PORTÁL NÚKIB

Aplikace přiměřenosti při zavádění bezpečnostních opatření v režimu nižších povinností

TLP:CLEAR

31. března 2026

Verze 1.1

Národní úřad
pro kybernetickou
a informační bezpečnost

Obsah

1 Co se dozvím v tomto dokumentu?

Materiál se zaměřuje na aplikaci zásady přiměřenosti při zajišťovaní kybernetické bezpečnosti poskytovatelem regulované služby **v režimu nižších povinností** (dále jen „poskytovatel regulované služby“) podle § 3 odst. 1 písm. a) vyhlášky č. 410/2025 Sb. o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností (dále jen „vyhláška“). Materiál popisuje poskytovateli regulované služby, jakým způsobem uvažovat nad zaváděním a prováděním bezpečnostních opatření, tak aby k tomu docházelo přiměřeným a informovaným způsobem.

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

Tento podpůrný materiál není použitelný jako výklad pro plnění povinností poskytovatele regulované služby v režimu vyšších povinností, 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.

2 Základní pojmy a principy

V této kapitole jsou představeny základní pojmy a principy pro řízení kybernetické bezpečnosti, které jsou relevantní pro zavádění a provádění **přiměřených bezpečnostních opatření** podle zákona č. 264/2025 Sb., o kybernetické bezpečnosti a vyhlášky.

Smyslem povinnosti zavádět bezpečnostní opatření je stanovit poskytovateli regulované služby průběžnou povinnost (založenou na tzv. PDCA cyklu) neustále reagovat na aktuální rizika, která mu plynou z možného narušení důvěrnosti, integrity nebo dostupnosti aktiv (tzv. CIA triáda) s cílem kontinuálně zvyšovat jeho kybernetickou bezpečnost. Podrobnější výklad k těmto pojmům naleznete v následujících podkapitolách.

Kybernetickou bezpečností se rozumí soubor opatření, technologií, procesů a postupů, jejichž cílem je chránit počítačové systémy, sítě, aplikace a data před neoprávněným přístupem, útoky, zneužitím nebo poškozením.

Kybernetická bezpečnost je zvyšována prostřednictvím zavádění a provádění organizačních a technických bezpečnostních opatření zahrnujících mj.:

- **Ochranu dat** – šifrování, řízení přístupových práv, politiku hesel, zálohování.
- **Síťovou bezpečnost** – firewally, segmentace, ochrana proti přetížení a výpadku služby.
- **Bezpečnost koncových zařízení – antiviry, aktualizace, správa uživatelských oprávnění.**
- **Bezpečnost uživatelů** – školení proti phishingu a sociálnímu inženýrství.
- **Kontinuitu činností** – odpovědnost konkrétních osob, postupy obnovy technických aktiv.
- **Cloudovou bezpečnost** – ochrana dat uložených v cloudových službách.
- **Řízení incidentů** – detekce, určování jejich významnosti, hlášení a zvládání kybernetických útoků.

2.1 Performativní pravidla

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) u vyhlášky využívá tzv. **model performativních pravidel**. Performativní pravidla jsou ve vyhlášce vyjádřena cílem, kterého má být dosaženo, poskytovatel regulované služby například

- vynucuje dodržování pravidel a postupů stanovených v bezpečnostní politice a bezpečnostní dokumentaci,
- v rámci zajištění fyzické bezpečnosti zamezí neoprávněnému přístupu ke svým aktivům a předchází poškození, odcizení, zneužití aktiv, neoprávněným zásahům do nich a narušení bezpečnosti poskytování regulované služby.

Tyto obecně formulované cíle musí poskytovatel regulované služby plnit tím, že zavede konkrétní bezpečnostní opatření v podobě přizpůsobené vlastní organizaci a technickým možnostem.

Takový model právní regulace umožňuje poskytovatelům regulované služby volit vhodné způsoby naplnění požadavků vyhlášky, které jsou přizpůsobeny jeho konkrétní organizaci, místo jednotného řešení pro všechny. Vychází z předpokladu, že poskytovatel nejlépe zná svou infrastrukturu a specifika provozu, zatímco NÚKIB tyto informace nemá, dokud neprovede kontrolu poskytovatele. Proto model podporuje **individualizovaný přístup** k zajištění bezpečnosti, který je efektivnější než jiné modely.

