

PŘÍLOHA 11: ZPRÁVA O HODNOCENÍ RIZIK PRO VEŘEJNOU ZAKÁZKU– MINISTERSTVO PRO CERTIFIKACI SENZORŮ

Verze dokumentu			
datum	verze	změněno	provedená změna
21. 2. 2026	1.0	Manažer KB	Vytvoření dokumentu
30. 3. 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, které bylo provedeno v souvislosti s předmětem výběrového řízení – **Nákup komunikačních prostředků a technického vybavení (HW) pro agendový IS pro evidenci a zpracování procesu certifikace senzorů**. Informace v tomto dokumentu slouží jako vstup do další fáze výběrového řízení a následné hodnocení rizik již implementovaného řešení.

Hodnocení rizik je detailně zaznamenáno v dokumentu *Příloha 10: Vzorové hodnocení rizik pro veřejnou zakázku*.

V rámci celého procesu hodnocení rizik byl použit postup popsáný v bezpečnostních politikách ministerstva. Byl použit především dokument *Příloha 2: Vzorová metodika pro určování a hodnocení aktiv a rizik*.

Při hodnocení bylo zohledněno varování Národního úřadu pro kybernetickou a informační bezpečnost ze dne 17. prosince 2018 před používáním technických a programových prostředků společnosti Huawei Technologies Co., Ltd., Šen-čen, Čínská lidová republika, protože jejich používání představuje bezpečnostní hrozbu (dále jen „varování NÚKIB“).

Předmětem hodnocení rizik jsou komunikační prostředky a technické vybavení (HW) pořizované pro zajištění chodu agendového IS pro evidenci a zpracování procesu certifikace senzorů, jehož správce je ministerstvo.

2 Přehled aktiv

Pro účely hodnocení rizik byla použita následující typová podpůrná aktiva:

- Switch (přepínač)
- Backup a obslužný server

Vzhledem k tomu, že při hodnocení podpůrných aktiv musí být vzata v úvahu hodnota relevantních primárních aktiv, bylo analyzováno, jaká primární aktiva budou mít vazbu na podpůrná aktiva, která jsou předmětem výběrového řízení. S ohledem na to, že primární aktivum Služba certifikace senzorů pracuje se všemi informacemi v agendovém IS a přebírá nejvyšší hodnoty těchto informací dle jednotlivých atributů, postačuje pro hodnocení rizik v souvislosti s výběrovým řízením zohlednit hodnotu primárního aktiva Služba certifikace senzorů.

Aktiva jsou hodnocena zvlášť z pohledu důvěrnosti, integrity a dostupnosti.

Primární aktivum Služba certifikace senzorů, na které jsou podpůrná aktiva navázána a samotná podpůrná aktiva, která jsou předmětem hodnocení, zobrazují následující tabulky:

Tabulka 1: Seznam relevantních primárních aktiv

ID	Typové primární aktivum	Název	Kategorie	Specifikace	Osobní údaje	Legislativa	Rozsah řízení KB	Dostupnost	Ztráta	Důvěrnost	Integrita
S1	Služba certifikace senzorů	S1: Služba certifikace senzorů	služba	Zajištění procesu certifikace a evidence senzorů	ano	Zákon o certifikaci	ano	3	4	3	3

Tabulka 2: Seznam soutěžených podpůrných aktiv

ID	Kategorie podpůrného aktiva	Skupina podpůrného aktiva	Typové podpůrné aktivum	Název	Popis podpůrného aktiva	Dostupnost	Ztráta	Důvěrnost	Integrita
PO 1	Komunikační prostředky	Síťová zařízení	Switch (přepínač)	PO1: Switch (přepínač)	velké L3 switche, 10 ks	3	2	2	3
PO 2	Technické vybavení (HW)	Servery	Backup a obslužný server	PO2: Backup a obslužný server	server, disková pole, páskové jednotky	3	3	3	3

3 Identifikace a hodnocení hrozeb a zranitelností

Pro vytvoření katalogu hrozeb a katalogu zranitelností sloužily jako podklady vyhláška č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností a metodika k varování NÚKIB ze dne 17. prosince 2018 dostupná na webových stránkách NÚKIB.

Katalog zranitelností obsahuje **17 obecných zranitelností**, které byly následně přizpůsobeny pro konkrétní hodnocení rizik podle charakteru hodnocených aktiv a zkušeností expertního týmu.

Katalog hrozeb obsahuje **21 obecných hrozeb**, které byly následně přizpůsobeny konkrétnímu hodnocení rizik podle charakteru hodnocených aktiv a zkušeností expertního týmu.

