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

Přehledový dokument

Verze dokumentu			
Datum	**Verze**	**Změněno**	**Provedená změna**
18. 2. 2022	1.0	Manažer kybernetické bezpečnosti	Vytvoření dokumentu
25. 2. 2022	1.0	Výbor 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 popsaný v bezpečnostních politikách Ministerstva pro certifikaci senzorů. Byl použit hlavně dokument Příloha 2: Vzorová metodika pro identifikaci a hodnocení aktiv a hodnocení rizik.

Předmětem hodnocení rizik je agendový IS pro evidenci a zpracování procesu certifikace senzorů, jehož správce je Ministerstvo pro certifikaci senzorů.

2 Přehled aktiv

Agendový IS pro evidenci a zpracování procesu certifikace senzorů byl pro účely hodnocení rizik rozdělen 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 atd. 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. 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

Expertním týmem byla navržena taková opatření, která by měla snížit hodnotu všech rizik s hodnotou 32 a vyšší na novou, nižší úroveň. Byla vybrána taková bezpečnostní opatření, která jsou ze zkušeností expertního týmu způsobilá identifikovaná 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 budou zanesena do plánu zvládání rizik. Plán zvládání rizik musí schválit výbor 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 2 identifikovaných podpůrných aktivech PO3: Webový server (HW) a PO21 Switch (přepínač). Příslušná identifikovaná 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 zvládání 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:

- Zajistit, aby byla všechna technická aktiva pod podporou.
- Zajistit pravidelnou aktualizaci antivirové ochrany.
- Aktualizovat smlouvu s dodavatelem A, doplnit do ní relevantní ustanovení z přílohy č. 7 VKB, 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 na školení pro uživatele ministerstva zajišťovaná dodavatele na používání dodávaného IS a opakování školení 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 včetně pravidel fyzické bezpečnosti, o hrozbách, např. phishing, pravidelně uživatele školit o 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.
- Nahradit zastaralé technologie novými.
- 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. 7 VKB, zohlednit v ní požadavky ISMS ministerstva, aktualizovat SLA, zapracovat do smlouvy exit strategii, předání know-how, požadovat vypracování, předání a pravidelnou aktualizaci dokumentace dodavatelem, doplnit požadavky na interval provádění pravidelných aktualizací.
- Stanovit pravidla pro dodavatele.
- Vytvořit samostatný segment pro zastaralé technologie.
- 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 identifikovaná rizika, která sice nepřesahují hranici pro akceptaci, ale přesto je vhodné je řídit a implementovat vybraná bezpečnostní opatření v souladu s bezpečnostními politikami, které říkají, 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.
- Aktualizovat smlouvu s dodavatelem C, doplnit do ní relevantní ustanovení z přílohy č. 7 VKB, zohlednit v ní požadavky ISMS ministerstva, doplnit požadavky na interval provádění pravidelných aktualizací, zvýšit sankce za nehlášení kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů.
- Provést zákaznický audit u dodavatele C 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 identifikaci a hodnocení aktiv a hodnocení rizik

Příloha 6: Vzorové hodnocení aktiv a rizik

Příloha 7: Vzorový plán zvládání rizik

Příloha 13: Zkratky a používané pojmy