

PŘÍLOHA 2: METODIKA PRO URČOVÁNÍ A HODNOCENÍ AKTIV A RIZIK – MINISTERSTVO PRO CERTIFIKACI SENZORŮ

Verze dokumentu			
datum	verze	změněno	provedená změna
3. 2. 2025	1.0	Manažer KB	Vytvoření dokumentu
30. 2. 2025	1.0	Výbor pro řízení KB	Schválení dokumentu
15. 3. 2026	2.0	Manažer KB	Přezkoumání Metodiky pro určování a hodnocení aktiv a rizik
10. 4. 2026	2.0	Výbor pro řízení KB	Schválení aktualizované verze dokumentu

Obsah

1	Účel.....	3
2	Stanovení odpovědností	4
3	Řízení aktiv	7
3.1	Primární aktiva	8
3.2	Podpůrná aktiva	15
4	Řízení rizik	17
4.1	Zranitelnosti a hrozby	19
4.2	Scénáře.....	35
5	Popis nástroje pro hodnocení aktiv a rizik.....	39
6	Prohlášení o aplikovatelnosti	44
6.1	Popis nástroje pro prohlášení o aplikovatelnosti	45
7	Zvládání rizik.....	46
8	Plán zvládání rizik.....	47
8.1	Popis nástroje pro plán zvládání rizik	47
9	Zpráva o hodnocení rizik.....	49
10	Řízení výjimek	50

1 Účel

Účelem této metodiky je popsat metody určování a hodnocení aktiv, výběru a ohodnocení zranitelností a hrozeb, určování a hodnocení rizik a postupy pro nakládání se zjištěnými riziky v prostředí Ministerstva pro certifikaci senzorů (dále jen „ministerstvo“).

Řízení aktiv a rizik je jedna ze základních povinností daná zákonem č. 264/2025 Sb., o kybernetické bezpečnosti (dále jen „zákon“) a vyhláškou o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností (dále jen „vyhláška“). Bez znalosti toho, jaká má organizace aktiva a jaká rizika ji ohrožují, nelze efektivně plnit většinu dalších povinností daných vyhláškou. Řízením aktiv organizace zjistí, co je pro ni důležité a co musí chránit. Řízením rizik organizace zjistí, jaká rizika ohrožují organizaci a její aktiva a jakým způsobem je potřeba aktiva chránit, tedy jaká bezpečnostní opatření je nutné zavést a dále prioritizuje zavádění těchto bezpečnostních opatření.

Jedním ze základních předpokladů zajištění bezpečnosti informací je správné nastavení procesu řízení aktiv a rizik a stanovení osob, které v tomto procesu budou mít svoji roli.

Metodika pro určování a hodnocení aktiv a rizik musí být minimálně 1× ročně přezkoumána manažerem kybernetické bezpečnosti (dále jen „KB“). I v případě, že nedojde k žádným změnám, musí být u verze uvedeno datum přezkoumání.

2 Stanovení odpovědností

V rámci ministerstva je využito dvouúrovňové stanovení garantů aktiv – gestor aktiva a garant aktiva.

Gestor aktiva je nejvýše postavený vedoucí pracovník organizačního celku, pod který dané aktivum přísluší. Gestor aktiva má příslušné pravomoci, aby mohl rozhodovat o nastavení požadavků nutných pro zajištění bezpečnosti aktiva.

Gestor aktiva stanovuje **garanta aktiva**, který má detailní znalosti daného aktiva. Garant aktiva se zpravidla zapojuje do procesu řízení aktiv a rizik, jehož výstupy schvaluje gestor aktiva.

V rámci procesu řízení aktiv a rizik jsou povinnosti stanoveny následující RACI maticí:

Tabulka 1: RACI matice

Činnosti	Výbor pro řízení KB	Odbor bezpečnostní	Manažer KB	Auditor KB	Architekt KB	Gestor PrA	Gestor PoA	Garant PrA	Garant PoA	Pověřenec pro OOÚ	Odbor ICT	Další osoby
Stanovení gestora aktiva	A, R	I	C	I	C	I	I					
Určování a evidence primárních aktiv		A	R		C	C		R				C (dodavatel, významný dodavatel, uživatel)
Určování a evidence garantů primárních aktiv		A	R			R		I				
Hodnocení primárních aktiv	I	A	R			R		R				
Určování a evidence podpůrných aktiv			A, R		C	C	R	C	R		C	
Určování a evidence vazeb mezi primárními a podpůrnými aktivy			A, R		C	R	R	R	R		C	
Určování a evidence garantů podpůrných aktiv		A	R			I	R	C	I		C	
Hodnocení podpůrných aktiv		A	R		C	I	R		R			
Vytvoření metodiky pro určování a hodnocení rizik včetně kritérií pro akceptovatelnost a výjimek		A	R									
Vytvoření katalogu hrozeb		A	R		R	R	R	R	R	C	C	C (osoby, které řeší incidenty a události)

INTERNÍ TLP:GREEN

Vytvoření katalogu zranitelností		A	R		R	R	R	R	R	C	C	C (osoby, které řeší incidenty a události)
Schválení metodiky pro určování a hodnocení rizik	A	R	I	I	I	I	I	I	I	I	I	
Určování kombinací aktiv, hrozeb a zranitelností (výstup – určená rizika)		A	R		R	R	R	R	R			
Stanovení konkrétní hodnot hrozeb a zranitelností pro aktiva		A	R		C	R	R	R	R			
Výpočet výsledné hodnoty rizika, návrh způsobu zvládání rizik a výběr bezpečnostních opatření do plánu zvládání rizik		A	R		R	R	R	R	R			
Vytvoření plánu zvládání rizik		A	R		C	C	C	C	C			
Schválení plánu zvládání rizik	A	R	I	I	I	I	I	I	I		I	
Vytvoření zprávy o hodnocení aktiv a rizik	I	A	R		I	I	I	I	I		I	
Souhlas se zbytkovými riziky	A, R											
Vytvoření prohlášení o aplikovatelnosti	I	A	R		C	C	C	C	C			
Zavádění bezpečnostních opatření		A	R		R	C	C	C	C		C	
Sledování a přezkoumávání rizik, zohlednění výstupů interního auditu a významných změn, zohlednění protiopatření podle § 20 zákona, pravidelná aktualizace celého procesu řízení aktiv a rizik	I	A	R		C	C	C	C	C	C	C	

Legenda

R – Responsible (ti, kteří práci / úkol vykonávají)

A – Accountable (ti, kteří zodpovídají za celkové splnění)

C – Consulted (ti, kteří by se k danému mohli vyjádřit a být nápomocni s jeho řešením)

I – Informed (ti, kteří mají být informováni)

3 Řízení aktiv

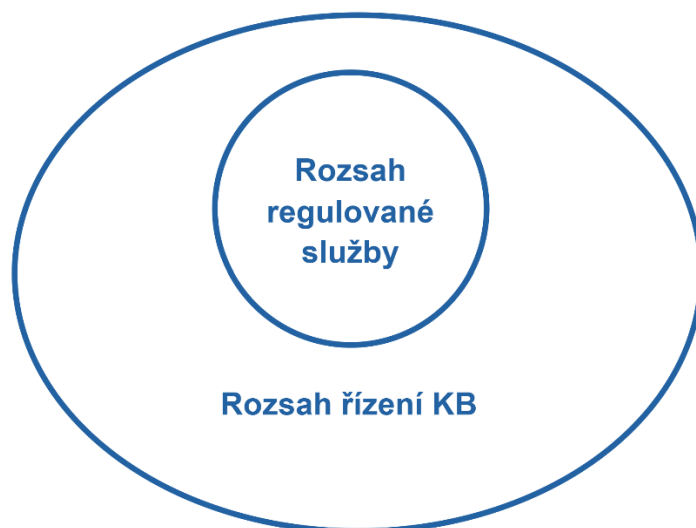
Do řízení aktiv musí být zahrnuta aktiva minimálně z rozsahu řízení KB popsáném v dokumentu *Příloha 1: Vzorová politika systému řízení bezpečnosti informací*.

Aktivum je vše, co má pro ministerstvo hodnotu. S ohledem na KB jsou rozlišována aktiva **primární** (služby a informace) a **podpůrná** (technická aktiva, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního systému, objekty, kde jsou aktiva umístěna).

Všechna aktiva musí mít evidována minimálně:

- Název aktiva
- Popis aktiva
- Gestora aktiva
- Garanta aktiva
- Hodnocení aktiva z pohledu důvěrnosti, integrity, dostupnosti a ztráty dat,
- Zařazení (určená regulovaná služba a veškerá aktiva související s poskytováním regulované služby, rozsah řízení KB, mimo rozsah řízení KB)

Na organizaci v rámci stanovení rozsahu řízení KB je třeba pohlížet jako na celek. Nejprve ministerstvo určí všechna svá primární aktiva, která zahrnují zpracovávané informace nebo poskytované služby. Poté posoudí, která primární aktiva mají přímou spojitost s poskytováním regulované služby, a u těchto aktiv následně určí i podpůrná aktiva. Do rozsahu řízení KB nemusí být zahrnuta pouze aktiva, která mají přímou vazbu na poskytování regulované služby, ale i ta ovlivňující její bezpečnost. Aktiva v rozsahu regulované služby jsou tedy podmnožinou aktiv spadajících do rozsahu řízení KB dané organizace. Primární aktiva, která byla z rozsahu řízení KB organizace vyjmuta, musí být evidována, a to včetně odůvodnění jejich vyjmutí.



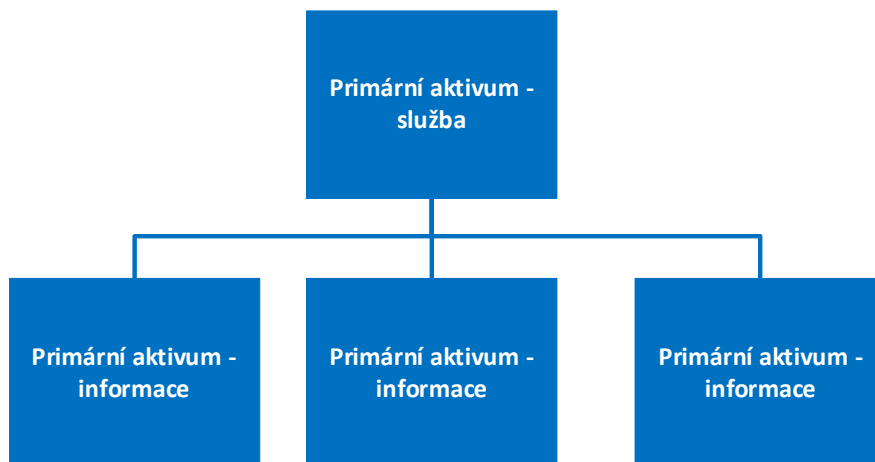
Obrázek 1: Schéma rozsahu řízení KB

Podpůrná aktiva musí mít nad rámec výše uvedeného evidovány také významné dodavatele.

Aktiva mohou být slučována do tzv. **typových aktiv**. Jsou to uměle vytvořené skupiny aktiv, které mají společné vlastnosti, a tato aktiva z určitého důvodu nechceme nebo nemůžeme dále dělit. Seskupování aktiv je nutné podložit logickou úvahou. Jednotlivá aktiva seskupená do jednoho typového aktiva si musí být svou povahou natolik podobná, aby na ně působily stejné hrozby a zranitelnosti. Dále nelze seskupovat aktiva, jejichž hodnocení z pohledu důvěrnosti, integrity, dostupnosti a ztráty se významně liší. Při seskupování podpůrných aktiv je třeba věnovat pozornost také vazbám na primární aktiva.

3.1 Primární aktiva

Za hlavní primární aktivum jsou považovány **služby**, které pracují s dalšími primárními aktivy typu **informace**. Viz následující obrázek:



Obrázek 2: Vazby mezi primárními aktivy

V případě, že není možné samostatně určit jednotlivá primární aktiva typu informace (např. v rámci využívání e-mailových služeb) je pracováno pouze s primárním aktivem typu služba a při jeho hodnocení jsou zároveň uvažovány informace, se kterými služba pracuje.

