?

*Pod typy faktorů si lze představit například informaci, kterou uživatel **zná** (heslo, PIN kód), čím fyzicky **je** (biometrický údaj) nebo předmět, který **vlastní** (autentizační karta, token ve formě USB klíčenky).*

*Lze také využít **kontinuální autentizaci** vycházející z principu tzv. „zero-trust", kdy je identita uživatele ověřována průběžně (například pomocí biometrických či behaviorálních charakteristik). Tento přístup může dále snížit riziko kompromitace systému v případě, že by byl překonán počáteční autentizační mechanismus.*

Důvěrnost

Při vytváření výchozích autentizačních údajů a při obnově přístupu je nutné zajistit jejich důvěrnost a technicky vyžadovat změnu výchozího nebo obnovovacího hesla při jeho prvním použití. Jedná se zejména o:

- zneplatnění hesla nebo identifikátoru pro obnovu přístupu nejpozději do 24 hodin od jeho vytvoření,
- bezodkladnou změnu přístupového hesla v případě důvodného podezření na jeho kompromitaci a
- zabezpečení administrátorských účtů technických aktiv určených zejména pro případ obnovy po kybernetickém bezpečnostním incidentu a jejich využití pouze v nezbytných případech.

Příklady plnění:

- Organizace využívá vícefaktorovou autentizaci, která je nasazena u vybraných autentizačních mechanismů.
- U autentizačních mechanismů na bázi přihlašování pomocí uživatelského jména a hesla je dodržována politika hesel v souladu s požadavky VBO-N.

Vhodná pravidla pro tvorbu hesel:

- *nepovolovat slabá a běžně známá hesla (například „admin" a „123456"),*
- *zakázat hesla založená na opakování znaků nebo odvozená z jmen, e-mailu či názvu systému a*
- *zajistit, aby uživatel nemohl znovu použít alespoň 12 předchozích hesel.*

4.3 Detekce a zaznamenávání kybernetických bezpečnostních událostí

Ustanovení VBO-N: § 9 VBO-N

Cíl bezpečnostního opatření: Nasazení nástrojů, které jsou schopny detekovat kybernetické bezpečnostní události, které mohou vést ke kybernetickým bezpečnostním incidentům, kdy tyto nástroje se schopností detekce mohou pomoci těmto incidentům předcházet.

Ochrana dat na perimetru komunikační sítě

Pro data přenášená přes perimetr komunikační sítě je třeba zajistit jejich ověření a kontrolu. Perimetr zpravidla odděluje interní síť od veřejné sítě, důvěryhodné prostředí od nedůvěryhodného nebo různé bezpečnostní zóny (například interní LAN od segmentu tzv. demilitarizované zóny – DMZ). Bude-li na síťovém perimetru detekována nežádoucí komunikace, mělo by dojít k jejímu zablokování.

Příklady plnění:

- Veškerá perimetrová komunikace probíhá skrze specializovaný HW prvek (hraniční firewall), zajišťující plnění požadavku bezpečnostního opatření.
- Organizace nedisponuje takovým typem sítě (například s HW hraničním firewallem), na který by bylo možné dané opatření aplikovat, tedy zavedla pouze firewally a obdobná bezpečnostní opatření na úrovni SW na jiných technických aktivech.
- Organizace má v rámci smlouvy o poskytování internetového připojení od operátora zajištěn i aspekt kyberbezpečnosti na vstupu do sítě internet.

Ochrana před škodlivým kódem

Pro technická aktiva, zejména koncové stanice a servery, musí být zajištěna nepřetržitá a automatická ochrana před škodlivým kódem pomocí vhodného nástroje.

Příklady plnění:

- Mimo běžná IT technická aktiva, jako běžné počítače a servery, organizace využívá i aktiva průmyslového charakteru, která často bývají dodávána jako tzv. *black-box*, tedy zařízení, u kterých zákazník nezná jeho dílčí části, funkcionality či nastavení. U těchto technických aktiv je omezeno zavádění bezpečnostních opatření, jelikož zákazník nemá informace potřebné pro jejich zavedení přímo na daném aktivu. O těchto aktivech je vedena evidence s posouzením stavu a jsou chráněna dodatečným způsobem jako je omezení síťové komunikace, fyzické zablokování komunikačních portů a řízení fyzického přístupu k těmto aktivům.
- Veškerá aktiva jsou chráněna SW nástrojem pro nepřetržitou automatickou ochranu před škodlivým kódem s centrální správou. V případě výskytu bezpečnostní události je o tomto stavu notifikována zodpovědná bezpečnostní role, která musí událost vyhodnotit a rozhodnout o dalším postupu.