Zjednodušeně řečeno vyhláška nemůže přesně říkat „*nainstalujte si software XY a nastavte ho podle přílohy č. 1 této vyhlášky*“. Takový postup by nikdy nebyl univerzálně použitelný pro všechny organizace, navíc by byl v rozporu se zásadou technologické neutrality.

2.2 Zajištění bezpečnosti informací (CIA triáda)

Důležitým bezpečnostním východiskem pro funkční pochopení specifik regulatorních požadavků je tzv. CIA triáda, která definuje klíčové prvky kybernetické bezpečnosti regulované služby:

Důvěrnost	informace a data jsou dostupné pouze oprávněným osobám
Integrita	informace a data jsou přesné, úplné a nebyly neoprávněně změněny či poškozeny
Dostupnost	informace a data jsou v případě potřeby dostupné oprávněným uživatelům

Při správném zavádění bezpečnostních opatření v organizaci je potřeba nahlížet na hrozby a rizika působící na danou organizaci pohledem všech těchto tří výše uvedených prvků. Pokud by byla zavedena jen bezpečnostní opatření zajišťující dostupnost nějakého systému, organizace bude nadále ohrožena hrozbou narušení integrity a důvěrnosti takového systému.

2.3 Zlepšování kybernetické bezpečnosti (PDCA cyklus)

Jde o čtyřkrokový neustále se opakující cyklus, jehož cílem je zlepšování procesů a řízení kvality. Používá se v průmyslu, službách, kybernetické bezpečnosti i projektovém managementu. Zavádění a provádění bezpečnostních opatření probíhá právě touto cyklickou metodou. Budování kybernetické bezpečnosti v organizaci není jednorázovou činností, ale postupným stále probíhajícím procesem.

1. PLAN (Plánujte)

Identifikujte relevantní hrozby pro jednotlivá aktiva či skupiny aktiv (např. ztráta, poškození či odcizení aktiva) a vyhodnoťte jejich dopad a pravděpodobnost.

Zohlednění přiměřenosti v prvotní fázi:

- Neopominutelná (§ 3 odst. 2 až 6, § 4 až 6 a § 10 vyhlášky) i vyhodnotitelná bezpečnostní opatření jsou stanovena samotnou vyhláškou.
- Zvažte, zda konkrétní způsob zavedení a provádění bezpečnostního opatření odpovídá míře rizika, potažmo bezpečnostním potřebám organizace.
- Upřednostňujte taková bezpečnostní opatření, která snižují vysoce pravděpodobná rizika před těmi, která cílí na rizika nejistá. Vyhnete se tím nadměrným nákladům nebo přílišné složitosti, pokud nehrozí kritické riziko.

2. DO (Proveďte)

Implementujte bezpečnostní opatření. Některá bezpečnostní opatření je vhodné implementovat postupně (částečně) a v průběhu vyhodnocovat jejich efektivitu.

- Například zavedení vícefaktorové autentizace pouze pro vybranou skupinu uživatelů (testovací množinu).

Průběžně dokumentujte způsob realizace, využité zdroje a vzniklé náklady.

3. CHECK (Kontrolujte)

Vyhodnoťte účinnost zavedených bezpečnostních opatření, a tedy i stavu kybernetické bezpečnosti organizace. V rámci vyhodnocování je dobré si zodpovědět následující otázky:

- Snížila se pravděpodobnost vzniku kybernetického bezpečnostního incidentu?
- Jsou náklady a dopad na uživatele přiměřené?

4. ACT (Jednejte)

Pokud bezpečnostní opatření splňuje cíle a je přiměřené, pokračujte v jeho zavádění či ho rozšiřte na celou organizaci. Pokud není, upravte plán (např. zvolte méně nákladné řešení nebo zjednodušte proces).

2.4 Rizika

Vyhláška nestanovuje podrobné povinnosti vedoucí k dokumentovanému řízení rizik (zpracování podrobné analýzy rizik je povinné pouze v režimu vyšších povinností). To však neznamená, že by se poskytovatelé regulovaných služeb měli úvahám nad možnými riziky zcela vyhnout.

Riziko je možnost, že určitá hrozba využije zranitelnosti aktiva a způsobí škodu.

Riziko tedy bude například situace, kdy útočník podvodným e-mailem (hrozba) využije toho, že uživatel nebyl dostatečně proškolený (zranitelnost), a proto otevře podvodný e-mail obsahující škodlivý kód a umožní napadení infrastruktury organizace (způsobená škoda).

