

PŘÍLOHA 9: ZPRÁVA O HODNOCENÍ RIZIK – MINISTERSTVO PRO CERTIFIKACI SENZORŮ

Verze dokumentu			
datum	verze	změněno	provedená změna
18. 2. 2026	1.0	Manažer KB	Vytvoření dokumentu
30. 2. 2026	1.0	Výbor pro řízení KB	Schválení dokumentu

1 Účel dokumentu a předmět hodnocení

Účelem dokumentu je shrnutí procesu a výsledků provedeného hodnocení rizik na Ministerstvu pro certifikaci senzorů. Hodnocení rizik je detailně zaznamenáno v dokumentu *Příloha 6: Vzorové hodnocení aktiv a rizik*. V rámci celého procesu hodnocení rizik byl použit postup popsáný v bezpečnostních politikách ministerstva a primárně dokument *Příloha 2: Vzorová metodika pro identifikaci a hodnocení aktiv a hodnocení rizik*.

Předmětem hodnocení rizik je určená služba certifikace senzorů, jenž ministerstvo poskytuje.

2 Přehled aktiv

Poskytovaná služba certifikace senzorů byla pro účely hodnocení rizik rozdělena na několik typových primárních a podpůrných aktiv. Primární aktiva, na která jsou podpůrná aktiva navázána a samotná podpůrná aktiva, jejich hodnocení, gestoři a garanti aktiv a popisy jednotlivých hodnot jsou obsahem dokumentu *Příloha 6: Vzorové hodnocení aktiv a rizik*.

3 Zvládání rizik

3.1 Kritéria pro akceptovatelnost

Rizika, která přesáhla hranici 32, jsou neakceptovatelná a pro jejich snížení je nutné zavádět bezpečnostní opatření. Tento postup je popsán v rámci příslušné metodiky v dokumentu *Příloha 2: Vzorová metodika pro identifikaci a hodnocení aktiv a hodnocení rizik*. Seznam neakceptovatelných rizik se nachází v dokumentu *Příloha 6: Vzorové hodnocení aktiv a rizik* na záložce Katalog rizik. Rizika, která nepřesáhla hranici 32, jsou považována za akceptovatelná, případně budou snižována méně náročnými opatřeními a jejich hodnota bude dále pravidelně sledována.

3.2 Shrnutí

Celkový počet rizik:	78
Neakceptovatelná rizika:	20
Potřebná bezpečnostní opatření:	20
Odhad ceny za zavedení bezpečnostních opatření:	40 700 000 Kč

3.3 Zvládání rizik identifikovaných v rámci hodnocení rizik

Manažer KB a další osoby podílející se na zajišťování bezpečnosti informací navrhli taková bezpečnostní opatření, která by měla snížit hodnotu všech rizik s hodnotou 32 a vyšší na novou, nižší úroveň. Byla vybrána taková bezpečnostní opatření, která jsou způsobitelná rizika skutečně a účinně snížit, za současného zohlednění přiměřenosti zvolených bezpečnostních opatření ve vztahu k požadovanému cíli a nákladům, které jsou s implementací opatření spojeny.

Tato opatření byla zanesena do plánu zvládání rizik. Plán zvládání rizik musí schválit výbor pro řízení KB a následně budou bezpečnostní opatření co nejdříve, v souladu s plánem, implementována. Následně bude vyhodnoceno, zda jsou tato opatření skutečně účinná a bude případně rozhodnuto o dalším postupu.

Ministerstvo v rámci hodnocení rizik zohlednilo Varování NÚKIB ze dne 17. 12. 2018 na dvou určených podpůrných aktivech PO20 Switch (přepínač) a PO21 Switch (přepínač). Příslušná

určená rizika jsou uvedena v dokumentu *Příloha 6: Vzorové hodnocení aktiv a rizik na záložce Katalog rizik*. U těchto rizik došlo k přehodnocení hrozby na hodnotu 4. Následně byl u neakceptovatelných rizik navržen vhodný způsob jejich zvládnání v souladu s metodikou.

3.4 Bezpečnostní opatření, která je nutno aplikovat

V rámci hodnocení rizik bylo identifikováno 20 rizik, která mají hodnotu 32 a vyšší.