V případě, že jsou určovány primární aktiva typu informace, jsou ohodnocena z pohledu důvěrnosti, integrity, dostupnosti a ztráty dat. Služba, která s těmito informacemi pracuje, následně přebírá nejvyšší hodnoty jednotlivých atributů.

Při posuzování hodnoty aktiv je nutné uvažovat o nejhorším možném scénáři a nebrat v úvahu zavedená bezpečnostní opatření.

Musí být evidovány jak vazby mezi primárními aktivy, tak také vazby mezi primárními a podpůrnými aktivy.

Stupnice pro hodnocení primárních aktiv

Hodnocení dopadů primárních aktiv probíhá na základě následující dopadové tabulky. Oblasti uvedené v tabulce jsou součástí přílohy č. 1
Hodnocení aktiv vyhlásky:

Tabulka 2: Dopadová tabulka

Úroveň	Ochrana osobních údajů – dopady na subjekty údajů (písmeno a) vyhlásky	Ochrana osobních údajů – finanční újma subjektů údajů (písmeno a) vyhlásky)	Obchodní tajemství (písmeno a) vyhlásky)	Zákonné a smluvní povinnosti (písmeno b) vyhlásky)	Narušení vnitřních řídicích a kontrolních činností (písmeno c) vyhlásky)	Veřejný pořádek (písmeno d) vyhlásky)	Finanční ztráty (písmeno d) vyhlásky)	Zajišťování nezbytných nebo základních služeb* (písmeno e) vyhlásky)	Narušení běžných činností (písmeno f) vyhlásky)	Ztráta důvěryhodnosti (písmeno g) vyhlásky)	Bezpečnost a zdraví osob (písmeno h) vyhlásky)	Mezinárodní vztahy (písmeno i) vyhlásky)	Dopad na uživatele regulované služby (písmeno j) vyhlásky)	Trestně-právní řízení (nad rámec vyhlásky)
1 nízká	Může vést k nepohodlí subjektu osobních údajů (podrážděnost, krátkodobé časové nároky pro opětovné zadávání údajů, nutnost další komunikace s organizací).	žádné vodítko	žádné vodítko	žádné vodítko	žádné vodítko	žádné vodítko	Může přímo nebo nepřímo vést ke ztrátám menším než 0,05 % ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace)	Může způsobit drobné komplikace pro malé množství osob.	K narušení běžných činností nedochází, nanejvýše ke zvýšeným časovým nárokům při provádění běžných činností.	Může negativně ovlivnit vztahy s jinými částmi organizace, jinými organizacemi nebo vztahy s veřejností, negativní publicita bude ale omezena na bezprostřední okolí a nebude mít dlouhé trvání. Např. pro osobní údaje – nepřijemnosti s klienty, nutnost jednání s dalšími klienty, nutnost jednání s dalšími subjekty, negativní někdy i veřejná reakce subjektů údajů apod.	žádné vodítko	Může mít negativní vliv na spolupráci organizace se zahraniční společností. Např. pro osobní údaje – může vyvolat nutnost jednání mezi organizací a zahraničním partnerem o charakteristikách zpracování osobních údajů.	Může způsobit krátkodobé nepřijemnosti při používání IS regulované služby (zdržení a podráždění uživatelů, jiné zdravotní dopady na uživatele nehrozí).	žádné vodítko
2 střední	Může vést k menší újmě subjektu osobních údajů (stres, nepohodlí, drobné fyzické obtíže, nedostatek porozumění)	Odhadovaná finanční újma do 5000 Kč/subjekt údajů.	Může mít negativní dopad na skutečnosti obchodní, výrobní či technické povahy související s podnikem	Může zapříčinit porušení interních předpisů a postupů, nikoli však porušení zákonných a smluvních povinností, např.	Může mít negativní dopad na řídicí a kontrolní činnosti organizace.	Může zapříčinit rozsahem, formou nebo místem omezené protesty (lokální nepokoje).	Může přímo nebo nepřímo vést ke ztrátám mezi 0,05 % a 2 % ročního rozpočtu, popř. obratu organizace	Může způsobit omezení či narušení nezbytných nebo základních služeb pro malé množství osob, může způsobit	Může omezit provádění běžných činností, narušit řádné řízení nebo fungování části nebo celé organizace.	Může negativně ovlivnit vztahy s jinými organizacemi nebo veřejností, negativní publicita se ale bude týkat omezené zájmové skupiny nebo bude široká, avšak krátkodobá. Např. pro osobní údaje –	Může vést k újmě (ohrožení osobní bezpečnosti, svobody nebo zranění) jedné nebo několika osob.	Může vytvářet negativní obraz organizace v jednom teritoriu, popř. v jednom státě. Např. pro osobní údaje – může vést	Může negativně ovlivnit výkon činnosti interního nebo externího uživatele IS regulované služby (např. zvýšené časové nároky, stres uživatelů, drobné fyzické	Může vytvořit podmínky pro páčání trestné činnosti nebo může ztížit její vyšetřování.

		, omezení přístupu ke službám organizace nebo jiných subjektů, časové nároky spojené s řešením dopadů).		, které mají skutečno u nebo alespoň potenciální materiální či nemateriální hodnotu.	provozní důvody, nedostatek zaměstnanců.			(v závislosti na typu organizace).	krátkodobý výpadek služeb organizace. Může způsobit méně závažné finanční ztráty.		úbytek klientů o 10 % u organizace, krátkodobé omezení přístupu ke službám využívaným správcem, negativní, avšak krátkodobé ohlasy v médiích.		k dočasnému omezení zahraniční participace na zpracování osobních údajů.	a zdravotní obtíže uživatelů).	
3	vysoká	Může vést k závažné újmě subjektu osobních údajů (napadení, nepříznivý zdravotní stav, deprese, ztížené uplatnění, ekonomické znevýhodnění (černé listiny), krádež identity, předvolání vyšetřujícím i orgány).	Odhadovaná finanční újma od 5000 Kč do 50 000 Kč/subjekt údajů (zneužití finančních prostředků subjektu údajů, poškození majetku).	Může mít podstatný dopad na skutečností obchodní, výrobní či technické povahy související s podnikem, které mají skutečno u nebo alespoň potenciální materiální či nemateriální hodnotu.	Může zapříčinit správní nebo občanskoprávní řízení vedoucí k pokutě nebo k náhradě škody.	Může mít podstatný dopad na řídicí a kontrolní činnosti organizace a zapříčinit dočasné zastavení chodu či podstatný zásah do fungování organizace , značné finanční ztráty související s obnovením chodu.	Může zapříčinit rozsahem, formou nebo místem omezené protesty na úrovni významné části správního území obce s rozšířenou působností , jejichž řešení si může vyžádat aktivaci krizového řízení na úrovni kraje.	Může přímo nebo nepřímo vést ke ztrátám vyšším než 2 % a nižším či rovným 10 % ročního rozpočtu , popř. obratu organizace (v závislosti na typu organizace).	Může způsobit závažné omezení či narušení nezbytných nebo základních služeb pro větší množství osob, omezení nebo krátkodobé zastavení přístupu ke službám.	Může způsobit dočasné zastavení nebo podstatné narušení běžných činností organizace nebo poškodit rozvoj nebo prosazování cílů a zájmů organizace.	Může závažně ovlivnit vztahy s jinými organizacemi nebo veřejností s následkem celostátní negativní publicity . Např. pro osobní údaje – úbytek klientů 10-50 % u organizace, masivní negativní, avšak krátkodobé ohlasy v médiích.	Může vést k újmě (ohrožení osobní bezpečnosti, svobody nebo zranění) větší skupiny osob, nebo ohrožení na životě jednotlivců .	Může vytvářet negativní obraz organizace ve světě . Např. pro osobní údaje – může být spojené s trvalým nebo dlouhodobým omezením participace zahraničních partnerů na zpracování osobních údajů.	Může způsobit závažné krátkodobé omezení výkonu činnosti interního nebo externího uživatele IS regulované služby (zhoršení zdravotního stavu uživatelů, krátkodobá pracovní neschopnost).	Může vést k narušení vyšetřování trestné činnosti nebo soudního řízení (méně závažná kriminalita, v jednotlivých případech).
4	kritická	Může vést k velmi vážné újmě subjektu osobních údajů, přímému ohrožení či ztrátě života (smrt, invalidita, dlouhodobě nepříznivý zdravotní stav a pracovní	Odhadovaná finanční újma od 50 000 Kč/subjekt údajů (neschopnost splácet dluh, ztráta majetku).	Může mít závažný dopad na skutečností obchodní, výrobní či technické povahy související s podnikem, které mají skutečno u nebo alespoň	Může zapříčinit porušení právních předpisů vedoucí k zahájení trestního stíhání.	Může mít závažný dopad na řídicí a kontrolní činnosti a zapříčinit dlouhodobé zastavení chodu celé organizace.	Může zapříčinit hromadné nepokoje , např. generální stávku, nebo jinak závažně narušit veřejný pořádek s celostátními dopady .	Může přímo nebo nepřímo vést ke ztrátám přesahujícím 10 % ročního rozpočtu , popř. obratu organizace (v závislosti na typu organizace).	Může způsobit rozsáhlé dlouhodobé omezení, narušení či nedostupnost poskytování nezbytných nebo základních služeb pro větší množství osob, může způsobit	Může způsobit dlouhodobé zastavení běžných činností organizace.	Může závažně a dlouhodobě ovlivnit vztahy s jinými organizacemi nebo veřejností s následkem celostátní či nadnárodní negativní publicity, s dlouhodobými účinky a požadavky přijetí politické odpovědnosti. Např. pro osobní	Může vést k přímému ohrožení či ztrátě života osob.	Může negativně ovlivnit nebo poškodit diplomatické vztahy a tím způsobit nevýhodu pro zájmy ČR. Např. pro osobní údaje – dlouhodobé nebo trvalé omezení participace zahraničních subjektů	Může způsobit závažné dlouhodobé omezení výkonu činnosti interního nebo externího uživatele IS regulované služby (útoky na uživatele, odchod zaměstnanců, dlouhodobá pracovní neschopnost	Může vést k závažnému, dlouhodobému narušení schopnosti vyšetřovat trestnou činnost , popřípadě zpochybnění soudního řízení a rozhodnutí (závažná kriminalita, celkové