Pravidla pro automatické spouštění obsahu datových médií

Pokud poskytovatel regulované služby využívá výměnná datová média či obdobné přenosné datové nosiče, je v souvislosti s těmito zařízeními nutné řídit automatické spouštění jejich obsahu.

Příklady plnění:

- Je zajištěno skenování obsahu datových nosičů před jeho spuštěním pomocí vybraného nástroje po jejich připojení ke koncové stanici.
- Blokování automatického spouštění datových nosičů je řešeno u všech systémů vynucením bezpečnostní politikou a nastavením na úrovni domény.
- U průmyslových výrobních zařízení jsou volně dostupné USB porty zamčeny mechanickými klíči.

Hlášení z nástrojů detekce kybernetických bezpečnostních událostí

O detekovaných kybernetických bezpečnostních událostech musí být vyrozuměny všechny relevantní osoby (například osoba pověřená kybernetickou bezpečností), a to tak, aby následně mohlo dojít k zahájení procesů spojených s řešením kybernetických bezpečnostních událostí a incidentů.

Aktualizace nástrojů pro detekci kybernetických bezpečnostních událostí

Pro nástroje zajišťující nepřetržitou a automatickou ochranu před škodlivým kódem a další detekční nástroje musí být zajištěna jejich pravidelná a bezodkladná aktualizace včetně kontroly aktuálnosti detekčních pravidel.

Příklady plnění:

- Instalovaný nástroj automatické ochrany před škodlivým kódem disponuje centrální konzolí, zobrazující stav bezpečnostních klientů zapojených koncových stanic. V případě výskytu podezření na bezpečnostní událost konzole automaticky zašle příslušným zaměstnancům notifikaci.
- Veškerou správu bezpečnostních opatření zajišťuje dodavatel, se kterým má organizace nastavené vhodné komunikační kanály a mechanismy pro řešení případných problémů.

Požadavky na zaznamenávané informace pro relevantní události či detekce

V souladu s požadavky na detekci kybernetických bezpečnostních událostí je zapotřebí, aby poskytovatel regulované služby zaznamenával bezpečnostní události a relevantní provozní události.

Záznam těchto událostí je klíčový především z důvodů:

- **včasné identifikace** – bez záznamu události nelze spolehlivě odhalit pokusy o neoprávněný přístup, škodlivý kód nebo jiné anomálie,

- **analýzy a reakce** – zaznamenaná data poskytují podklady pro šetření nebo určení příčiny kybernetického bezpečnostního incidentu a přijetí nápravných opatření a
- **prevence opakování** – historické záznamy pomáhají identifikovat vzorce útoků a zlepšovat preventivní opatření.

Proto je u záznamů nutné, aby byly zajištěny a uchovávány následující údaje:

- datum a čas, včetně specifikace časového pásma,
- typ činnosti,
- jednoznačná identifikace technického aktiva a identifikace účtu původce a
- úspěšnost nebo neúspěšnost činnosti.

Příklady plnění:

- Organizace zavedla interní zdroj jednotného času ve vlastní infrastruktuře, díky čemuž mají všechna zařízení sjednocený čas. Další možností je připojení relevantních technických aktiv k veřejnému internetu a veřejně dostupné servery poskytující jednotný čas.
- Organizace provozuje bezpečnostní řešení zaznamenávající informace, v případě výskytu bezpečnostní události musí být tato událost dále posouzena odpovědným pracovníkem, který provede okomentování události včetně vyhodnocení její úspěšnosti.
- Veškerou správu bezpečnostních opatření zajišťuje dodavatel, se kterým má organizace nastavené vhodné komunikační kanály a mechanismy pro řešení případných problémů.