Z hodnocení rizik vyplynula následující opatření, která je nutné implementovat:

- Nahradit zastaralé technologie a technická aktiva novými
- Zajistit, aby byla všechna technická aktiva výrobcem, dodavatelem nebo jinou osobou podporována
 - Vytvořit samostatný segment pro nepodporovaná technická aktiva či zastaralé technologie
- Zajistit pravidelnou aktualizaci antivirové ochrany
- Aktualizovat smlouvu s dodavatelem A:
 - Doplnit do ní relevantní ustanovení z přílohy č. 5 vyhlášky
 - Zohlednit v ní požadavky ISMS ministerstva
 - Doplnit požadavek, aby byli administrátoři dodavatele dostatečně odborně vzdělaní
 - Doplnit požadavek, aby byli administrátoři dodavatele poučeni o relevantních politikách ministerstva
 - Doplnit požadavek, aby dodavatel poskytoval školení pro uživatele ministerstva a jeho opakování při každém upgradu
 - Doplnit požadavky na zachování mlčenlivosti
 - Doplnit ustanovení týkající se zdrojového kódu
 - Aktualizovat SLA
- Vytvořit školení pro zaměstnance ministerstva o:
 - Základech KB, včetně poučení o bezpečnostních politikách ministerstva zahrnující pravidla fyzické bezpečnosti
 - Hrozbách, např. phishing, vishing
 - Pravidelně uživatele školit a ověřovat znalosti závěrečným testem
 - Aktualizovat plán rozvoje bezpečnostního povědomí
- Provést analýzu dopadů a stanovit cíle řízení kontinuity činností
- Na základě analýzy dopadů vypracovat plány kontinuity činností a havarijní plány a do nich zahrnout i dodavatele
- Zpracovat provozní pravidla a postupy včetně stanovení odpovědností
- Vytvořit a obsadit nová pracovní místa pro zajištění činností spojených s KB a zajištěním provozu
- Aktualizovat smlouvu s dodavatelem B:
 - Doplnit do ní relevantní ustanovení z přílohy č. 5 vyhlášky

- Zohlednit v ní požadavky ISMS ministerstva
- Aktualizovat SLA
- Zapracovat do smlouvy exit strategii
- Předání know-how
- Požadovat vypracování, předání a pravidelnou aktualizaci dokumentace dodávané dodavatelem
- Doplnit požadavky na interval provádění pravidelných aktualizací
- Stanovit pravidla pro dodavatele
- Stanovit bezpečnostní požadavky na projekty akvizice, vývoje a údržby

Odhad ceny za navrhnutá bezpečnostní opatření: 8 700 000 Kč

3.5 Bezpečnostní opatření, která je vhodné aplikovat

V rámci hodnocení rizik byla určena rizika, která sice nepřesahují hranici pro akceptaci, ale přesto je vhodné je řídit a implementovat vybraná bezpečnostní opatření v souladu s bezpečnostními politikami, ve kterých je uvedeno, že tato rizika mohou být snižována méně náročnými bezpečnostními opatřeními. V případě dlouhodobého ignorování těchto rizik může dojít k přesáhnutí hodnoty akceptace a tato bezpečnostní opatření budou muset být implementována.

Tato bezpečnostní opatření jsou následující:

- Zajistit odborná školení pro bezpečnostní role a administrátory a aktualizovat plán rozvoje bezpečnostního povědomí
- Nasadit nástroj PIM/PAM
- Zajistit novou hlavní serverovnu odpovídající aktuálním standardům v odlišné lokalitě a stávající ponechat jako záložní
- Provést zákaznický audit u dodavatele B zaměřený na zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů
- Pořídit nový perimetrový FW v clusteru
- Vytvořit politiku řízení přístupů a pravidla v ní uvedená technicky vynucovat

Odhad ceny za navrhnutá bezpečnostní opatření: 32 000 000 Kč

4 Související dokumentace

- Příloha 1: Vzorová politika systému řízení bezpečnosti informací
- Příloha 2: Vzorová metodika pro určování a hodnocení aktiv a rizik
- Příloha 6: Vzorové hodnocení aktiv a rizik
- Příloha 8: Vzorový plán zvládání rizik
- Příloha 14: Zkratky a používané pojmy