		neschopnost, ztráta zaměstnání, velmi ztížené uplatnění, vyloučení, omezení práv).		potenciální materiální či nemateriální hodnotu.				újm (např. soudní proces, likvidace, vznik nesplátného dluhu).		údaje – úbytek klientů nad 50 % u organizace, černé listiny, ztráta konkurenceschopnosti, masivní negativní dlouhodobé ohlasy v médiích včetně zahraničních.		nebo i států na zpracování osobních údajů.	uživatelů, úmrtí).	zpochybnění systému).
Popis kategorie	V této kategorii je posuzováno, jaký dopad bude mít narušení primárních aktiv přímo na subjekty údajů, tedy na jednotlivé osoby, jejichž údaje jsou v daném IS zpracovávány. Jak moc budou jednotlivé osoby po fyzické nebo psychické stránce dotčeny, když budou narušeny jejich osobní údaje.	V této kategorii je posuzováno, jaký dopad bude mít narušení primárních aktiv přímo na subjekty údajů, tedy na jednotlivé osoby, jejichž údaje jsou v daném IS zpracovávány. Jaká finanční újma vznikne jednotlivým osobám, když budou narušeny jejich osobní údaje.	V této kategorii je posuzováno, jaký dopad bude mít narušení primárních aktiv na ochranu obchodního tajemství organizace.	V této kategorii je posuzováno, jaký dopad bude mít narušení primárních aktiv na plnění zákonných a smluvních povinností, kterými je organizace zavázána.	V této kategorii je posuzováno, jaký dopad bude mít narušení primárních aktiv na vnitřní řídicí a kontrolní činnosti organizace (kontrolní mechanismy organizace, její vedení, správu apod.).	V této kategorii je posuzováno, jaký dopad bude mít narušení primárních aktiv na zajištění veřejného pořádku.	V této kategorii je posuzováno, jaký dopad bude mít narušení primárních aktiv na zajišťování bezpečnosti organizace (schopnost komunikovat v rámci organizace a mimo ni, přijímat zaměstnance apod.).	V této kategorii je posuzováno, jaký dopad bude mít narušení primárních aktiv na zajišťování běžných činností organizace (schopnost komunikovat v rámci organizace a mimo ni, přijímat zaměstnance apod.).	V této kategorii je posuzováno, jaký dopad bude mít narušení primárních aktiv na zajišťování bezpečnosti organizace (schopnost komunikovat v rámci organizace a mimo ni, přijímat zaměstnance apod.).	V této kategorii je posuzováno, jaký dopad bude mít narušení primárních aktiv na zajišťování bezpečnosti organizace (schopnost komunikovat v rámci organizace a mimo ni, přijímat zaměstnance apod.).	V této kategorii je posuzováno, jaký dopad bude mít narušení primárních aktiv na zajišťování bezpečnosti organizace (schopnost komunikovat v rámci organizace a mimo ni, přijímat zaměstnance apod.).	V této kategorii je posuzováno, jaký dopad bude mít narušení primárních aktiv na zajišťování bezpečnosti organizace (schopnost komunikovat v rámci organizace a mimo ni, přijímat zaměstnance apod.).	V této kategorii je posuzováno, jaký dopad bude mít narušení primárních aktiv na zajišťování bezpečnosti organizace (schopnost komunikovat v rámci organizace a mimo ni, přijímat zaměstnance apod.).	V této kategorii je posuzováno, jaký dopad bude mít narušení primárních aktiv na zajišťování bezpečnosti organizace (schopnost komunikovat v rámci organizace a mimo ni, přijímat zaměstnance apod.).
Příklady	Únik osobních údajů fyzické osoby z IS (např. o zdravotním stavu apod.) a jejich	Neoprávněná modifikace osobních údajů fyzické osoby v IS způsobí výplatu sociálních	Odcizení patentů evidovaných v IS konkurenční firmou.	Nemožnost vydání rozhodnutí v zákonné lhůtě z důvodu nedostupnosti IS. Narušení povinnosti	Neúplnost či modifikace informací potřebných pro rozhodování vedení a	Nedostupnost informací zveřejňovaných na webu organizace může vést k neinformování veřejnosti o důležitých	Nedostupnost informací o fakturách na základě nedostupnosti ekonomického systému.	Narušení všech informací, procesů a služeb vztahených směrem k hlavnímu business cíli (účelu	Narušení činností personálních, ekonomických, správy budov a autoparku, neschopnost přijímat	Vlivem úniku citlivých informací organizace na internet bude narušena její reputace.	V důsledku nedostupnosti informací evidovaných v nemocničním IS není možné provést	Únik informací, které organizace získala od zahraničních partnerů.	Ztráta možnosti přístupu uživatelů ke službě vlivem její nedostupnosti (např. při výpadku internetového bankovníctví se	Z důvodu úniku informací v policejním IS v rámci trestního řízení bude zastaveno trestní řízení.

	následné zveřejnění na internetu.	dávek jiné fyzické osobě.		zveřejňovat dokumenty na elektronické úřední desce, která je nepřetržitě dostupná vzdáleným přístupem.	kontrolní činnost.	skutečnostech (záplavy, ekologické katastrofy atd.). Dlouhodobá nedostupnost informací potřebných pro výplatu sociálních dávek, důchodů apod.	Nedostupnost informací o možných obchodních příležitostech a z toho plynoucí ušlý zisk.	existence) organizace (např. v případě Ministerstva pro certifikaci senzorů by se jednalo o narušení vydávání certifikací).	datové zprávy apod. Neschopnost přijímat nové zaměstnance z důvodu nedostupnosti personálních o systému.		nezbytné operace a pacienti jsou ohroženi na životě.		tento problém dotkne velkého počtu uživatelů – nemožnost zadat platební příkaz online).	
--	-----------------------------------	---------------------------	--	--	--------------------	---	---	---	--	--	--	--	---	--

Hodnocení primárních aktiv probíhá pouze u těch oblastí, které jsou pro dané aktivum relevantní.

Hodnocení primárních aktiv z hlediska dostupnosti, ztráty, důvěrnosti a integrity je prováděno v souladu s následující stupnicí:

Tabulka 3: Stupnice pro hodnocení primárních aktiv z hlediska dostupnosti, ztráty, důvěrnosti a integrity

		Dostupnost												Ztráta							Důvěrnost			Integrita				
Výsledná hodnota		Dostupnost	Provozní doba pod SLA	Přípustná doba kumulovaných výpadků s měsíčním vyhodnocováním	Nedostupnost 15 min	Nedostupnost 1h	Nedostupnost 4 h	Nedostupnost 8 h	Nedostupnost 1den	Nedostupnost 2 dny	Nedostupnost 1 týden	Nedostupnost 14 dní	Nedostupnost měsíc a více	Ztráta dat od zálohy (15 min)	Ztráta dat od zálohy (1 h)	Ztráta dat od zálohy (4 h)	Ztráta dat od zálohy (8 h)	Ztráta dat od zálohy (1 den)	Ztráta dat od zálohy (2 dny)	Ztráta dat od zálohy (1 týden)	Ztráta dat od zálohy (14 dní)	Úplná ztráta dat	Prozrazení v rámci organizace	Prozrazení smluvním partnerům	Prozrazení vně organizaci	Modifikace dat malého rozsahu	Modifikace dat velkého rozsahu	
0	Nerelevantní																											
1	nízká	96,16 %	Provozní doba pod SLA: minimálně určených 10 hodin v pracovní dny. Nezapočítávají se dny pracovního volna a dny pracovního klidu stanovené pro ČR. Např. r. 2018 má 250 pracovních dní, na bázi 10 hod. pod SLA denně, což dává max. měsíční výpadek 8,3 hod. při dostupnosti 96 % (vztaženo na dobu pod SLA).	Max. 8 hod., avšak pouze v rámci definované pracovní doby	1	1	1	1	1	1	2	2	2	nejvyšší hodnota							nejvyšší hodnota			nejvyšší hodnota				
2	střední	99,45 %	Provozní doba pod SLA: 24x7 (připravenost pro služby související s úplným el. podáním). Avšak určité služby, u nichž to lze předpokládat vzhledem k provozním aspektům, lze nabízet s omezením Provozní doby pod SLA na pracovní dny a vymezenou pracovní dobu. To znamená, že el. podání bude obvykle fungovat nepřetržitě, ale	Max. 4 hod. na bázi 24x7	1	1	1	2	2	3	3	3	3															

			reakce poskytovatele na nahlášené incidenty je omezena.													
3	vysoká	99,90 %	Provozní doba pod SLA: 24x7 (připravenost pro služby úplného el. podání). Určité služby, u nichž to lze předpokládat vzhledem k provozním aspektům, lze nabízet s omezením Provozní doby pod SLA na pracovní dny a vymezenou pracovní dobu.	Max. 43 min. na bázi 24x7	1	1	3	3	3	3	4	4	4	nejvyšší hodnota	nejvyšší hodnota	nejvyšší hodnota
4	kritická	99,99 %	Plně fault-tolerantní systém s georedundancí a replikací transakčních dat. Smluvní penále při výpadku dostupnosti služby delší než celkem 52 minut za rok (odpovídá 99,99 %).	Jednotlivý výpadek max. 15 min. Max. kumulovaný roční výpadek 52 min. (odpovídá 99,99 %)	1-2	3-4										

Způsob získání výsledné hodnoty dostupnosti na základě výše uvedené tabulky

Výše uvedená tabulka je pouze orientační. Hodnoty nedostupnosti pro jednotlivé časové řezy u hodnoceného aktiva se nemusí přesně rovnat hodnotám uvedeným v této tabulce. Pro určení výsledné hodnoty dostupnosti je potřeba porovnat všechny údaje v tabulce uvedené výše a vybrat úroveň dostupnosti, která nejvíce odpovídá reálným potřebám při práci s aktivem.

3.2 Podpůrná aktiva

Jedná se o aktiva nutná pro správnou funkčnost, zpracování, uchování a zajištění bezpečnosti primárních aktiv. Sama o sobě podpůrná aktiva netvoří hodnotu pro organizaci.

Vazby mezi primárními a podpůrnými aktivy musí být evidovány.

Podpůrná aktiva jsou členěna do následujících kategorií:

Technické vybavení (HW)

Do technického vybavení (HW) spadají fyzické komponenty (zpravidla si na ně můžeme sáhnout) IS nebo jejich části. Typickými příklady technického vybavení jsou pracovní stanice (včetně periferií), datová úložiště, servery, ale také mobilní zařízení. Do této kategorie též spadají výměnná média (včetně CD, DVD apod.).

Komunikační prostředky

Do komunikačních prostředků spadají komponenty, které spojují jednotlivá technická vybavení dohromady a vytváří z nich síť. Do této kategorie jsou zahrnuta jak drátová (ethernet, optické vlákno apod.), tak i bezdrátová (Wi-Fi apod.) připojení a veškeré komponenty, které jsou potřebné pro realizaci těchto připojení – tedy mimo aktivních prvků, např. síťová zařízení jako jsou směrovače (router), přepínače (switch) apod.

Programové vybavení (SW)

Do programového vybavení (SW) spadají veškeré programy / aplikace, které běží na technickém vybavení a komunikačních prostředcích. Bez nich by technické vybavení a komunikační prostředky byly pouze kusem železa bez využití. Programové vybavení zajišťuje, že je možné technické vybavení a komunikační prostředky ovládat a vykonávat na nich požadované úkony. Do této kategorie jsou zahrnuty např. OS, firmware, kancelářské balíky, ale i přístupové a bezpečnostní aplikace.

Objekty

Do objektů spadají fyzické prostory, ve kterých se IS regulované služby nebo jeho části nachází. Do této kategorie spadají areály, objekty, inženýrské sítě apod.

Lidské zdroje

Do lidských zdrojů spadá veškerý personál, který má vliv na regulovanou službu nebo její části. Do této kategorie jsou zahrnuti např. uživatelé, administrátoři, vývojáři, bezpečnostní role, ale také vedení organizace nebo administrátoři dodavatele.

Dodavatelé

Do kategorie dodavatelů spadají např. významní dodavatelé, subdodavatelé, výrobci nebo poskytovatel cloud computingu.

Externí systémy a služby

Do externích systémů a služeb spadají veškeré externí systémy a služby, které jsou nezbytné pro zajištění funkčnosti regulované služby nebo jejích částí. Do této kategorie jsou zahrnuty např. dodávky elektřiny, certifikační služby.

Podpůrná aktiva mohou být velmi komplexní a spadat do více z těchto kategorií, pro potřeby navazujících činností, např. hodnocení aktiv a rizik, je možné vytvořit jedno typové aktivum, které bude obsahovat více kategorií. V navazujícím hodnocení rizik je ale **nutné určit relevantní hrozby a zranitelnosti pro všechny kategorie** příslušného typového aktiva.

Jako pomůcka pro určování podpůrných aktiv slouží dokument *Příloha 4: Struktura podpůrných aktiv*.

Hodnocení podpůrných aktiv probíhá na základě vzorce, který pracuje s váhou vlivu podpůrného aktiva na primární aktivum a hodnotou příslušného primárního aktiva. V případě potřeby může manažer KB ve spolupráci s příslušným gestorem provést individuální přehodnocení aktiva.

Váha vlivu je číselně ohodnocena síla vazby mezi primárním a podpůrným aktivem, přičemž váha vlivu je posuzována individuálně pro jednotlivé atributy bezpečnosti informací (důvěrnost, integrita, dostupnost, ztráta) a individuálně pro každou dvojici primárního a podpůrného aktiva.

Váha vlivu nabývá hodnot podle následující tabulky:

Tabulka 4: Váha vlivu

Úroveň		Popis
1	Nízká	Hodnocený atribut bezpečnosti informací nemá vliv na stejný atribut daného primárního aktiva.
2	Střední	Hodnocený atribut bezpečnosti informací má vedlejší vliv na stejný atribut daného primárního aktiva.
3	Vysoká	Hodnocený atribut bezpečnosti informací má hlavní vliv na stejný atribut daného primárního aktiva, může způsobit významnou škodu.
4	Kritická	Hodnocený atribut bezpečnosti informací má kritický vliv na stejný atribut daného primárního aktiva, může způsobit jeho znehodnocení.