Doba uchovávání záznamů

Záznamy bezpečnostních a relevantních provozních událostí (v praxi často nazývané jako „logy“) je potřeba uchovávat po dobu, kterou si poskytovatel regulované služby na základě svých bezpečnostních potřeb stanoví.

V případě vzniku kybernetického bezpečnostního incidentu mohou tyto záznamy představovat zásadní důkazy pro forenzní analýzu. Bez dostatečných dat nelze spolehlivě určit příčinu kybernetického bezpečnostního incidentu ani přijmout účinná nápravná opatření.

Mezi relevantní provozní události se mohou řadit například:

- **Výpadek konektivity** – může indikovat útok typu DoS nebo selhání infrastruktury.
- **Abnormální zatížení linky** – může signalizovat pokus o přetížení sítě nebo nelegitimní datové toky.
- **Výrazné vytížení technických aktiv** – může naznačovat provozní anomálii nebo pokus o zneužití technického aktiva.

Příklady plnění:

- Na základě analýzy množství doposud šetřených bezpečnostních událostí organizace stanovila dobu uchovávání relevantních záznamů na 1,5 roku.
- V oblasti fyzické bezpečnosti kvůli velkému množství bezpečnostních kamer s vysokým rozlišením musela organizace zohlednit přiměřenost finančních nákladů na paměťovou kapacitu souvisejících úložišť kamerových záznamů. Organizace vyhodnotila, že bude po 7 dnech docházet k automatickému přepisování pořizovaných záznamů.
- Na základě konzultace s dodavateli jsou z hlavních bezpečnostních nástrojů sbírány pouze bezpečnostní záznamy (například tzv. *security logy*), které se dle kapacity dedikovaného separátního úložiště přepisují. K vyhodnocování relevantních provozních logů sice dochází, avšak nedochází k jejich dlouhodobému ukládání.

4.4 Bezpečnost komunikačních sítí

Ustanovení VBO-N: § 11 VBO-N

Cíl bezpečnostního opatření: Zajištění ochrany komunikačních sítí poskytovatele regulované služby pomocí vhodné síťové segmentace a zajištění ochrany sítě na jejím komunikačním perimetru.

Segmentace komunikační sítě a oddělení provozu

Komunikační síť by měla být segmentována, například dle:

- účelu použití technických aktiv (segment pro tiskárny, koncové stanice, servery či zálohy),
- účelu použití vzhledem k organizačním jednotkám (segment s koncovými stanicemi účtárny, segment s koncovými stanicemi administrátorů),
- specifických požadavků na bezpečnost (segment s přímým přístupem do veřejného internetu DMZ),
- nutnosti komunikovat se specifickými technologiemi (dispečerské stanice průmyslových technologií) či
- jiné vhodné kombinace v souladu s relevantními požadavky organizace.

Segmentace se vztahuje i na jednotlivá provozovaná prostředí (oddělení produkčního prostředí od ostatních prostředí, zálohovací řešení, prostředí aplikačního vývoje, testovací prostředí). Uvedené oddělení může být technicky realizováno jak na fyzické síti, tak i na vyšší logické komunikační vrstvě. Je třeba zajistit i vhodný způsob řízení komunikace (mezi jednotlivými segmenty interní komunikační sítě, řízení komunikace na síťovém perimetru či vůči externím sítím, tedy veřejnému internetu), aby nebylo možné potenciální šíření škodlivého kódu či útočníka mezi segmenty.

Příklady plnění:

- V organizaci je implementovaná pokročilá segmentace, mikrosegmentace, řízení provozu, oddělení záloh.
- Dochází k řízení provozu mezi segmenty.
- Je oddělený segment pro průmyslová zařízení a související aktiva ve výrobě.
- Dochází k základnímu rozdělení interní sítě na segmenty jako je kancelářská síť, servery a zálohy.