Poskytovatelé regulovaných služeb stále musí zohledňovat své bezpečnostní potřeby a alespoň rámcově uvažovat nad možnými riziky a dopady, aby v souladu s § 3 odst. 1 písm. a) vyhlášky zavedli přiměřená bezpečnostní opatření.

Při rozhodování o zavedení či nezavedení **vyhodnotitelných** bezpečnostních opatření je v rámci principu přiměřenosti potřeba zohlednit:

- Velikost organizace.
- Personální a finanční možnosti (zdroje ve smyslu nalezení optimální nákladové přiměřenosti při zavádění bezpečnostních opatření).
- Pravděpodobnost výskytu incidentů.
- Kritičnost poskytované služby (i v případech kdy poskytovatel regulované služby poskytuje více služeb svým zákazníkům, některé jsou více či méně důležité, například z pohledu ochrany zdraví, nebo zajištění veřejné bezpečnosti),
- Bezpečnostní povědomí vrcholného vedení.
- Znalosti administrátorů.
- Stáří a technický stav výpočetní techniky.
- Další skutečnosti, které jsou specifické pro činnosti, které poskytovatel regulované služby poskytuje – cílem je, aby poskytovatel regulované služby zohlednil to, co pro něj může znamenat riziko a je pro něj relevantní.

PDCA cyklus se provádí opakovaně, což umožňuje kontinuální zlepšování a adaptaci na nové skutečnosti.

Tento cyklus je zohledněn v povinnosti každoročně zpracovat a minimálně po dobu 4 let uchovávat tzv. **Přehled bezpečnostních opatření**, jehož náležitosti upravuje § 3 odst. 2 vyhlášky a jeho vzor je obsahem přílohy č. 1 vyhlášky.

Tento dokument slouží především poskytovateli regulované služby, který má díky němu přehled o tom, jaká bezpečnostní opatření má zavedena, jaká má v plánu zavést, případně proč některá opatření nezavádí a nemá v plánu je zavádět.

3 Jak správně aplikovat přiměřenost při zavádění bezpečnostních opatření

Podle § 3 odst. 1 písm. a) vyhlášky poskytovatel regulované služby zavede a provádí bezpečnostní opatření, která jsou **přiměřená bezpečnostním potřebám**.

Zároveň podle § 3 odst. 1 písm. b) vyhlášky poskytovatel regulované služby zavede a provádí alespoň bezpečnostní opatření podle § 3 odst. 2 až 6, § 4 až 6 a § 10 vyhlášky. Tato opatření představují absolutní minimum v oblasti kybernetické bezpečnosti a je nutné je zavést vždy, i kdyby se poskytovatel domníval, že je nepotřebuje.

Aby mohla organizace uvažovat o přiměřenosti při zavádění bezpečnostních opatření, je vhodné připravit si několik základních podkladů. Doporučujeme vytvořit jednoduchý **seznam kritických aktiv**, tedy informací, systémů a služeb, které jsou pro fungování organizace nejdůležitější. U každého kritického aktiva je vhodné stručně popsat, **k čemu slouží a kdo jej využívá**. Dále doporučujeme identifikovat **kritické procesy**, jejichž narušení bude mít na poskytovatele regulované služby zásadní dopad.

Tyto podklady jsou nezbytné k zavedení neopominutelných bezpečnostních opatření podle § 4 odst. 6 vyhlášky (stanovení priority obnovy primárních aktiv) a § 6 vyhlášky (řízení kontinuity činností).

Organizace by si také měla definovat několik **základních hrozeb**, které mohou v jejím prostředí realisticky nastat, jako je například výpadek dodavatele, škodlivý kód, ztráta zařízení nebo neoprávněný přístup. U každé hrozby pak stačí orientačně posoudit **možný dopad** na provoz, finance nebo pověst a **pravděpodobnost**, s jakou může nastat. Tyto jednoduché podklady zpravidla postačují k tomu, aby i menší organizace dokázala určit přiměřená bezpečnostní opatření bez nutnosti provádět komplexní analýzu rizik. Při rozhodování o zavedení přiměřeného bezpečnostního opatření je třeba zvážit:

1. Možnost **výskytu rizika**.
2. Možný **dopad** na organizaci (finanční, reputační, provozní apod.).
3. **Očekávané snížení rizika** po zavedení opatření.
4. **Přímé i nepřímé náklady** spojené s implementací a provozem opatření.
5. **Existenci alternativních, méně nákladných, ale stejně účinných řešení**.