Hodnota podpůrného aktiva = váha vlivu × hodnota primárního aktiva

Vzhledem k tomu, že podpůrné aktivum může mít více vazeb na primární aktiva, je pro účely hodnocení podpůrných aktiv vybrána nejvyšší hodnota dle jednotlivých atributů bezpečnosti informací.

Dopad podpůrného aktiva je hodnota v intervalu <1;16>, musí tedy dojít k úpravě výsledné hodnoty podpůrného aktiva na čtyřstupňovou škálu použitou pro primární aktiva. Tato úprava je dána následující tabulkou:

Tabulka 5: Hodnota podpůrného aktiva

Hodnota podpůrného aktiva = váha vlivu × hodnota primárního aktiva		Hodnota primárního aktiva			
		1	2	3	4
Váha vlivu podpůrného aktiva na primární aktivum	1	1	2	3	4
	2	2	4	6	8
	3	3	6	9	12
	4	4	8	12	16

Výsledná hodnota podpůrného aktiva	
1-4	1
5-8	2
9-12	3
13-16	4

4 Řízení rizik

Do řízení rizik musí být zahrnuta všechna aktiva z určeného rozsahu řízení KB popsaném v dokumentu *Příloha 1: Vzorová politika systému řízení bezpečnosti informací*.

Rizika jsou určena na základě relevantních kombinací aktivum-zranitelnost-hrozba.

Pro hodnocení rizik je využit výpočet pomocí funkce, kterou ovlivňuje dopad, hrozba a zranitelnost. Dopadem se myslí hodnota aktiva příslušného atributu (důvěrnost, integrita, dostupnost).

Riziko = dopad (hodnota příslušného atributu aktiva) × hrozba × zranitelnost

Hodnocení rizik se řídí následující tabulkou:

Tabulka 6: Stupnice pro hodnocení rizik a kritéria pro akceptovatelnost

STUPNICE PRO HODNOCENÍ RIZIK			PROCES ZVLÁDÁNÍ RIZIKA
1-16	Nízká	Riziko je považováno za přijatelné – akceptovatelné.	Riziko akceptuje manažer KB ve spolupráci s gestorem aktiva. Dále riziko monitorují. V případě zájmu se výbor pro řízení KB může o těchto rizicích informovat.
17-31	Střední	Riziko může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti opatření je riziko akceptovatelné.	V případě řešení rizika akceptací, činí tak manažer KB ve spolupráci s gestorem aktiva. V případě řešení snížením rizika architekt KB ve spolupráci s manažerem KB navrhuje bezpečnostní opatření. Navržený způsob zvládání rizik včetně bezpečnostního opatření prezentuje manažer KB výboru pro řízení KB, který jej buď schválí, nebo rozhodne o jiném způsobu zvládání.
32-47	Vysoká	Riziko je dlouhodobě nepřijatelné a musí být zahájeny systematické kroky k jeho odstranění.	Způsob zvládání rizika navrhuje manažer KB ve spolupráci s gestorem aktiva. V případě řešení snížením rizika architekt KB ve spolupráci s manažerem KB navrhuje bezpečnostní opatření. Navržený způsob zvládání rizik včetně bezpečnostního opatření prezentuje manažer KB výboru pro řízení KB, který jej buď schválí, nebo rozhodne o jiném způsobu zvládání.
48-64	Kritická	Riziko je nepřijatelné a musí být neprodleně zahájeny kroky k jeho odstranění.	Způsob zvládání rizika navrhuje manažer KB ve spolupráci s gestorem aktiva. V případě řešení snížením rizika architekt KB ve spolupráci s manažerem KB navrhuje bezpečnostní opatření. Navržený způsob zvládání rizik včetně bezpečnostního opatření prezentuje manažer KB výboru pro řízení KB, který jej buď schválí, nebo rozhodne o jiném způsobu zvládání. V případě naléhavosti zvládnutí rizika lze postupovat způsobem popsaným v metodice.

Tabulka 7: Rozložení úrovně rizika

		Hrozba × zranitelnost								
		1	2	3	4	6	8	9	12	16
Hodnota dopadu aktiva	1	1	2	3	4	6	8	9	12	16
	2	2	4	6	8	12	16	18	24	32
	3	3	6	9	12	18	24	27	36	48
	4	4	8	12	16	24	32	36	48	64

Hodnocení rizik musí být provedeno:

- Nejméně jednou ročně
- Při významné změně
- Při změně rozsahu řízení KB
- V případě potřeby v souvislosti s vydáním protiopatření dle § 20 zákona

Hodnocení rizik musí dále zohledňovat:

- Relevantní hrozby a zranitelnosti s ohledem na aktiva a posoudit jejich možné dopady na aktiva
- Významné změny
- Změny stanoveného rozsahu podle § 12 zákona
- Kybernetické bezpečnostní incidenty, včetně dříve řešených
- Výsledky auditů a kontrol v oblasti KB
- Výsledky penetračního testování a skenování zranitelností
- Výsledky vyhodnocení účinnosti ISMS

Hodnocení rizik prováděno u významných dodavatelů v rámci výběrového řízení před uzavřením smlouvy související s plněním předmětu výběrového řízení se řídí touto metodikou přiměřeně.

4.1 Zranitelnosti a hrozby

Katalog hrozeb a katalog zranitelností vychází z kategorií popsanych v příloze č. 3 vyhlášky.

Zranitelnosti jsou doplněny o kategorii aktiv, u kterých se mohou vyskytovat.

Tabulka 8: Katalog zranitelností

ID	Typové zranitelnosti	Označení	Příklady zranitelností	Technické vybavení (HW)	Programové vybavení (SW)	Komunikační prostředky	Objekty	Lidské zdroje	Dodavatelé	Externí systémy a služby
1	Nedostatečná údržba aktiv	Z1: Nedostatečná údržba aktiv	1) Proces pro správu a řízení technických zranitelností není zdokumentován ani plně zaveden do praxe. Není používán nástroj pro řízení technických zranitelností. Není nasazena technologie pro skenování zranitelností. 2) Stává se, že seznam ICT komponent nově zaváděné techniky není kompletní, v organizaci se vyskytuje neevidovaný ICT HW. V případě krádeže je HW administrativně nedohledatelný. 3) Nedostatečná dokumentace interní sítě. 4) Pro testování jsou používána produkční data. 5) Nejsou stanoveny priority obnovy informačních systémů ze zálohy. 6) Neprobíhá profylaxe a údržba. 7) Jsou vydávány aktualizace dodavatelem/výrobcem, ale nejsou aplikovány do provozního prostředí.	x	x	x	x			

			8) Neprobíhá pravidelné čištění skladových prostor, hromadí se hořlavý materiál. 9) Servery jsou zanášeny prachem a nejsou pravidelně čištěny. 10) Informace popsané v dokumentaci nejsou pravidelně aktualizovány. 11) Aktualizace nejsou dostatečně testovány před nasazením do provozního prostředí. 12) Nejsou odstraňovány nedostatky zjištěné v průběhu skenování zranitelností nebo penetračního testování.							
2	Zastaralost aktiv	Z2: Zastaralost aktiv	1) Jsou provozovány zastaralé nebo nepodporované operační systémy. 2) Nejsou vydávány aktualizace. 3) Jsou používány zastaralé aktivní prvky. 4) Zastaralá serverovna nesplňující aktuální předpisy a normy. 5) Jsou používány zastaralé kryptografické algoritmy. 6) Nemá prováděno pravidelné přezkoumání používaných kryptografických algoritmů.	x	x	x	x			
3	Nedostatečná ochrana perimetru	Z3: Nedostatečná ochrana perimetru	1) Nemá implementovanou ochranu proti Web application útokům na externí služby. 2) Nemá aplikován hardening serverů, zejména těch vystavených do internetu. 3) Externí FW není zapojen v clusteru. 4) Nedostatečné fyzické zabezpečení objektů a lokalit.	x	x	x	x			

			5) Routery mají nastaveno defaultní jméno a heslo pro přístup do administrátorského rozhraní. 6) Vstup do objektu je umožněn komukoliv bez prověření jeho totožnosti, účelu návštěvy atd. 7) Absence ostrahy/dozoru u vstupu atd.							
4	Nedostatečné bezpečnostní povědomí uživatelů, administrátorů, osob zastávající bezpečnostní role, dodavatelů a vrcholového vedení	Z4: Nedostatečné bezpečnostní povědomí uživatelů, administrátorů, osob zastávající bezpečnostní role, dodavatelů a vrcholového vedení	1) Nedostatečné vzdělávání běžných uživatelů ICT v oblasti bezpečnosti informací. 2) Nedostatečné ověřování znalostí běžných uživatelů ICT v oblasti bezpečnosti informací. Není prováděno testování formou phishingových kampaní a dalších metod sociálního inženýrství. 3) Absence vzdělávacích programů pro administrátory a bezpečnostní techniky. 4) Dodavatelé nejsou poučeni o svých právech a povinnostech. 5) Bezpečnostní role pravidelně neabsolvují odborná školení. 6) Zaměstnanci nejsou proškoleni o tom, že nesmí do objektu pouštět neautorizované osoby (např. není ověřena identita pracovníka dodavatele a účel jeho návštěvy). 7) Zaměstnanci nejsou poučeni o pravidlech ochrany aktiv (např. klasifikace informací, pravidla pro sdílení informací atd.). 8) Zaměstnanci nejsou poučeni o způsobech zacházení se zaměstnaneckou kartou (např. nenechávat kartu volně ležet					x	x	x

			bez dozoru). 9) Zaměstnanci nejsou školeni o způsobech odhalování pochybení, nevhodných nebo závadných způsobů chování.							
5	Nedostatečné zálohování	Z5: Nedostatečné zálohování	1) Nepravidelné zálohování. 2) Nedostatečná ochrana záloh. 3) Nedostatečné testování obnovy záloh. 4) Zálohy jsou uloženy na stejném fyzickém nebo virtuálním místě, jako originální data.	x	x		x	x	x	x
6	Nevhodné nastavení přístupových oprávnění	Z6: Nevhodné nastavení přístupových oprávnění	1) Některá ICT zařízení nemají od výrobce přístup chráněný heslem (defaultně). 2) Není nastavena jednotná politika hesel jak v rámci domény, tak na jednotlivých IS. 3) Neprobíhá pravidelné přezkouvání přístupových práv jak uživatelů, tak administrátorů. 4) Při přihlašování do IS neprobíhá autentizace uživatelů přes centrální správu uživatelů (AD). IS mají svou vlastní DB uživatelů. 5) Není implementován centrální systém řízení identit (IDM). 6) Nedostatečně fyzicky zabezpečené vstupy do serverovny. 7) Absence rozdělení odpovědných rolí a jim přidružených oprávnění – všichni mají přístup všude (porušená či ignorovaná zásada "need to know"). 8) Není aplikována metoda	x	x	x	x	x	x	x

			minimálních oprávnění (least privilege principle).							
7	Nedostatečné postupy a procesy pro detekování kybernetických bezpečnostních událostí a identifikování kybernetických bezpečnostních incidentů	Z7: Nedostatečné postupy a procesy pro detekování kybernetických bezpečnostních událostí a identifikování kybernetických bezpečnostních incidentů	1) Nedostatečné školení zaměstnanců. 2) Chybějící nebo neaktuální bezpečnostní politiky v rámci řízení KBI a KBU. 3) Nejednoznačné stanovení pravomocí a odpovědností.		x	x		x	x	
8	Nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit činnost, která může mít vliv na bezpečnost regulované služby	Z8: Nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit činnost, která může mít vliv na bezpečnost regulované služby	1) Neexistuje dohled nad aktivitami privilegovaných (administrátorských) účtů. 2) Nejednotná úroveň logování uživatelských aktivit u jednotlivých informačních systémů, není prováděno pravidelné vyhodnocování logů. 3) Nejsou vyhodnocovány informace ze síťových sond. 4) Záznamy z kamerového systému nejsou ukládány. 5) Vedoucí pracovník nekontroluje dodržování nastavených pravidel podřízenými. 6) Záznamy z kamerového systému neexistují či nejsou ukládány.	x	x	x		x	x	x
9	Nedostatečné stanovení bezpečnostních pravidel a postupů, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů, osob zastávající bezpečnostní role,	Z9: Nedostatečné stanovení bezpečnostních pravidel a postupů, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů, osob zastávající bezpečnostní role,	1) Bezpečnostní politiky nejsou vytvořeny v dostatečném rozsahu. 2) Neexistuje incident management dokumentace. 3) Není dokumentovaná odpovědnost a role za řízení bezpečnosti informací. 4) Nedochází k systematickému a jednotnému řízení aktiv a rizik. 5) Manažer KB není součástí	x	x	x	x	x		