Omezení komunikace na perimetru sítě na nezbytně nutnou

Cílem je zajistit, aby síťová komunikace procházející přes bezpečnostní perimetr byla v příchozím i odchozím směru omezena tak, aby byl umožněn průchod pouze pro tu komunikaci, která je nezbytně nutná k zajištění poskytování regulované služby. Pro ostatní typy komunikací, které nejsou pro chod regulované služby nezbytně nutné, by mělo dojít k posouzení jejich potřebnosti – případně je dle stanovených pravidel poskytovatele regulované služby vhodné zvážit i jejich úplné zablokování.

Ačkoli je požadavek pro poskytovatele regulované služby formálně vztažen pouze k perimetru komunikační sítě, Úřad doporučuje aplikovat toto opatření i v celé interní síti. Jde o běžnou praxi v souladu s principy zero-trust, která pomáhá omezit šíření škodlivého kódu nebo útočníka uvnitř prostředí, čímž i zvyšuje úroveň kybernetické bezpečnosti.

Příklady plnění:

- Organizace využívá bezpečnostního řešení pro řízení komunikace mezi technickými aktivy a síťovým perimetrem (například perimetrový firewall, řízení a monitorování segmentu DMZ). U používaných řešení dochází ke kontrole zajištění technické podpory výrobce (aktualizace firewallu/softwaru), periodicky se kontroluje nastavení a konfigurace bezpečnostních pravidel vzhledem k aktuálním potřebám provozovaných aktiv.
- Dochází k řízení komunikace k technickým aktivům exponovaným do veřejného internetu (omezení služeb a portů na veřejných IP adresách).

Používání bezpečných komunikačních protokolů

Poskytovatel regulované služby by měl vědět, jaké druhy síťových protokolů jsou pro komunikaci provozovaných aktiv využívány. Bezpečnostní opatření má zajistit používání pouze takových síťových komunikačních protokolů, které jsou v době jejich používání bezpečné a odolné. Je-li nutné k provozu aktiv využívat i méně odolné komunikační protokoly, je třeba zvážit dodatečné přiměřené zabezpečení pomocí dalších technických prostředků, například zajištěním šifrování na úrovni jiné komunikační vrstvy či zapouzdření do šifrovaného přenosu.

Příklady plnění:

- Organizace má díky analýze síťového provozu na perimetru i v interní komunikační síti povědomí o používaných síťových protokolech.
- Dochází k pravidelnému vyhodnocování používaných síťových protokolů a jejich parametrů (například jejich verzí a použitých kryptografických prostředků).
- Organizace provozuje v sousedním areálu průmyslová zařízení, u kterých zjistila výskyt síťových protokolů komunikujících v otevřené nechráněné podobě. Bylo zavedeno vhodné náhradní technické opatření zapouzdřující uvedené komunikace do síťového tunelu, chráněného kryptografickou šifrou odolnou dle doporučení Úřadu.
- Organizace má základní přehled o tom, že nejsou používány nešifrované a neodolné síťové komunikační protokoly (například HTTP).

Vzdálená připojení

Potřebuje-li poskytovatel regulované služby zřizovat nějaký druh vzdáleného připojení či správy, musí být tyto vzdálené přístupy vhodným způsobem omezeny na takovou úroveň, která umožní jejich využití pouze k nezbytně nutnému účelu.

Požadavky na vzdálené připojení:

- **zajištění důvěrnosti a integrity** všech přenášených dat přes vzdálené připojení,
- vedení **přehledu o uživatelích či administrátorech**, kteří mají oprávnění využívat vzdálené připojení a
- **zvýšená ochrana přístupů z veřejného internetu**, jelikož jsou více ohrožené.

Pozor na termín „vzdálené připojení“

Vzdáleným připojením není myšlen pouze vzdálený VPN přístup, ale jakákoliv forma přístupu, která není lokální. Vzdáleným připojením je tak například i přístup z uživatelského počítače prostřednictvím webového prohlížeče k online informačnímu systému organizace.