Pokud náklady na plné zavedení a provádění bezpečnostního opatření **významně převyšují očekávaný přínos** (např. snížení potenciálních škod), je vhodné prvně zvážit alespoň částečné zavedení opatření. Není-li opatření přiměřené ani při zavedení v omezeném rozsahu, je možné jej nezavést, pokud nejde o jedno z neopominutelných opatření zmíněných výše.

Příklad 1:

Pokud má poliklinika IT vybavení v hodnotě přibližně 300 000 Kč (několik počítačů v síti, vlastní server a licenční software pro evidenci pacientů). Při bližší znalosti kontextu organizace a důležitosti určených aktiv, v tomto případě zejména z pohledu zajištění důvěrnosti zpracovávaných dat a informací o pacientech, není ekonomicky přiměřené investovat 800 000 Kč do software monitorujícího aktivitu všech uživatelů IT vybavení (například prostřednictvím tzv. SIEM) či zajištění nepřetržitého monitoringu od dohledové centra (SOC). Při zohlednění typických hrozeb a určené hodnoty aktiv je vhodnější investovat do základního antiviru, pravidelného zálohování, školení personálu, vhodné segmentace sítě – tedy do opatření v řádu desítek tisíc korun, která výrazně sníží riziko a zároveň jsou udržitelná.

Příklad 2:

Zemědělský podnik provozuje evidenci zvířat, dálkovou správu a řízení krmení a základní účetnictví na několika počítačích s připojením k internetu a lokální síti. Při bližší znalosti kontextu organizace a důležitosti určených aktiv je možné prohlásit, že v tomto konkrétním případě není přiměřené pořizovat kybernetické zabezpečení za 300 000 Kč, zahrnující pokročilé firewally, redundantní servery a komplexní auditní systém. Mnohem efektivnější je investovat do osvěty zaměstnanců, zabezpečení přístupu (např. silným heslem a dvoufaktorovou autentizací), pravidelné aktualizace softwaru, jednoduchého zálohovacího řešení a funkčního fyzického zabezpečení – tedy opatření v řádu desítek tisíc korun. Úroveň zabezpečení odpovídá hodnotě určených aktiv a reálným hrozbám a zároveň je dlouhodobě udržitelná bez nutnosti například externí správy.

Pokud je finanční náročnost bezpečnostního opatření poskytovatelem regulované služby důvodně vyhodnocena jako nepřiměřená, je možné zvolit jiné, alternativní opatření či pokrýt riziko jen částečně levnějším opatřením. Tato situace může nastat např. při využívaní zastaralé technologie. V takovém případě je třeba začít vytvářet strategii i pro tzv. odstavení těch aktiv, se kterými riziko souvisí a jejich nahrazení aktivy novými, která již toto riziko neponesou.

Bezpečnostní opatření není nutné implementovat všechna najednou a okamžitě. V dokumentu **„Přehled bezpečnostních opatření“** lze jejich zavádění plánovat postupně, a to s ohledem na aktuální rozpočet, dostupné zdroje a s přihlédnutím k důležitosti opatření s ohledem na předpokládanou výši rizika. Před zpracováním Přehledu bezpečnostních opatření doporučujeme dokumentovanou formou určit prioritu zavedení bezpečnostních opatření, odrážející nejen důležitost regulované služby, ale celkový přístup k zajišťovaní kybernetické bezpečnost.

NÚKIB publikuje pravidelné informace o kybernetických hrozbách. Na základě těchto informací lze získat přehled o zvýšené či snížené možnosti výskytu rizika v kontextu společenské důležitosti a významnosti regulované služby včetně konkrétních zranitelností využívaných technických aktiv.

Klíčové body přiměřenosti

- **Proporcionalita**: Opatření musí odpovídat závažnosti rizika a bezpečnostním potřebám.
- **Ekonomická efektivita**: Náklady nesmí převyšovat přínos a možný dopad incidentu.
- **Uživatelská přívětivost**: Příliš složitá opatření mohou vést k obcházení.

Při zavádění bezpečnostních opatření vždy upřednostňujte taková konkrétní řešení, která při vynaložení přiměřeného úsilí skutečně snižují možné negativní dopady na důvěrnost, integritu a dostupnost regulované služby.

Smyslem regulace kybernetické bezpečnosti není formální splnění veškerých požadavků vyhlášky, ale **reálné zvýšení úrovně kybernetické bezpečnosti v organizaci**.

Další informace k zavadění a provádění bezpečnostních opatření najdete v Manuálu pro poskytovatele regulovaných služeb v režimu nižších povinností na Portálu NÚKIB.