dodavatelů a vrcholového vedení	dodavatelů a vrcholového vedení	všech akvizičních procesů ICT. Manažer KB se nevyjadřuje k bezpečnostním požadavkům na nové technologie nebo při obměně stávajících technologií. 6) Nedostatečné řízení dodavatelů, ve smlouvách nejsou stanoveny požadavky na bezpečnost, ve smlouvách absentují informace a požadavky na připojení do sítí (topologie infrastruktury, datové rozvaděče, způsob zapojení apod.). 7) Nejsou nastavena pravidla pro změny defaultních hesel na zařízeních. 8) Neexistují pravidla pro vzdálenou práci a pro BYOD. 9) Nejsou nastavena bezpečnostní pravidla, která musí být zohledněna při zpracování veřejných zakázek. 10) Nejsou nastaveny závazné postupy při identifikaci negativních bezpečnostních jevů, KBU, KBI od formy jejich hlášení, postupů řešení, seznamu zainteresovaných řešitelů a vyhodnocení těchto jevů a následného přezkoumání. 11) Staré smlouvy nezahrnují požadavky na bezpečnost nebo jen částečně. 12) Neexistuje bezpečnostní provozní příručka k IS. 13) Není nastavena forma hlášení a řešení bezpečnostních událostí a incidentů ke správci IS od dodavatele.							
------------------------------------	------------------------------------	--	--	--	--	--	--	--	--

10	Nedostatečná ochrana aktiv	Z10: Nedostatečná ochrana aktiv	1) Nejsou stanoveni garanti aktiv, nedošlo k jejich jmenování a neznají své povinnosti. 2) Není zavedena klasifikace aktiv (informací). 3) Není zdokumentován ani zaveden proces pro správu a likvidaci výměnných médií. Není vedena jejich evidence. 4) Není zaveden standard pro šifrování e-mailové komunikace (externí i interní). 5) Média (např. s interní dokumentací) nejsou při vložení do technických aktiv organizace nijak omezována ani skenována antivirovým řešením. 6) Nedostatečně technicky zajištěna ochrana citlivých informací. Není nasazeno DLP řešení. 7) Organizační opatření nejsou zavedena do praxe. Procesy jsou nastaveny pouze formálně v dokumentaci. 8) Nedostatečná konfigurace ICT aktiv (servery, komunikační prvky, databáze apod.). 9) Nedostatečně zdokumentovaná kabeláž. 10) Nedostatečná ochrana koncových zařízení (endpoint security), vč. antiviru. 11) Slabá ochrana před vnějšími vlivy. 12) Minimální ochrana před útoky zvenčí – organizovanou skupinou, osamocenými hackery atd.	x	x	x	x	x	x	x
----	----------------------------	---------------------------------	--	---	---	---	---	---	---	---

11	Nevhodně navržená bezpečná architektura	Z11: Nevhodně navržená bezpečná architektura	1) Nižší úroveň vysoké dostupnosti z důvodu přepínání celých větví a nejen zařízení, které vypadne. 2) Uživatelský segment není od DMZ oddělen pomocí interního FW. 3) VLAN jsou zakončeny na core switchi, což ztěžuje management prostupů mezi VLAN. 4) Na serverech není instalován FW. 5) Není používáno nastavení DNSSEC. 6) DMZ je provozována na stejných fyzických serverech jako interní servery. Je oddělena pouze síťově na úrovni pomocí VLAN. 7) Nedostatečná segmentace sítě. 8) Nejsou definovány ACL.	x	x	x				
12	Nedostatečná míra nezávislé kontroly	Z12: Nedostatečná míra nezávislé kontroly	1) Neprobíhá pravidelný interní audit. 2) Neprobíhá pravidelný externí audit. 3) Neprobíhá penetrační testování. 4) Neprobíhá skenování zranitelností. 5) Neadekvátní kontrola změn. 6) Neprobíhají zákaznické audity u dodavatele.	x	x	x	x	x	x	x
13	Neschopnost včasného odhalení pochybení ze strany uživatelů, administrátorů, osob zastávajících bezpečnostní role,	Z13: Neschopnost včasného odhalení pochybení ze strany uživatelů, administrátorů, osob zastávajících bezpečnostní role,	1) Nedostatečné školení, uživatelů, administrátorů, bezpečnostních rolí, dodavatelů a vrcholného vedení. 2) Nedostatečná kontrola dodavatelů.	x	x	x	x	x	x	x

	dodavatelů a vrcholného vedení	dodavatelů a vrcholového vedení	3) Špatné nastavení pravidel a politik technických aktiv. 4) Absence programového vybavení pro detekci.							
14	Nedostatek zaměstnanců s potřebnou odbornou úrovní znalostí	Z14: Nedostatek zaměstnanců s potřebnou odbornou úrovní znalostí	1) Nedostatek kvalifikovaných zájemců o práci v informačních a komunikačních technologiích. 2) Nedostatek zaměstnanců způsobený hromadnou nemocí, karanténou.					x	x	x
15	Umístění aktiva mimo fyzickou kontrolu (například na území cizího státu)	Z15: Umístění aktiva mimo fyzickou kontrolu (například na území cizího státu)	1) Nedostatečná fyzická bezpečnost. 2) Umístění v cizím státě může podléhat jiným právním a regulačním požadavkům. 3) Nedostatečné monitorování technických aktiv. 4) Nedostatečná kontrola přístupu k aktivům. 5) Vzdálenost aktiva mimo fyzickou kontrolu.	x	x	x	x	x	x	x
16	Umístění aktiva na území státu, o jehož právním prostředí nemá povinná osoba dostatečné povědomí	Z16: Umístění aktiva na území státu, o jehož právním prostředí nemá povinná osoba dostatečné povědomí	1) Neoprávněný přístup k citlivým informacím nebo jejich zneužití v zemi s nejasnými zákony o ochraně dat.	x	x		x		x	x
17	Zranitelnosti odhalené při skenování zranitelností a penetračním testování	Z17: Zranitelnosti odhalené při skenování zranitelností a penetračním testování	1) Nezabezpečené řízení komunikace. 2) Zastaralý software. 3) Slabá hesla uživatelů. 4) Nešifrovaná komunikace. 5) Nepodporovaná technická aktiva.	x	x	x	x	x	x	x

Hrozby jsou doplněny o vektor útoku, působnost varování NÚKIB ze dne 17. prosince 2018 a atributy, na které působí. Hrozby u technických nebo programových prostředků, pro které je relevantní varování NÚKIB ze dne 17. prosince 2018, musí být hodnoceny na **úrovni 4 – kritická**. Tyto hrozby jsou označovány podbarvením.

Tabulka 9: Katalog hrozeb

ID	Typové hrozby	Označení	Příklady hrozeb	Vektor útoku	Je relevantní varování NÚKIB ze dne 17. prosince 2018?	Dův.	Int.	Dost.
1	Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů, administrátorů, osob zastávající bezpečnostní role, dodavatelů a vrcholového vedení	H1: Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů, administrátorů, osob zastávající bezpečnostní role, dodavatelů a vrcholového vedení	1) Zaměstnanec nedodrží interní předpisy organizace. 2) Nedodržení zákonných předpisů dopadajících na organizaci. 3) Zaměstnanec nebo dodavatel záměrně poruší bezpečnostní politiku organizace. 4) Zaměstnanec nebo dodavatel záměrně eskaluje svá oprávnění. 5) Zaměstnanec nebo dodavatel do infrastruktury organizace připojí neschválený HW. 6) Zaměstnanec (vývojář) provede neoprávněné změny v aplikačním kódu a jiné změny vyvíjeného SW. 7) Zaměstnanec se seznámí s informacemi, které pro něj nebyly určeny. 8) Zaměstnanec sdílí informace s osobami, pro které nebyly určeny.	Interní/Externí	NE	x	x	x
2	Poškození nebo selhání technického nebo programového vybavení	H2: Poškození nebo selhání technického nebo programového vybavení	1) Náhodné přetížení HW serveru, sítě, koncové stanice. 2) Nedostupnost záloh. 3) Selhání HW zařízení (klimatizace, server, diskové pole). 4) Selhání operačního systému. 5) Zaplavení nebo požár serverovny. 6) Živelná pohroma – záplavy, tornádo, zemětřesení apod.	Vyšší moc/Externí	ANO		x	x

3	Zneužití identity	H3: Zneužití identity y	1) Útočník se snaží o prolomení (hádání) hesel. 2) Útočník se snaží prolomit zabezpečení bezdrátové Wi-Fi sítě. 3) Útočník se snaží do organizace proniknout z guest Wi-Fi sítě. 4) Cílený kybernetický útok (hacking) - pokus o krádež identity prostřednictvím SQL Injection, XSS, session hijacking apod. 5) Útočník zneužije fyzickou přístupovou kartu. 6) Útočník odcizí heslo doménového administrátora/privátní klíče k PKI. 7) Útočník zneužije důvěru zaměstnance a donutí jej jednat ve svůj prospěch. 8) Zaměstnanec zneužije přístupové údaje/kartu jiného zaměstnance.	Interní/Externí	NE	x	x	
4	Užívání programového vybavení v rozporu s licenčními podmínkami	H4: Užívání programového vybavení v rozporu s licenčními podmínkami	1) Zaměstnanec instaluje nepovolený SW na uživatelskou stanici. 2) Porušení licenčních podmínek SW. 3) Užívání pirátských kopií, falšování licencí. 4) Stahování programů z nezabezpečených a neoficiálních serverů.	Interní	NE		x	x
5	Škodlivý kód	H5: Škodlivý kód	1) Zaměstnanec infikuje pracovní stanici škodlivým kódem při práci (např. stažení přílohy, vyhledávání na internetu apod.). 2) Zaměstnanec infikuje počítačovou síť vložením infikovaného vyměnitelného zařízení či datových nosičů (USB disk, CD, DVD). 3) Napadení plošně šířeným malware.	Interní/Externí	ANO	x	x	x
6	Narušení fyzické bezpečnosti	H6: Narušení fyzické bezpečnosti	1) Zaměstnanec zneužije fyzické přístupy do lokalit organizace po ukončení pracovního poměru. 2) Zaměstnanec zpřístupní neoprávněné osobě zabezpečené prostory (serverovny, rozvodna, archiv apod.). 3) Teroristický útok. 4) Útočník se snaží fyzicky proniknout do organizace – destruktivní/nedestruktivní metody (např. odvrtání zámku, otevření zámku pomocí šperháků, přerezáání mříží, rozbití oken apod.).	Interní/Externí	NE	x	x	x