Příklady plnění:

- Je vedena evidence zařízení a uživatelů, kteří mají umožněn vzdálený přístup a jakého druhu (například VPN či protokoly Remote Desktop nebo Secure Shell).
- Vzdálené připojování do interní sítě je povolené pouze z řízených koncových stanic (například pod správou MDM), u kterých je kontrolováno splnění bezpečnostních požadavků před připojením (aktuální verze OS, ochrany před škodlivým kódem atd.)
- Vzdálená připojení dodavatelů jsou smluvně ošetřena, řízena a technicky připravena (přidělení certifikátů, identit a MFA), připojení je na straně organizace povoleno pouze po předchozí komunikaci s dodavatelem, kterému není umožněno svévolného přístupu k síti organizace.
- K aktivům organizace je dodavateli umožněn přístup pouze skrze pro tento účel vytvořenou stanici (tzv. „jump server“) organizace, která zajišťuje bezpečnostní monitoring nad prováděnými činnostmi.
- Vzdálené připojování ke správě technických aktiv mimo interní síť je podmíněné vícefaktorovu autentizací.
- Vzdálené připojování do interní sítě není skrze absenci relevantních technických aktiv umožněno.
- Vzdálené připojování a správa technických aktiv pomocí software pro vzdálenou správu nebo pomocí alternativních způsobů je organizačně řízena a zaměstnanci i dodavatelé jsou poučeni o podmínkách použití těchto nástrojů.

4.5 Aplikační bezpečnost

Ustanovení VBO-N: § 12 VBO-N

Cíl bezpečnostního opatření: Zajištění nasazení bezpečnostních opatření a skenování zranitelností technických aktiv v kontextu dlouhodobé udržitelnosti provozovaných technických aktiv.

Bezpečnostní aktualizace

Jsou-li výrobcem, dodavatelem či jinou osobou uvolněny bezpečnostní aktualizace na provozovaná technická aktiva, měly by být tyto bezpečnostní aktualizace aplikovány bez zbytečného odkladu.

Příklady plnění:

- Aktualizace OS koncových stanic.
- Aktualizace uživatelského SW (nástroj pro centrální správu a dohled).
- Aktualizace uživatelského SW (manuální kontrola a nasazování aktualizací).
- Aktualizace řadičů virtualizačních platforem.
- Aktualizace firmwaru síťových prvků.
- Aktualizace OT komponent, které si organizace sama spravuje v oblasti řízení technologií budovy.

Nepodporovaná technická aktiva

Může nastat situace, kdy poskytovatel regulované služby provozuje aktiva, u kterých již není například z důvodu jejich zastaralosti zajištěno vydávání nových bezpečnostních aktualizací. U takových aktiv je nutné:

- důsledné vedení jejich evidence,
- podniknout takové kroky, které pomocí dalších bezpečnostních opatření zajistí bezpečnostní úroveň na stejné či vyšší úrovni jako u aktiv, která mají bezpečnostní podporu výrobce zajištěnou a
- omezení jejich síťové komunikace v rámci provozované komunikační sítě pouze na komunikaci nezbytně nutnou pro zajištění provozu těchto aktiv.

Příklady plnění:

- Organizace vede důkladnou evidenci veškerého používaného SW a HW. Evidence zahrnuje přesnou identifikaci aktiva, informaci o verzi systému či sestavení a dodatečně jsou evidovány aplikované bezpečnostní záplaty či zda má systém zajištěnu bezpečnostní podporu výrobce.
- Některé stroje výrobní linky elektrotechnických zařízení zakoupené jako „*black-box*“ disponují vysoce zastaralými OS; uvedené stroje byly izolovány v rámci síťového perimetru a síťová komunikace je povolena pouze na relevantní stanice technologů, které jsou vybaveny podporovaným systémem a implementují další monitorovací nástroje.
- Organizace vede evidenci používaného SW včetně jeho verzí a umístění (původní motivací byla kontrola nad vypršením platností licencí, jelikož jsou SW aktiva nakupována na omezenou dobu).

Skenování zranitelností

Poskytovatel regulované služby musí u relevantních technických aktiv zajistit pravidelné skenování zranitelností a na základě zjištěných výsledků aplikovat přiměřená bezpečnostní opatření. Na základě těchto výsledků je nutné posoudit přiměřenost zavádění dílčích bezpečnostních opatření (například bezpečnostních aktualizací a záplat) v kontextu relevantních technických aktiv, tak aby byla zajištěna jejich provozní funkčnost i bezpečnost.