Zranitelnosti nebo hrozby, případně jejich kombinace, které se v rámci výsledného hodnocení rizik nevyskytují, byly vyhodnoceny jako nerelevantní v kombinaci aktivum-zranitelnost-hrozba, a nebylo s nimi tedy dále pracováno.

Přiřazení konkrétních hodnot jednotlivým zranitelnostem a hrozbám bylo provedeno na základě znalostí a zkušeností hodnotitelů s obdobnými technickými a programovými prostředky a s jejich fungováním ve strukturách Ministerstva pro certifikaci senzorů.

4 Hodnocení rizik

4.1 Metodika hodnocení rizik a kritéria pro akceptovatelnost

V rámci hodnocení rizik byly vytvořeny relevantní kombinace aktivum-zranitelnost-hrozba. Jednotlivé položky byly ohodnoceny v souladu s bezpečnostními politikami na stupnici 1 až 4. Následně byly tyto hodnoty mezi sebou vynásobeny, čímž vznikla výsledná hodnota rizika. Matematicky lze tento postup vyjádřit následujícím vzorcem:

$$\text{Hodnota rizika} = \text{hodnota dopadu} \times \text{hodnota hrozby} \times \text{hodnota zranitelnosti}$$

Rizika, která přesáhla hranici 32, jsou neakceptovatelná a pro jejich snížení je nutné zavádět bezpečnostní opatření. Tento postup je popsán v rámci *Přílohy 2: Vzorová metodika pro identifikaci a hodnocení aktiv a rizik*, ze které vychází i níže uvedená Tabulka 3:

Tabulka 3: Seznam relevantních primárních aktiv

Hodnocení rizik		
Úroveň		Popis
Nízká	1–16	Riziko je považováno za přijatelné – akceptovatelné.
Střední	17–31	Riziko může být sníženo méně náročnými bezpečnostními opatřeními nebo v případě vyšší náročnosti bezpečnostních opatření je riziko akceptovatelné.
Vysoká	32–47	Riziko je dlouhodobě nepřijatelné a musí být zahájeny systematické kroky k jeho odstranění.
Kritická	48–64	Riziko je nepřijatelné a musí být neprodleně zahájeny kroky k jeho odstranění.

Rizika, která nepřesáhla hranici 32, jsou považována za akceptovatelná, případně budou snižována méně náročnými bezpečnostními opatřeními a jejich hodnota bude dále pravidelně sledována.

4.2 Výsledky hodnocení rizik

Byla provedena celkem 3 hodnocení rizik:

4.2.1 Výchozí hodnocení ve stávajícím prostředí v případě vysoutěžení prvků společností uvedených ve varování NÚKIB

Z důvodu možného vysoutěžení prvků společností uvedených ve varování NÚKIB bylo při tomto výchozím hodnocení postupováno v souladu s „Metodikou k varování ze dne 17. prosince 2018“, která říká, že hrozbu, na kterou je v rámci varování NÚKIB upozorněno, je nutné hodnotit v souladu s tabulkou č. 1 přílohy č. 4 vyhlášky jako velmi pravděpodobnou až více méně jistou. Tyto hrozby jsou označeny v použitém katalogu hrozeb oranžovou barvou a ve sloupci „Působení varování NÚKIB ze dne 17. prosince 2018“ mají hodnotu „Ano“. V rámci analýzy rizik byly v souladu s metodikou NÚKIB ohodnoceny hodnotou 4.

Tabulka 4: Výsledky výchozího hodnocení rizik

Hodnoty rizik	Počet rizik
Kritická s dopadem na dostupnost	48
Kritická s dopadem na důvěrnost	27
Kritická s dopadem na integritu	44
Vysoká s dopadem na dostupnost	34
Vysoká s dopadem na důvěrnost	41
Vysoká s dopadem na integritu	24
Suma rizik nad hranici 32:	218
Střední s dopadem na dostupnost	54
Střední s dopadem na důvěrnost	43
Střední s dopadem na integritu	62
Nízká s dopadem na dostupnost	33
Nízká s dopadem na důvěrnost	60
Nízká s dopadem na integritu	38
Suma rizik pod hranici 32:	290

4.2.1.1 Návrh bezpečnostních opatření pro snížení neakceptovatelných rizik

Z důvodu výskytu **218** neakceptovatelných rizik bylo nutné přistoupit k jejich snížení, a to pomocí vhodných bezpečnostních opatření. Dle povahy byla bezpečnostní opatření rozdělena do dvou variant:

Varianta A

Tabulka 5: Návrh bezpečnostních opatření pro snížení neakceptovatelných rizik varianta A

ID bezpečnostního opatření	Popis bezpečnostního opatření
OP2	Pořízení duplicitní technologie od společností, které nejsou uvedeny ve varování NÚKIB ze 17. prosince 2018.
OP3	Zavedení podrobného monitoringu obsahu přenášených dat.
OP4	Zavedení podrobné kontroly SW kódu.
OP5	Zavedení šifrování zařízení.
OP6	Nevracení vadných komponent dodavateli/výrobci.
OP7	Zohlednění kybernetické bezpečnosti ve smluvním ustanovení.

V případě varianty A nebudou vyloučeny prvky společností uvedených ve varování NÚKIB, čímž tedy nedojde ke snížení pravděpodobnosti hrozeb s nimi souvisejících z hodnoty 4, avšak budou přijata bezpečnostní opatření, která sníží hodnotu závažnosti zranitelností u těchto prvků. Hrozby spojené s prvky z varování NÚKIB působí na všechny atributy informační bezpečnosti, tedy dostupnost, důvěrnost i integritu, proto při návrhu bezpečnostních opatření bylo nutné zvažovat bezpečnostní opatření pro ochranu všech atributů informační bezpečnosti. Bezpečnostní opatření OP2 cílí zejména na zajištění dostupnosti primárních aktiv v případě, kdy by prvek společnosti uvedený ve varování NÚKIB selhal, nebo byl záměrně vyřazen z provozu. Ostatní bezpečnostní opatření cílí zejména na zajištění důvěrnosti a integrity primárních aktiv. Předpokládané výsledky hodnocení rizik po přijetí bezpečnostních opatření z varianty A jsou uvedeny v [kapitole 4.2.2 Varianta A: Hodnocení rizik ve stávajícím prostředí v případě vysoutěžení prvků společností uvedených ve varování NÚKIB s dodatečnými bezpečnostními opatřeními](#).

Varianta B

Tabulka 6: Návrh bezpečnostního opatření pro snížení neakceptovatelných rizik varianta B

ID bezpečnostního opatření	Popis bezpečnostního opatření
OP1	Vyloučení prvků společností uvedených ve varování NÚKIB ze 17. prosince 2018 z veřejné zakázky.

V případě varianty B budou vyloučeny prvky společností uvedených ve varování NÚKIB z veřejné zakázky, čímž dojde ke snížení pravděpodobnosti hrozeb s nimi souvisejících z hodnoty 4 a také ke změně hodnot závažnosti zranitelností u těchto prvků. Předpokládané výsledky hodnocení rizik po přijetí bezpečnostních opatření z varianty B jsou uvedeny v [kapitole 4.2.3 Varianta B: Hodnocení rizik ve stávajícím prostředí v případě, že budou vyloučeny prvky společností uvedených ve varování NÚKIB](#).

4.2.2 Varianta A: Hodnocení rizik ve stávajícím prostředí v případě vysoutěžení prvků společností uvedených ve varování NÚKIB s dodatečnými bezpečnostními opatřeními

Tabulka 7: Výsledky hodnocení rizik varianta A

Hodnoty rizik	Počet rizik	Rozdíl oproti výchozímu hodnocení
Kritická s dopadem na dostupnost	0	-48
Kritická s dopadem na důvěrnost	0	-27
Kritická s dopadem na integritu	0	-44
Vysoká s dopadem na dostupnost	44	+10
Vysoká s dopadem na důvěrnost	23	-18
Vysoká s dopadem na integritu	34	+10
Suma rizik nad hranici 32:	101	-117
Střední s dopadem na dostupnost	72	+18
Střední s dopadem na důvěrnost	59	+16
Střední s dopadem na integritu	78	+16
Nízká s dopadem na dostupnost	53	+20
Nízká s dopadem na důvěrnost	89	+29
Nízká s dopadem na integritu	56	+18

Suma rizik pod hranici 32:	407	+117
----------------------------	-----	------

4.2.2.1 Zhodnocení a vyčíslení varianty A

Díky navrženým bezpečnostním opatřením dojde v případě varianty A k předpokládanému snížení dodatečných 117 neakceptovatelných rizik (z celkového počtu 218) na akceptovatelnou úroveň (pod hranici 32). Nadále však zůstane 101 rizik nad hranicí akceptovatelnosti, a to z toho důvodu, že **bezpečnostní opatření, která je nutné zavést nesouvisí s předmětem veřejné zakázky a jsou řešena standardním hodnocením rizik a souvisejícím plánem zvládnutí rizik.**