INTERNÍ TLP:GREEN

7	Přerušení poskytování služeb elektronických komunikací, satelitních služeb nebo dodávek elektrické energie nebo jiných důležitých služeb	H7: Přerušení poskytování služeb elektronických komunikací, satelitních služeb nebo dodávek elektrické energie nebo jiných důležitých služeb	1) Selhání dodávky elektrické energie, konektivity nebo jiných důležitých služeb pro provoz ICT. 2) Krátkodobé přerušení dodávek elektrické energie.	Externí/Vyšší moc	NE		x	x
8	Narušení dostupnosti primárních a podpůrných aktiv umístěných mimo území České republiky	H8: Narušení dostupnosti primárních a podpůrných aktiv umístěných mimo území České republiky	1) Zavedení nových zákonů o ochraně dat nebo omezení určitých technologií. 2) Přírodní katastrofa (např. zemětřesení), která zasáhne serverové technologie nebo datová centra umístěná mimo území České republiky.	Externí/Vyšší moc	NE			x
9	Zneužití nebo neoprávněná modifikace informací	H9: Zneužití nebo neoprávněná modifikace informací	1) Útočník získá přístup k aplikaci/systému. 2) Administrátor provede neoprávněnou změnu v nastavení SW. 3) Útočník v databázi pozmění data. 4) Útočník získá přístup k datům v databázi a využije je k zacílení svých dalších útoků. 5) Neautorizované spuštění řídicích síťových služeb.	Interní/Externí	ANO	x	x	x
10	Ztráta, odcizení nebo poškození aktiva	H10: Ztráta, odcizení nebo poškození aktiva	1) Zaměstnanec odcizí nebo smaže data nebo informace. 2) Útočník odcizí přenosné zařízení (notebook/mobilní telefon) či listinné dokumenty s daty nebo informacemi mimo prostory organizace (např. z auta, v restauraci apod.). 3) Útočník odcizí aktivum (notebook, mobilní telefon, klasifikované listinné dokumenty) z lokalit organizace. 4) Neoprávněná osoba přečte citlivé volně ležící dokumenty nebo vyhozené do koše, přečte citlivá data z obrazovky /stolu, ke kterým by se neměl dostat nebo přečte dokumenty z tiskárny. 5) Zaměstnanec si neoprávněně ponechá aktiva po ukončení pracovního poměru.	Interní/Externí	ANO	x		x

11	Nedodržení smluvního závazku ze strany dodavatele	H11: Nedodržení smluvního závazku ze strany dodavatele	1) Nedodržení pokynů organizace zaměstnanci dodavatele. 2) Nedodržování bezpečnostních opatření při vzdáleném přístupu přes VPN, RDP. 3) Únik nebo zneužití informací dodavatelem dodávek/služeb a porušení NDA. 4) Výpadek služby dodavatele. 5) Poškození aktiva při dodávce. 6) Dodavatel poruší nastavená SLA ve smlouvě. 7) Dodavatel přestane zajišťovat nasmlouvanou podporu HW a SW. 8) Dodavatel přestane dodávat nasmlouvané služby. 9) Dodavatel nedodává služby v požadované kvalitě a rozsahu.	Externí	NE	x	x	x
12	Pochybení ze strany uživatelů, administrátorů, osob zastávajících bezpečnostní role, dodavatelů a vrcholného vedení	H12: Pochybení ze strany uživatelů, administrátorů, osob zastávajících bezpečnostní role, dodavatelů a vrcholného vedení	1) Nezodpovědné chování při práci s e-mailem a při výměně informací s třetí stranou. 2) Sdílení citlivých dat na veřejných úložištích (Cloud). 3) Nákup nebo akvizice ICT prostředků pouze na základě ekonomické výhodnosti. 4) Nákup nevhodného zařízení s nedostatečnými funkcionalitami (např. nedostatečné šifrování přenosu dat / informací (plain text) nebo využívání nezabezpečených síťových protokolů). 5) Nedostatečné finanční zdroje. 6) Neúmyslně poškodí aktivum. 7) Opomenutí uzamknutí pracovní stanice při odchodu z kanceláře. 8) Narušení provozu chybami administrátorů. 9) Neadekvátní konfigurace aktivních síťových komponentů. 10) Nezákonné zpracování dat (vč. osobních údajů).	Interní	NE	x	x	x
13	Zneužití vnitřních prostředků, sabotáž	H13: Zneužití vnitřních prostředků, sabotáž	1) Vydírání zaměstnanců za účelem ohrožení aktiv organizace. 2) Zničení/poškození chráněné lokality vandalismem. 3) Působení kryptominerů na serverech organizace. 4) Zaměstnanci sledují nebo stahují nepovolený obsah.	Interní/Externí	ANO	x	x	x

INTERNÍ TLP:GREEN

14	Dlouhodobé přerušení poskytování služeb elektronických komunikací, satelitních služeb, dodávky elektrické energie nebo jiných důležitých služeb	H14: Dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb	1) Útoční se snaží o zablokování účtu. 2) Úmyslné přetížení HW servery, sítě, koncové stanice, zahlcením DOS, DDOS útokem. 3) Živelné pohromy (např. vichřice, popadané stromy na elektrickém vedení) a pandemická situace. 4) Překopnuté kabely. 5) Zničení rozvodů elektrické energie.	Externí/Vyšší moc	ANO			x
15	Zaměstnanci s nedostatečnou odbornou úrovní znalostí	H15: Zaměstnanci s nedostatečnou úrovní znalostí	1) Zaměstnanec neidentifikuje podvodné jednání. 2) Zaměstnanec neabsolvuje potřebná odborná školení. 3) Nedostatečné finanční zdroje pro zabezpečení lidských zdrojů.	Interní/Externí	NE	x	x	x
16	Cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik	H16: Cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik	1) Útočník využije technik sociálního inženýrství (včetně spear-phishingu) k získání přístupu do systému nebo do prostor organizace, využívá metod OSINT pro sběr informací o zaměstnancích a fungování organizace. 2) Útočník si vytvoří vlastní bezdrátovou síť, na které odchytává přístupové údaje uživatelů. 3) Zaměstnanec dodavatele provede útok (vzdáleně, interně) za účelem znepřístupnění služby. 4) Útočník fyzicky odezírá informace z obrazovky monitoru. 5) Útočník fyzicky odposlouchává citlivé rozhovory a jednání. 6) Zneužití nedostatků v kódu. 7) Cílené hrozby na organizaci (APT - Advanced Persistent Threat). 8) Instalace škodlivého kódu na uživatelské stanice útočníkem. 9) Útočník se snaží zašifrovat data pomocí ransomware.	Externí	ANO	x	x	x
17	Zneužití vyměnitelných technických nosičů dat	H17: Zneužití vyměnitelných technických nosičů dat	1) Útočník obnoví data ze zničených, poškozených nebo vadných disků. 2) Zaměstnanci ztratí vyměnitelné nosiče dat/jsou jim odcizeny apod.	Interní/Externí	ANO	x		

18	Napadení (odposlech, modifikace, podvržení) elektronické komunikace, satelitních služeb nebo jiných důležitých služeb	H18: Napadení (odposlech, modifikace, podvržení) elektronické komunikace, satelitních služeb nebo jiných důležitých služeb	1) Zaměstnanec nebo útočník se snaží proniknout do provozních systémů (nebo systémů s osobními údaji) - hacking, webové útoky - SQL Injection, Cross site scripting, Data tampering - MITM (nechráněná komunikace mezi zařízeními a serverem umožní neoprávněnou manipulaci s informacemi. 2) Útočník změní čas na serveru/koncové stanici, aby zamaskoval stopy. 3) Zaměstnanec nebo útočník odposlouchává nestíněné kabely/serverovnu. 4) Útočník zachycuje (interní/externí serverovou) komunikaci (např. e-mail). 5) Zaměstnanec nebo útočník přesměrovává komunikaci.	Interní/Externí	ANO	x	x	
19	Závislost na dodavateli	H19: Závislost na dodavateli	1) Výpadek u dodavatele způsobí nedostupnost poskytovaných služeb organizace a narušení provozu. 2) Dodavatel náhle zvýší cenu za své služby nebo produkty. 3) Monopol dodavatele. 4) Změna vlastnické struktury. 5) Špatné stanovení smluvních podmínek (vlastnictví zdrojového kódu).	Externí/Interní	ANO	x	x	x
20	Zneužití státní moci pro přístup k aktivům	H20: Zneužití státní moci pro přístup k aktivům	1) Státní orgán zabaví technická aktiva, nebo jiné fyzické vybavení organizace v rámci vyšetřování. 2) Neoprávněný přístup k citlivým informacím.	Externí	NE	x	x	x
21	Znepřístupnění nebo předání aktiv na základě žádosti státu	H21: Znepřístupnění nebo předání aktiv na základě žádosti státu	1) Státní orgány si vyžádají přístup k datům, které má organizace uloženy na svých technických aktivech v rámci vyšetřování. 2) Státní orgány zavedou zákon nebo regulaci, která omezuje přístup k určitým technologiím, které organizace využívá.	Externí	NE	x	x	x

Zranitelnosti jsou hodnoceny podle následující stupnice:

Tabulka 10: Stupnice pro hodnocení zranitelností

STUPNICE PRO HODNOCENÍ ZRANITELNOSTÍ		
1	Nízká	Zranitelnost neexistuje nebo je zneužití zranitelnosti málo pravděpodobné. Jsou zavedena bezpečnostní opatření, která jsou schopna včas detekovat možné zranitelnosti nebo případné pokusy o jejich zneužití.
2	Střední	Zneužití zranitelnosti je málo pravděpodobné až pravděpodobné. Jsou zavedena bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné zranitelnosti nebo případné pokusy o překonání opatření je omezena. Nejsou známy žádné úspěšné pokusy o překonání bezpečnostních opatření.
3	Vysoká	Zneužití zranitelnosti je pravděpodobné až velmi pravděpodobné. Bezpečnostní opatření jsou zavedena, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známy dílčí úspěšné pokusy o překonání bezpečnostních opatření.
4	Kritická	Zneužití zranitelnosti je velmi pravděpodobné až víceméně jisté. Bezpečnostní opatření nejsou realizována nebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známy úspěšné pokusy překonání bezpečnostních opatření.

Hrozby jsou hodnoceny podle následující stupnice:

Tabulka 11: Stupnice pro hodnocení hrozeb

STUPNICE PRO HODNOCENÍ HROZEB		
1	Nízká	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.
2	Střední	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let
3	Vysoká	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.
4	Kritická	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.

4.2 Scénáře

Následující tabulka udává relevantní kombinace zranitelností a hrozeb, které lze použít při určování rizik, tj. kombinací aktivum-zranitelnost-hrozba.

Tabulka 12: Kombinace hrozeb a zranitelností

		Hrozby																			
ID	Zranitelnosti	Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů, administrátorů, osob zastávajících bezpečnostní role, dodavatelů a vrcholové vedení	Poškození nebo selhání technického nebo programového vybavení	Zneužití identity	Užívání programového vybavení v rozporu s licenčními podmínkami	Škodlivý kód	Narušení fyzické bezpečnosti	Přerušování poskytování služeb elektronických komunikací, satelitních služeb nebo dodávek elektrické energie nebo jiných důležitých služeb	Narušení dostupnosti primárních a podpůrných aktiv umístěných mimo území České republiky	Zneužití nebo neoprávněná modifikace informací	Ztráta, odcizení nebo poškození aktiva	Nedodržení smluvního závazku ze strany dodavatele	Pochybení ze strany uživatelů, administrátorů, osob zastávajících bezpečnostní role, dodavatelů a vrcholového vedení	Zneužití vnitřních prostředků, sabotáž	Dlouhodobé přerušování poskytování služeb elektronických komunikací, satelitních služeb, dodávky elektrické energie nebo jiných důležitých služeb	Cílený kybernetický útok pomocí sociálního inženýrství, použití špiónážních technik	Zneužití vyměnitelných technických nosičů dat	Napadení (odposlech, modifikace, podvržení) elektronické komunikace, satelitních služeb nebo jiných důležitých služeb	Závislost na dodavateli	Zneužití státní moci pro přístup k aktivům	Zpřístupnění nebo předání aktiv na základě žádosti státu
1	Nedostatečná údržba aktiv	1	1	1		1	1	1	1	1	1		1	1	1	1	1	1	1		
2	Zastaralost aktiv	1	1	1		1	1	1		1	1		1	1	1	1	1	1	1		
3	Nedostatečná ochrana perimetru	1	1	1		1	1	1	1	1	1		1	1	1	1	1	1		1	1
4	Nedostatečné bezpečnostní povědomí uživatelů, administrátorů,	1		1	1	1	1		1	1	1	1	1			1	1	1	1	1	1

	osob zastávajících bezpečnostní role, dodavatelů a vrcholového vedení																				
5	Nedostatečné zálohování	1	1			1	1	1	1	1	1	1			1			1			
6	Nevhodné nastavení přístupových oprávnění	1		1	1	1	1			1	1	1	1	1			1	1	1		
7	Nedostatečné postupy a procesy pro detekování kybernetických bezpečnostních událostí a identifikování kybernetických bezpečnostních incidentů					1	1	1	1		1	1	1		1	1	1	1	1		
8	Nedostatečné monitorování činnosti uživatelů a administrátorů a, neschopnost odhalit činnost, která může mít vliv na	1		1		1			1	1	1	1	1	1		1	1	1	1	1	1

	bezpečnost regulované služby																				
9	Nedostatečné stanovení bezpečnostních pravidel a postupů, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů, osob zastávajících bezpečnostní role, dodavatelů a vrcholové vedení	1		1	1	1	1	1	1	1	1	1		1	1	1	1		1	1	1
10	Nedostatečná ochrana aktiv	1	1	1		1	1	1	1	1	1	1	1	1	1		1			1	1
11	Nevhodně navržená bezpečná architektura		1			1			1				1					1	1		
12	Nedostatečná míra nezávislé kontroly	1		1	1			1	1	1	1	1	1	1	1				1	1	1
13	Neschopnost včasného odhalení pochybení ze strany uživatelů	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1		
14	Nedostatek zaměstnání	1	1		1				1			1	1						1	1	1