Příklady plnění:

- Organizace má komplexní přehled o veškerých provozovaných technických aktivech, je vedena důsledná evidence SW a HW. Nástroj evidence aktiv provádí automatizovanou kontrolu oproti katalogům veřejně známých zranitelností. Pro případ pozitivní detekce zranitelného aktiva je postupováno dle zpracovaného plánu mitigace zranitelností.
- Pro vybranou část infrastruktury je prováděno fyzické bezpečnostní skenování či skenování zranitelností ve spolupráci s dodavatelem, tato činnost je zanesena v podnikové směrnici v návaznosti na zprovozňování nových výrobních celků.
- IT pracovníci organizace zavedli v interní síti skenovací zařízení, které dle schváleného procesu využívají při kontrolách technických aktiv. Obdobná technologie je permanentně provozována i ve virtualizační platformě, kde zajišťuje skenování vybraných síťových segmentů automatizovaně.
- Skenování zranitelností není prováděno, ale na základě pečlivé evidence SW a HW se periodicky dle procesu kontroluje, zda pro dané aktivum nebyla zveřejněna zranitelnost.
- Organizace pro svoji činnost využívá cloudovou platformu, jejíž součástí je bezpečnostní řešení, zajišťující sběr informací z klientů připojených koncových stanic. Automaticky je vyhodnocována dostupnost aktualizací instalovaného SW a je upozorněno na výskyt kritické zranitelnosti.

4.6 Kryptografické algoritmy

Ustanovení VBO-N: § 13 VBO-N

Cíl bezpečnostního opatření: Zajištění správného užívání kryptografických algoritmů a bezpečné komunikace, zejména za účelem zajištění důvěrnosti předávaných dat a informací.

Aktuální a odolná kryptografie

Provozovatel regulované služby by měl pravidelně kontrolovat, zda jím používané kryptografické algoritmy jsou aktuálně odolné a prosazovat bezpečné nakládání s kryptografickými algoritmy.

Vhodným zdrojem informací v této oblasti jsou doporučení vydávaná Úřadem, obzvláště pokud jsou v organizaci využívány kryptografické certifikáty, digitální podpisy či šifrovací algoritmy. Doporučení Úřadu jsou obsažena v materiálu Minimální požadavky na kryptografické algoritmy.

Zajištění bezpečnosti komunikačních kanálů

Požadavek cílí na zabezpečení hlasové, audiovizuální a textové komunikace, a to včetně e-mailové komunikace. Zde je možné se odkázat na využívání komunikačních platforem, které podporují end-to-end šifrování či ochranné opatření na zabezpečení e-mailové komunikace vydané Úřadem. Pro případ nouzových situací je na místě také zajistit i bezpečnost tzv. nouzové komunikace, která bude použita v případě výpadku běžně používaných komunikačních linek, na které ale ovšem lze zpravidla aplikovat obdobná bezpečnostní opatření jako na ty běžné používané (například využívání end-to-end šifrování).

Příklady plnění:

- IT zaměstnanci odpovědní za nastavení technických aktiv jsou si vědomi problematiky kryptografie a náležitě upravují jednotlivé konfigurace a nastavení. Organizace si spravuje vlastní infrastrukturu kryptografických klíčů (PKI).
- Zaměstnanci organizace disponují jednotlivými nástroji, pravidly a postupy pro práci se šifrovacími algoritmy (například pro zasílání citlivých dokumentů) a jejich používání je hlídáno, aby nedocházelo například k nedůvěrnému předávání informací klientům či jiné organizaci.
- Doporučení a metodiky vydávané Úřadem v organizaci slouží k revizi a dílčím úpravám nastavení a konfigurací technických aktiv.
- Pro zabezpečenou hlasovou, audiovizuální a textovou komunikaci využívají zaměstnanci mobilní aplikaci s end-to-end šifrováním dle doporučení Úřadu. Zaměstnanci jsou v průběhu školení poučeni o používání end-to-end šifrování v rámci pracovní komunikace, totéž platí pro nouzovou komunikaci.
- Pro zabezpečenou e-mailovou komunikaci se řídí opatřeními Úřadu v oblasti zabezpečení elektronické pošty.
- V organizaci existuje obecné povědomí o tom, že by nemělo docházet k používání nešifrovaných či zastaralých protokolů (HTTP, telnet atd.) a oblast kryptografie je řešena spíše na povrchové úrovni komunikačních protokolů a názvů používaných algoritmů, nikoliv jejich parametrů.
- Uživatelé jsou v rámci vstupních či pravidelných školení upozorňováni na důležitost používání odolného šifrovaní při důvěrné komunikaci (end-to-end šifrování, šifrování souborů, HTTPS atd.)
- Organizace si je vědoma doporučení a metodik Úřadu v oblasti kryptografie a snaží se je zavádět.