Tabulka 8: Finanční vyjádření bezpečnostních opatření varianty A

ID bezpečnostního opatření	Předpokládaná cena bezpečnostního opatření (bez DPH)
OP2	370 000 Kč
OP3	4 400 000 Kč
OP4	14 500 000 Kč
OP5	1 500 000 Kč
OP6	750 000 Kč
OP7	0 Kč
Suma:	21 520 000 Kč

4.2.3 Varianta B: Hodnocení rizik ve stávajícím prostředí v případě, že budou vyloučeny prvky společností uvedených ve varování NÚKIB

Tabulka 9: Výsledky hodnocení rizik varianty B

Hodnoty rizik	Počet rizik	Rozdíl oproti výchozímu hodnocení
Kritická s dopadem na dostupnost	0	-48
Kritická s dopadem na důvěrnost	0	-27
Kritická s dopadem na integritu	0	-44
Vysoká s dopadem na dostupnost	0	-34
Vysoká s dopadem na důvěrnost	0	-41
Vysoká s dopadem na integritu	0	-24
Suma rizik nad hranici 32:	0	-218
Střední s dopadem na dostupnost	101	-47
Střední s dopadem na důvěrnost	50	-7
Střední s dopadem na integritu	98	-36
Nízká s dopadem na dostupnost	69	-36
Nízká s dopadem na důvěrnost	121	-61
Nízká s dopadem na integritu	70	-32
Suma rizik pod hranici 32:	509	+219

4.2.3.1 Zhodnocení a vyčíslení varianty B

V případě varianty B dojde k předpokládanému snížení **všech rizik** na akceptovatelnou úroveň (tedy pod hranici 32). Vyloučení prvků společností uvedených ve varování NÚKIB z veřejné zakázky navýší cenu zakázky cca o **75 000 Kč**, protože prvky těchto společností bývají zpravidla nejlevnější.

Tabulka 10: Finanční vyjádření bezpečnostního opatření varianty B

ID bezpečnostního opatření	Předpokládaná cena bezpečnostního opatření (bez DPH)
OP1	75 000 Kč
Suma:	75 000 Kč

5 Posouzení navržených variant z pohledu cena/bezpečnost

Tabulka 11: Srovnání navržených variant z pohledu bezpečnosti

	Výchozí hodnocení	Varianta A	Varianta B
Hodnoty rizik	Počet rizik	Počet rizik	Počet rizik
Kritická s dopadem na dostupnost	48	0	0
Kritická s dopadem na důvěrnost	27	0	0
Kritická s dopadem na integritu	44	0	0
Vysoká s dopadem na dostupnost	34	44	0
Vysoká s dopadem na důvěrnost	41	23	0
Vysoká s dopadem na integritu	24	34	0
Suma rizik nad hranici 32:	218	101	0
Střední s dopadem na dostupnost	54	72	101
Střední s dopadem na důvěrnost	42	58	50
Střední s dopadem na integritu	62	78	98
Nízká s dopadem na dostupnost	33	53	69
Nízká s dopadem na důvěrnost	60	89	121
Nízká s dopadem na integritu	38	56	70
Suma rizik pod hranici 32:	289	406	509

5.1 Srovnání ceny navržených variant

Tabulka 12: Srovnání navržených variant z pohledu ceny

Varianta A	Varianta B
Cena celkem (bez DPH)	Cena celkem (bez DPH)
21 520 000 Kč	75 000 Kč

6 Závěr a zvolená varianta

Na základě výše uvedených informací a posouzení variant z pohledu cena/bezpečnost pro agendový IS pro evidenci a zpracování procesu certifikace senzorů **byla zvolena jako nejvhodnější varianta B**, tedy vyloučení prvků společností uvedených ve varování NÚKIB z veřejné zakázky – **Nákup komunikačních prostředků a technického vybavení (HW) pro agendový IS pro evidenci a zpracování procesu certifikace senzorů**. Tato varianta přinese systému nejvíce bezpečnosti za nejméně peněz.

7 Související dokumentace

Příloha 1: Vzorová politika systému řízení bezpečnosti informací

Příloha 2: Vzorová metodika pro určování a hodnocení aktiv a rizik

Příloha 10: Vzorové hodnocení rizik pro veřejnou zakázku

Příloha 14: Zkratky a používané pojmy