INTERNÍ TLP:GREEN

	nců s potřebnou odbornou úrovní znalostí																				
15	Umístění aktiva mimo fyzickou kontrolu (například na území cizího státu)		1	1		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
16	Umístění aktiva na území státu, o jehož právním prostředí nemá povinná osoba dostatečn é povědomí		1	1		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
17	Zraniteln osti odhalené při skenování zraniteln ostí a penetračn ím testování		1	1	1	1	1	1		1		1	1	1		1					

5 Popis nástroje pro hodnocení aktiv a rizik

K evidenci aktiv, vazeb mezi aktivy a hodnocení rizik je využíván nástroj MS Excel. Příslušná šablona je přílohou této metodiky.¹

Karta Verze

Tato karta obsahuje údaje o změnách v dokumentu a kdo je provedl, o verzi dokumentu a datum, kdy byla vytvořena.

Karta Tabulky

Tato karta obsahuje stupnice pro hodnocení aktiv, hrozeb, zranitelností a rizik. Tyto stupnice jsou převzaty z této metodiky a slouží pro usnadnění procesu hodnocení aktiv a rizik.

Karta Matice dopadu

Tato karta obsahuje matici dopadu převzatou z metodiky a slouží pro usnadnění procesu hodnocení aktiv a rizik.

Karta Katalog primárních aktiv

Tato karta obsahuje údaje o jednotlivých primárních aktivech, příp. typových primárních aktivech. Jedná se o souhrnný seznam všech primárních aktiv, která jsou podrobněji popsána v kartách S1-P4.

¹ Vzhledem k tomu, že se jedná o modelový příklad, bude pro vysvětlení použito přímo vzorové hodnocení aktiv a rizik obsažené v dokumentu *Příloha 6: Vzorové hodnocení aktiv a rizik*. V praxi by v této kapitole byla popsána šablona.

Tabulka 13: Popis položek v Katalogu primárních aktiv

Položka	Popis
ID	Jedinečný identifikátor primárního aktiva.
Typové primární aktivum	Krátký slovní popis primárního aktiva.
Název	Kombinace identifikátoru a slovního popisu vytváří název primárního aktiva.
Kategorie	Zařazení primárního aktiva do kategorie „služba“ nebo „informace“.
Specifikace	Detailní popis primárního aktiva.
Gestor aktiva	Určený gestor primárního aktiva.
Garant aktiva	Určený garant primárního aktiva.
Osobní údaje	Informace o tom, zda primární aktivum obsahuje osobní údaje.
Legislativa	Popis relevantní legislativy, která má na primární aktivum vliv.
Rozsah řízení KB	Informace o tom, zda je primární aktivum součástí rozsahu řízení KB.
Dostupnost	Hodnocení primárního aktiva z pohledu dostupnosti.
Ztráta	Hodnocení primárního aktiva z pohledu ztráty.
Důvěrnost	Hodnocení primárního aktiva z pohledu důvěrnosti.
Integrita	Hodnocení primárního aktiva z pohledu integrity.
Poznámka	Místo pro případné doplnění informací o primárním aktivu.

Karta Vazby primárních aktiv

Tato karta obsahuje evidenci vazeb mezi primárními aktivy. Pokud mezi aktivy existuje vazba, je označena symbolem „x“.

Karty S1-P4

Tyto karty obsahují detailní informace o primárních aktivech včetně jejich hodnocení dle příslušných stupnic a matice dopadu.

Karta Katalog podpůrných aktiv

Tato karta obsahuje údaje o jednotlivých podpůrných aktivech, příp. typových podpůrných aktivech.

Tabulka 14: Popis položek v Katalogu podpůrných aktiv

Položka	Popis
ID	Jedinečný identifikátor podpůrného aktiva.

Kategorie podpůrného aktiva	Zařazení podpůrného aktiva do příslušné kategorie (technické vybavení (HW), komunikační prostředky, programové vybavení (SW), objekty, lidské zdroje, dodavatelé, externí systémy a služby).
Skupina podpůrného aktiva	Zařazení podpůrného aktiva do skupiny v rámci kategorie podpůrného aktiva (viz <i>Příloha 4: Struktura podpůrných aktiv</i>).
Typové podpůrné aktivum	Zařazení podpůrného aktiva do obecného typového aktiva v rámci skupiny podpůrného aktiva.
Název	Kombinace identifikátoru a slovního popisu vytváří název podpůrného aktiva.
Popis podpůrného aktiva	Detailní popis podpůrného aktiva.
Gestor aktiva	Určený gestor podpůrného aktiva.
Garant aktiva	Určený garant podpůrného aktiva.
Významný dodavatel	Evidence významného dodavatele (pokud je k podpůrnému aktivu určen).
Rozsah řízení KB	Informace o tom, zda je podpůrné aktivum součástí rozsahu řízení KB.
Dostupnost	Hodnocení podpůrného aktiva z pohledu dostupnosti.
Ztráta	Hodnocení podpůrného aktiva z pohledu ztráty.
Důvěrnost	Hodnocení podpůrného aktiva z pohledu důvěrnosti.
Integrita	Hodnocení podpůrného aktiva z pohledu integrity.
Poznámka	Místo pro případné doplnění informací o podpůrném aktivu.

Karta Struktura podpůrných aktiv

Tato karta obsahuje upravenou strukturu podpůrných aktiv popsanou v *Příloze 4: Struktura podpůrných aktiv*, která byla přizpůsobena prostředí ministerstva a obsahuje určená podpůrná aktiva.

Karta Vazby

Tato karta slouží jako evidence vazeb mezi primárními a podpůrnými aktivy a zároveň jako evidence váhy vlivu těchto vazeb. V případě, že byly určeny vazby na všechna primární aktiva, byla vazba označena pouze u příslušného primárního aktiva typu služba. Důvodem bylo to, že primární aktiva typu služba jsou zastřešující a přebírají hodnoty navázaných primárních aktiv typu informace a pro následné hodnocení jsou rozhodující nejvyšší hodnoty.

Karta Hodnoty podpůrných aktiv

Tato karta slouží pro výpočty výsledných hodnot podpůrných aktiv dle příslušných vzorců. Hodnoty podpůrných aktiv jsou automaticky vypočteny a zapsány do Katalogu podpůrných aktiv.

Karta Katalog zranitelností

Tato karta obsahuje seznam kategorií zranitelností dle přílohy č. 3 vyhlášky, ke kterým jsou přiřazeny konkrétní příklady. Dále je označeno, u jakých typů aktiv (HW, SW, komunikační prostředky, objekty, lidské zdroje, dodavatelé a externí služby) se mohou zranitelnosti vyskytovat.

Karta Katalog hrozeb

Tato karta obsahuje seznam kategorií hrozeb dle přílohy č. 3 vyhlášky, ke kterým jsou přiřazeny konkrétní příklady. Dále je doplněn vektor útoku (interní/externí), zda je relevantní varování NÚKIB ze dne 17. prosince 2018 a jestli hrozba působí na důvěrnost, integritu nebo dostupnost.

Karta Zranitelnosti a hrozby

Tato karta obsahuje předpřipravené scénáře, kde je posuzováno, zda může hrozba zneužít příslušnou zranitelnost.

Karta Katalog rizik

Tato karta obsahuje katalog rizik, který je rozdělen do tří částí: hodnocení rizik aktuálního stavu v organizaci, hodnocení rizik s předpokládaným snížením hodnot po zavedení bezpečnostních opatření a hodnoty se zohledněním varování NÚKIB ze dne 17. prosince 2018 (se započítáním bezpečnostních opatření).

V každém řádku je uvedeno riziko (kombinace aktivum-zranitelnost-hrozba), jehož výsledná hodnota se mění s ohledem na změny podmínek (např. zavedení bezpečnostního opatření).

Tabulka 15: Popis nástroje pro hodnocení aktiv a rizik

Položka	Popis
ID	Jedinečný identifikátor rizika.
Aktivum	Příslušné aktivum, kterého se riziko týká (společně se zranitelností a hrozbou tvoří výslednou kombinaci aktivum-zranitelnost-hrozba).
Hodnota dopadu – dostupnost	Hodnota příslušného aktiva z pohledu dostupnosti (převzatá z katalogu aktiv).
Hodnota dopadu – důvěrnost	Hodnota příslušného aktiva z pohledu důvěrnosti (převzatá z katalogu aktiv).
Hodnota dopadu – integrita	Hodnota příslušného aktiva z pohledu integrity (převzatá z katalogu aktiv).
Zranitelnost	Příslušná zranitelnost, které se riziko týká (společně s aktivem a hrozbou tvoří výslednou kombinaci aktivum-zranitelnost-hrozba).
Hodnota zranitelnosti	Ohodnocení zranitelnosti podle příslušné stupnice na úrovni 1-4.
Hrozba	Příslušná hrozba, které se riziko týká (společně s aktivem a zranitelností tvoří výslednou kombinaci aktivum-zranitelnost-hrozba).
Hodnota hrozby	Ohodnocení hrozby podle příslušné stupnice na úrovni 1-4.

Hodnota rizika – dostupnost	Výpočet výsledné hodnoty rizika (vynásobení hodnoty aktiva pro atribut dostupnosti, zranitelnosti a hrozby).
Hodnota rizika – důvěrnost	Výpočet výsledné hodnoty rizika (vynásobení hodnoty aktiva pro atribut důvěrnosti, zranitelnosti a hrozby).
Hodnota rizika – integrita	Výpočet výsledné hodnoty rizika (vynásobení hodnoty aktiva pro atribut integrity, zranitelnosti a hrozby).
Způsob zvládání rizika	Evidence způsobu zvládání rizika (akceptace, redukce, sledování).
Komentář	Místo pro případné doplnění informací o riziku.

6 Prohlášení o aplikovatelnosti

Prohlášení o aplikovatelnosti musí obsahovat:

- Všechna bezpečnostní opatření požadovaná vyhláškou
- Popis bezpečnostního opatření
- Informaci o tom, zda je bezpečnostní opatření aplikované
- Způsob plnění u aplikovaných bezpečnostních opatření
- Odůvodnění neaplikování bezpečnostního opatření (pokud je relevantní)
- Přijatá náhradní bezpečnostní opatření u neaplikovaných bezpečnostních opatření (pokud je relevantní)
- Označení úrovně, na které je bezpečnostní opatření zavedeno (pokud je relevantní)

Prohlášení o aplikovatelnosti má dále funkci GAP analýzy a popisuje aktuální stav zabezpečení ministerstva. Zároveň je využíváno při hodnocení rizik jako pomůcka pro hodnocení zranitelností jako tzv. Katalog opatření.

Jednotlivá aplikovaná bezpečnostní opatření jsou hodnocena na úrovni 1-4, v závislosti na tom, jak je jejich zavedení účinné. Zároveň jsou zmapovány vazby mezi bezpečnostními opatřeními a zranitelnostmi. Na základě hodnocení úrovně účinnosti zavedených bezpečnostních opatření je vypočítána výsledná hodnota pro úroveň zranitelnosti, která slouží jako výchozí hodnota pro hodnocení zranitelnosti v rámci procesu hodnocení rizik. Při hodnocení kombinace aktivum-zranitelnost-hrozba může být výchozí hodnota zranitelnosti zvýšena nebo snížena na základě konkrétních okolností souvisejících s určeným rizikem.