5 Stanovení významnosti dopadu kybernetického bezpečnostního incidentu

Ustanovení VBO-N: § 14 VBO-N a § 15 zákona

Cíl: V souladu s požadavky zákona a VBO-N stanovit, jaké kybernetické bezpečnostní incidenty jsou významného dopadu, a je tedy nutné je hlásit.

Významnost dopadu kybernetického bezpečnostního incidentu

Určení významnosti dopadu kybernetického bezpečnostního incidentu je důležitým krokem pro rozhodnutí, zda je potřeba jej hlásit.

Této problematice se podrobně věnuje materiál Významnost incidentu v režimu nižších povinností.

Povinnost hlásit incident je blíže rozebrána v materiálu Hlášení kybernetických bezpečnostních incidentů.

6 Přílohy

6.1 Příloha č. 1 – Přehled bezpečnostních opatření

Tento dokument obsahuje příklad řešení přehledu bezpečnostních opatření, který je jedním z klíčových dokumentů požadovaných VBO-N. Uvedený přehled bezpečnostních opatření slouží pouze jako inspirace a ukázka možného řešení. **Vždy bude nutné jej přizpůsobit pro případ konkrétní organizace.**

6.2 Příloha č. 2 – Bezpečná likvidace informací a dat

Likvidací se rozumí odstranění, přepsání, nebo fyzická likvidace informací a dat, jejich kopií a technických nosičů tak, aby po vyřazení zařízení nedošlo k neoprávněnému zpřístupnění nebo zneužití dat.

VBO-N ukládá dle § 3 odst. 4 povinnost stanovit v rámci řízení aktiv pravidla pro používání a manipulaci s technickými aktivy. Součástí manipulace s technickými aktivy je i problematika jejich likvidace a likvidace informací a dat na nich uložených.

Pravidla likvidace informací a dat by měla být nastavena přiměřeně důležitosti jednotlivých aktiv. To v praxi znamená volit takové postupy, které odpovídají charakteru informací, dat, typu nosiče, hrozbám i možnostem organizace, aniž by ji neúměrně zatěžovaly. Organizace musí rozumět důležitosti a hodnotě svých informací a dopadům případného zneužití, aby mohla určit, zda postačí běžné odstranění, bezpečné přepsání, nebo je nutná fyzická likvidace nosiče.

Tento princip zavádění a provádění přiměřených bezpečnostních opatření se týká všech bezpečnostních opatření ve VBO-N a je uveden v § 3 odst. 1 VBO-N, dle kterého povinná osoba zavede a provádí bezpečnostní opatření, která jsou přiměřená bezpečnostním potřebám. O tématu přiměřenosti zavádění bezpečnostních opatření více pojednává podpůrný materiál dostupný na odkazu: Přiměřenost při zavádění bezpečnostních opatření v režimu nižších povinností | Portál NÚKIB.

Při posuzování citlivosti sdílených informací a s tím související důvěrnosti informací může organizace zohlednit také pravidla označování informací podle protokolu Traffic Light Protocol (TLP), dle aktuální verze mezinárodního standardu tzv. Traffic Light Protocol (TLP), který je podrobně popsán zde: Národní úřad pro kybernetickou a informační bezpečnost – sdílení informací.

Stanovená pravidla a postupy nejen v oblasti likvidace by měly být následně v praxi důsledně dodržovány a vynucovány, aby bylo předcházeno narušení bezpečnosti informací. Tato pravidla by měla být pravidelně přezkoumávána, aktualizována a promítána do provozních postupů. Organizace by měla zajistit, aby byla pravidla součástí běžného provozu a byla dostupná všem osobám, které se na manipulaci (včetně likvidace aktiv) podílejí.