4 Praktické příklady zavedení bezpečnostních opatření zohledňující přiměřenost

4.1 Bezpečnost lidských zdrojů - § 5

Souhrn požadavků vyhlášky:

- Stanovení politiky bezpečného chování uživatelů (relevantní témata dle přílohy č. 3 vyhlášky).
- Stanovení pravidel rozvoje bezpečnostního povědomí.
- Postupy kontroly dodržování nastavených pravidel.
- Provádění vstupních a pravidelných školení v oblasti kybernetické bezpečnosti.
- Vedení přehledů o provedených školeních a vedení seznamů školených osob.

Modelová organizace A (menší organizace):

Stanoví politiku bezpečného chování uživatelů a při její tvorbě přiměřeně zohlední relevantní témata uvedená v příloze č. 3 vyhlášky. Stanoví pravidla pro rozvoj bezpečnostního povědomí obsahově přizpůsobená pro jednotlivé role – vrcholné vedení, uživatelé, administrátoři a osoba či osoby pověřené kybernetickou bezpečností.

Všichni noví zaměstnanci absolvují školení kybernetické bezpečnosti. Školení všech stálých zaměstnanců probíhá každoročně (využívá bezplatný online kurz od NÚKIB – Základy kybernetické bezpečnosti: Dávej kyber 26). Vede přehledy o provedených školeních a seznamy osob, které školení

absolvovaly. Probíhá nepravidelná kontrola dodržování bezpečnostní politiky, a jsou stanoveny postupy pro případ řešení případů porušení bezpečnostní politiky.

Modelová organizace B (větší organizace):

Stanoví politiku bezpečného chování uživatelů a při její tvorbě přiměřeně zohlední všechna témata uvedená v příloze č. 3 vyhlášky. Stanovení pravidla pro rozvoj bezpečnostního povědomí přizpůsobená pro jednotlivé role – vrcholné vedení, uživatelé, administrátoři a osoby pověřené kybernetickou bezpečností. Dále stanoví pravidla pro tvorbu hesel.

Všichni noví zaměstnanci absolvují školení kybernetické bezpečnosti. Školení všech stálých zaměstnanců probíhá každoročně prostřednictvím bezplatného online kurzu NÚKIB – Základy kybernetické bezpečnosti: Dávej kyber 26. Administrátoři a osoby odpovědné za kybernetickou bezpečnost mají specifický plán rozvoje bezpečnostního povědomí. Ten je více zaměřený na získávání účelných a (s ohledem na složitost a kritičnost poskytované služby) přiměřených znalostí a dovedností určených k dalšímu odbornému rozvoji při zajišťovaní kybernetické bezpečnosti, a to nejen u technický aktiv.

Vede přehledy o provedených školeních a eviduje osoby, které školení absolvovaly. Dále vede evidenci o provedených školeních či jiném prohlubování odborné způsobilosti u administrátorů a osob pověřených kybernetickou bezpečností. Probíhá pravidelná (i neohlášená) kontrola dodržování bezpečnostní politiky ze strany vedoucích zaměstnanců. Nedodržování bezpečnostní politiky je postihováno a jsou stanovený postupy pro řešení případů jejich porušení (např. odebráním přístupových práv nebo zahájením kárného řízení).

4.2 Řízení kontinuity činností - § 6

Souhrn požadavků vyhlášky:

- Stanovení priority, pořadí a postupů obnovy.
- Vytváření pravidelných záloh informací, dat a konfigurací nezbytných pro případ obnovy.

Modelová organizace A (menší organizace):

Vrcholné vedení určilo, která aktiva (například servery, systémy a data) jsou kritická pro zajištění provozu regulované služby a mají být obnovena jako první. Následně určila a zaevidovala s ohledem na kritičnost aktiva a konkrétní pořadí obnovy relevantních technických aktiv. Pořadí obnovy je vedeno dokumentovanou formou společně s kontakty na odpovědné osoby a dodavatele. Prozatím nejsou prováděny zálohy všech informací, dat, konfigurací a nastavení technických aktiv nezbytných zejména pro účely obnovy regulované služby. Postupně jsou do procesu záloh přidávána aktiva dle určené priority.