Každé bezpečnostní opatření působí na jednu nebo více zranitelností (tedy snižuje jejich míru). Při určení vazeb mezi bezpečnostními opatřeními a zranitelnostmi byla využita zejména následující pravidla:

- Byla hledána tzv. primární vazba mezi bezpečnostním opatřením a zranitelnostmi, kdy bylo zjišťováno, na jaké zranitelnosti působí posuzované bezpečnostní opatření nejvíce
 - Pokud by byly hledány i sekundární vazby, tak by téměř všechna bezpečnostní opatření působila alespoň v malé míře na všechny zranitelnosti
- Bezpečnostním opatřením, která se týkala dokumentace, pravidel, nebo postupů byla vždy přiřazena primární vazba na zranitelnost „Nedostatečné stanovení bezpečnostních pravidel a postupů, nepřesné nebo nejednoznačné vymezení práv a povinností lidských zdrojů“
- Vzhledem k obecnější míře detailu jednotlivých zranitelností nebylo vždy možné najít adekvátní konkrétní zranitelnosti, v takovém případě byla využita vazba na zranitelnost „Nedostatečná ochrana aktiv“

Katalog opatření je průběžně doplňován o konkrétní bezpečnostní opatření zavedená v rámci organizace (čímž dochází ke konkretizaci obecněji definovaných ustanovení uvedených ve vyhlášce a aplikování na specifické prostředí ministerstva).

Prohlášení o aplikovatelnosti musí být pravidelně aktualizováno na základě stavu zavádění bezpečnostních opatření v rámci organizace. Nejpozději 1× ročně musí být revidováno v souvislosti s aktualizací hodnocení rizik.

Prohlášení o aplikovatelnosti schvaluje výbor pro řízení KB.

6.1 Popis nástroje pro prohlášení o aplikovatelnosti

Prohlášení o aplikovatelnosti je zpracováno v nástroji MS Excel. Příslušná šablona je přílohou této metodiky.²

Tabulka 16: Popis nástroje pro Prohlášení o aplikovatelnosti

Položka	Popis
ID	Jedinečný identifikátor bezpečnostního opatření.
Vazba	Odkaz na zákon nebo vyhlášku (konkrétní paragraf, příp. odst., písm. nebo příloha).
Otázka	Otázka popisující stav bezpečnostního opatření v organizaci (u dokumentace je potřeba současně posuzovat, jestli jsou popsány postupy zavedené v praxi a jestli je dokumentace aktualizovaná).
Aplikováno bezpečnostní opatření	Evidence, zda je příslušné bezpečnostní opatření v prostředí organizace aplikované nebo ne.
Odůvodnění neaplikování bezpečnostního opatření	V případě, že je bezpečnostní opatření neaplikované, je nutné vyplnit odůvodnění neaplikování opatření.
Přijatá náhradní bezpečnostní opatření	V případě, že je bezpečnostní opatření neaplikované, je nutné vyplnit přijatá náhradní bezpečnostní opatření.
Hodnocení účinnosti bezpečnostního opatření	Odpověď na otázku popisující stav bezpečnostního opatření. Účinnost bezpečnostního opatření je posuzována na stupnici 1-4, kde opatření na úrovni 1 nás chrání vždy, opatření na úrovni 2 nás chrání ve většině případů, opatření na úrovni 3 nás chrání jen někdy a opatření s účinností na úrovni 4 nejsou zavedena.
Komentář	Místo pro případné doplnění informací o bezpečnostním opatření.
Číselná hodnota účinnosti bezpečnostního opatření	Na základě slovního hodnocení účinnosti opatření je zde vyplněna příslušná číselná hodnota 1-4.
Kategorie zranitelností	Zde jsou uvedeny jednotlivé kategorie zranitelností z Katalogu zranitelností a tam, kde existuje vazba mezi zranitelností a bezpečnostním opatřením (viz začátek této kapitoly) je uveden symbol „x“.

Na konci příslušné tabulky jsou uvedeny maximální a průměrné hodnoty zranitelností vypočítané na základě vazeb mezi bezpečnostními opatřeními a zranitelnostmi (sloupce O–AE) a hodnoty účinnosti opatření (sloupec N). **Neaplikovaná bezpečnostní opatření nejsou do výpočtu zahrnuta.**

² Vzhledem k tomu, že se jedná o modelový příklad bude pro vysvětlení použito přímo prohlášení o aplikovatelnosti obsažené v dokumentu *Příloha 7: Vzorové prohlášení o aplikovatelnosti*. V praxi by v této kapitole byla popsána šablona.

7 Zvládání rizik

Rizika určená a ohodnocená v rámci hodnocení rizik je nutné dále zvládat. Je nutné porovnat výslednou hodnotu rizika s kritérii pro akceptovatelnost a na základě toho zvolit vhodný způsob zvládání rizika, mezi které patří:

- Akceptace rizika
- Sledování rizika
- Redukce a eliminace rizika
- Vyhnutí se riziku
- Přenesení a sdílení rizika

Akceptace

Při tomto způsobu zvládání se s rizikem jako takovým již nic dále nedělá, pouze se přijme, tedy dochází k podstoupení rizika. Používá se pro rizika nízké až střední úrovně.

Sledování

Při tomto způsobu zvládání již není riziko dále snižováno, ale je pečlivě sledováno v čase, zejména zda nedochází k navýšení v oblasti dopadu, pravděpodobnosti hrozby, nebo míry zranitelnosti s rizikem spojeným. Používá se pro rizika střední úrovně.

Redukce

Při tomto způsobu zvládání dochází k aplikování vhodných bezpečnostních opatření za účelem snížení rizika na nižší úroveň (v ideálním případě akceptovatelnou). Je možné využít pro všechny úrovně rizik, zejména se používá pro rizika střední až kritické úrovně.

Eliminace

Tento způsob zvládání rizika spočívá v nalezení jiného řešení dané situace, které rizikovou událost neobsahuje.

Vyhnutí

Tato metoda spočívá v utlumení (velmi omezeném využití) nebo vypnutí (nepoužívání) daného aktiva.

Přenos a sdílení

Při tomto způsobu zvládání se s rizikem jako takovým nic neděje, pouze dochází k jeho přenesení (resp. dopadu, který může nastat) na třetí stranu (např. pojišťovnu), která je s tímto přenosem ztotožněna a souhlasí s ním. Je možné využít pro všechny úrovně rizik, zejména se používá pro rizika střední až kritické úrovně.

Zvládání rizik navrhuje manažer KB ve spolupráci s architektem KB a gestory příp. garanty aktiv.

Všechna rizika musí být monitorována a přezkoumávána, přinejmenším 1× ročně v rámci hodnocení rizik.

Navržená bezpečnostní opatření jsou evidována v plánu zvládání rizik.

8 Plán zvládání rizik

Plán zvládání rizik musí obsahovat:

- Popis bezpečnostních opatření pro zvládání rizik
- Cíle a přínosy bezpečnostních opatření pro zvládání rizik
- Určení osoby zajišťující prosazování bezpečnostních opatření pro zvládání rizik
- Potřebné finanční, technické, lidské a informační zdroje pro zavedení bezpečnostních opatření
- Termín zavedení bezpečnostních opatření
- Popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními
- Konkrétní způsob realizace bezpečnostních opatření
- Způsob hodnocení úspěšnosti zavedení jednotlivých bezpečnostních opatření pro zvládání rizik

Do plánu zvládání rizik je nutné promítnout také významné změny, změny v rozsahu řízení KB, protiopatření podle § 20 zákona, kybernetické bezpečnostní incidenty, včetně dříve řešených, výsledky auditů a kontrol v oblasti KB, výsledky penetračního testování a skenování zranitelností a výsledky vyhodnocení účinnosti systému řízení bezpečnosti informací. V plánu je možné odkazovat na další dokumenty obsahující podrobnější informace k jednotlivým bezpečnostním opatřením.

Plán zvládání rizik musí být pravidelně aktualizován v souvislosti s vývojem zavádění bezpečnostních opatření v rámci organizace. Minimálně 1× ročně musí být revidován v souvislosti s aktualizací hodnocení rizik.

Plán zvládání rizik schvaluje výbor pro řízení KB.

8.1 Popis nástroje pro plán zvládání rizik

Plán zvládání rizik je zpracován v nástroji MS Excel. Příslušná šablona je přílohou této metodiky.³

Tabulka 16: Popis nástroje pro plán zvládání rizik

Položka	Popis
ID	Jedinečný identifikátor bezpečnostního opatření.
Popis bezpečnostního opatření pro zvládání rizik	Popis příslušného bezpečnostního opatření.
Priorita	Priorita jednotlivých bezpečnostních opatření dle důležitosti a naléhavosti jejich zavedení.
Zdroj	Zdroj, ze kterého byla určena potřeba zavedení bezpečnostního opatření.
Popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními	Vazba mezi bezpečnostním opatřením a riziky, které ošetřuje.
Stav	Stav bezpečnostního opatření, např. zavedeno, nezavedeno, v průběhu zavádění, čeká na provedení jiného bezpečnostního opatření, čeká na schválení výborem pro řízení KB.

³ Vzhledem k tomu, že se jedná o modelový příklad, bude pro vysvětlení použit přímo plán zvládání rizik obsažený v dokumentu *Příloha 8: Vzorový plán zvládání rizik*. V praxi by v této kapitole byla popsána šablona.

Cíle a přínosy bezpečnostních opatření pro zvládání rizik	Popis cílů a přínosů, které bude mít zavedení daného bezpečnostního opatření.
Určené osoby zajišťující zavedení bezpečnostních opatření	Přidělená osoba, která je odpovědná za dané bezpečnostní opatření.
Konkrétní způsob realizace bezpečnostních opatření	Konkrétní bezpečnostní opatření, která budou realizována pro snížení hodnoty rizika.
Požadovaný termín zavedení bezpečnostních opatření	Termín, dokdy musí být bezpečnostní opatření zavedeno.
Potřebné zdroje	Popis zdrojů potřebných pro zavedení bezpečnostního opatření (technické, finanční – investiční a provozní, lidské a informační).
Metrika pro vyhodnocení úspěšnosti	Popis postupu pro vyhodnocení účinnosti bezpečnostního opatření.
Poznámka	Místo pro případné doplnění informací o bezpečnostním opatření.

9 Zpráva o hodnocení rizik

Ke každému provedenému hodnocení rizik musí být vytvořena zpráva obsahující shrnutí informací pro výbor pro řízení KB. Obsahem zprávy je:

- Účel dokumentu a předmět hodnocení
- Přehled aktiv
- Zvládání rizik
 - Kritéria pro akceptovatelnost
 - Shrnutí rizik
 - Zvládání rizik určených v rámci hodnocení rizik
 - Bezpečnostní opatření, která je nutno aplikovat
 - Bezpečnostní opatření, která je vhodné aplikovat
- Související dokumentace

Zpráva o hodnocení rizik musí být schválena výborem pro řízení KB. Současně musí být schválen způsob zvládání rizik podle postupu uvedeného u kritérií pro akceptovatelnost.

10 Řízení výjimek

V případě, že riziko na úrovni vysoká nebo kritická nelze snížit zavedením bezpečnostního opatření do jednoho roku (a uvést v plánu zvládnání rizik pro daný rok), je nutné sepsat odůvodnění, např. zavedení bezpečnostního opatření je časově a finančně náročné. Toto odůvodnění slouží jako základ pro žádost o výjimku. Součástí odůvodnění je návrh na odstranění výjimky.

Žádosti o výjimky posuzuje výbor pro řízení KB, který může udělit výjimku na dobu nezbytně nutnou (dobu nutnou pro realizaci příslušného bezpečnostního opatření), čímž akceptuje riziko s výjimkou spojené. Po roce je nutné provést přezkoumání výjimek a způsobů jejich odstranění.

Výjimky eviduje manažer KB.