Organizace by měla stanovit základní pravidla likvidace zejména pro:

- informace v listinné podobě (například tištěné dokumenty, psané poznámky, ruční zápisy),
- nepřepisovatelná datová média (například CD-R, DVD-R, BD-R, jiná jednorázová média),
- přepisovatelná datová média (například HDD, magnetické pásky, SSD, USB Flash disky, CD-RW, DVD-RW, BD-RE, SD/microSD karty),
- mobilní a koncová zařízení (například počítače, mobilní telefony, tablety, IoT zařízení),
- nosiče obsahující šifrovací a jiné kryptografické algoritmy (například čipové karty, bezpečnostní tokeny),
- síťová zařízení (například routery, switche, modemy, firewally, access pointy),
- virtualizovaná média a interní cloud (například virtuální úložiště),
- technická aktiva mimo kontrolu organizace (například externí cloudové služby, osobní zařízení zaměstnanců, dodavatelů, komunikační infrastruktura pod správou dodavatele).

Likvidace technických aktiv je součástí odpovědného nakládání s informacemi. U subjektů v nižším režimu dle VBO-N má být postup jednoduchý, přiměřený a prakticky proveditelný. V případě potřeby stanovení konkrétní metody likvidace aktiva, se lze inspirovat v podpůrném materiálu **Bezpečná likvidace informací a dat: režim vyšších povinností**.

Pokud jsou technická aktiva, informace nebo data spravována prostřednictvím externí služby (například cloudové řešení), měla by být pravidla manipulace a likvidace stanovena i pro tato aktiva.

Pravidla a postupy likvidace informací a dat z pohledu řízení dodavatelů

Pokud jsou informace, data nebo technická aktiva umístěna mimo přímou kontrolu organizace (například v prostředí dodavatele poskytujícího cloudové služby nebo outsourcing), měla by ve smlouvě s dodavateli, přiměřeným způsobem, stanovit i pravidla pro likvidaci informací a dat, aby tím naplnila ustanovení pro zajištění bezpečnosti informací z pohledu důvěrnosti.

Pravidla a postupy likvidace v rámci smluvních vztahů s dodavateli by měly odpovídat významu aktiva a citlivosti zpracovávaných informací v souladu s § 3 odst. 5 VBO-N, kde je uvedeno, že povinná osoba při uzavírání smlouvy s dodavatelem do stanoveného rozsahu podle § 12 zákona zohlední hrozby a zranitelnosti spojené s tímto dodavatelem, celkovou kvalitu produktů a postupů v oblasti kybernetické bezpečnosti tohoto dodavatele, včetně postupů bezpečného vývoje.

Smluvní ustanovení by měla řešit zejména:

- způsob, jakým dodavatel likviduje informace a data po ukončení služby,
- jak bude organizace informována o provedené likvidaci dat a jak bude prokazatelně doložena,
- postupy pro nakládání se zálohami, kopiemi a obdobnými soubory,
- pravidla pro fyzickou likvidaci aktiv prováděnou dodavatelem,
- možnost provedení kontroly plnění smluvních podmínek.

I v případě zpracování smluvního ujednání by organizace měla zohlednit výše uvedený princip přiměřenosti a vycházet přitom z přílohy č. 2 VBO-N. Cílem je zajistit, aby data nebyla po ukončení jejich zpracování dostupná neoprávněným osobám a nemohla být zneužita ani na straně dodavatele.

7 Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol. Informace je označena příznakem, jenž určí podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
TLP:RED	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
TLP:AMBER+STRICT	Informace může být sdílena pouze v rámci organizace příjemce, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
TLP:AMBER	Informace může být sdílena v rámci organizace příjemce a jejím partnerům, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
TLP:GREEN	Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
TLP:CLEAR	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.

Verze dokumentu			
datum	**verze**	**změněno**	**popis změny**
31. března 2026	1.0	OK	Vytvoření dokumentu
2. června 2026	1.1	OK	Přidána příloha Bezpečná likvidace informací a dat