Modelová organizace B (větší organizace):

Vrcholné vedení určilo, která aktiva (například servery, systémy a data) jsou kritická pro zajištění provozu regulované služby a mají být obnovena jako první. Následně určila a zaevidovala, s ohledem na kritičnost aktiva, konkrétní pořadí obnovy relevantních technických aktiv. Pořadí obnovy je vedeno dokumentovanou formou ve formě interního aktu společně s kontakty na odpovědné osoby a dodavatele. Konkrétní povinnosti a odpovědnosti jsou specifikovány pro konkrétní dotčené osoby

a jsou pravidelně aktualizovány. Jsou prováděny pravidelné zálohy informací, dat, konfigurací a nastavení technických aktiv nezbytných zejména pro účel obnovy regulované služby pro případ kybernetického bezpečnostního incidentu.

4.3 Řízení přístupu - § 7

Souhrn požadavků vyhlášky:

- Zavedení principů oprávnění, jedinečných identifikátorů a oddělování privilegovaných účtů.
- Řízení přístupových práv rámci celého životního cyklu (přidělování, změna, odebírání, přezkum).
- Řízení mobilních zařízení a zařízení mimo správu organizace (např. BYOD).
- Řešení fyzické bezpečnosti k ochraně aktiv před fyzickým poškozením, krádeží apod.

Modelová organizace A (menší organizace):

Vede evidenci přístupových práv a oprávnění zaměstnanců v centralizovaném nástroji. Změny v přístupových právech a oprávněních jsou evidovány na papíře (např. při nástupu či odchodu zaměstnance evidenčním listem). Jednou ročně provádí interní IT zaměstnanec manuální kontrolu, při které upozorňuje nadřízené relevantních zaměstnanců o objevených nesrovnalostech.

Modelová organizace B (větší organizace):

Vede evidenci přístupových práv a oprávnění zaměstnanců a najímaných externistů v centralizovaném nástroji. Změny v přístupových právech a oprávněních jsou procesovány a evidovány v ticketovacím nástroji, ve kterém probíhají i veškerá potřebná schválení nadřízenými zaměstnanci. Jednou ročně jsou poskytnuty nadřízeným zaměstnancům výpisy s přidělenými přístupovými právy a oprávněními podřízených zaměstnanců a externistů, které musí odsouhlasit nebo nechat revidovat.

4.4 Detekce a zaznamenávání kybernetických bezpečnostních událostí - § 9

Souhrn požadavků vyhlášky:

- Ochrana perimetru komunikační sítě – firewall pro ochranu a blokování nežádoucí komunikace.
- Ochrana před škodlivým kódem na koncových stanicích a serverech, např. formou antiviru nebo monitoringu koncových zařízení (např. EDR).
- Zabezpečení používání vyměnitelných zařízení (např. USB flash disků).
- Zaznamenávání událostí z nástrojů, které detekují kybernetické bezpečnostní události.

Modelová organizace A (menší organizace):

Disponuje firewallem, u kterého je zapnuto výchozí nastavení doporučené výrobcem. Na koncových stanicích a serverech je zaveden výchozí nástroj pro nepřetržitou automatickou ochranu před škodlivým kódem, který je součástí operačního systému. Nástroj upozorňuje na výskyt relevantních detekovaných kybernetických bezpečnostních událostí prostřednictvím zasílání e-mailových upozornění IT zaměstnanci. Tento nástroj se aktualizuje samostatně v rámci dostupných aktualizací

vydaných výrobcem operačního systému. O rizicích spojených s automatickým spouštěním obsahu (např. škodlivého kódu či software) a připojováním vyměnitelných zařízení jsou zaměstnanci informováni při nástupním školení, ale technicky tato oblast více zabezpečena není.

Modelová organizace B (větší organizace):

Disponuje firewallem s pokročilými funkcionalitami, které průběžně ladí a nastavují zaměstnanci IT oddělení. Na koncových stanicích a serverech je zaveden nástroj pro nepřetržitou automatickou ochranu před škodlivým kódem s pokročilými EDR funkcionalitami, jako např. behaviorální analýzou. Nástroj disponuje konzolí pro centrální správu, která je aktivně monitorována IT zaměstnanci a poskytuje aktuální přehled o detekovaných kybernetických bezpečnostních událostech. Aktualizace tohoto nástroje jsou automatizované a mohou být více řízeny pomocí konzole pro centrální správu. V neposlední řadě tento nástroj technicky řídí a omezuje automatické spouštění obsahu a vyhodnocuje bezpečnost připojovaných vyměnitelných zařízení.

5 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**
12. ledna 2026	1.0	OK	Vytvoření dokumentu
31. března 2026	1.1	OK	Drobné úpravy příkladů, oprava chyb v textu