Úřad vlády České republiky

Odbor Rady pro výzkum, vývoj a inovace

Metodika řízení rizik kybernetické bezpečnosti IS VaVaI

Metodika definující způsob naplnění vybraných povinnosti dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti v oblasti identifikace, analýzy a řízení rizik informačního systému pro výzkum, vývoj a inovace (IS VaVaI).

Zpracoval: kolektiv RELSIE

Schválil: Marek Jan

Verze: 1.0

Datum: 16. ledna 2019

OBSAH

1 ÚVOD

1.1 Účel dokumentu

Tato dokument stanovuje metodiku provedení analýzy a řízení rizik IS VaVaI. Metodika a následný proces řízení rizik vychází z požadavků zákona č. 181/2014 Sb., o kybernetické bezpečnosti, dále vychází z doporučení norem řady ISO 27001.

Metodika řízení rizik je součástí bezpečnostní dokumentace IS VaVaI, tj. systému řízení kybernetické bezpečnosti. Zároveň slouží jako podklad pro kontrolu, že řízení rizik KB je realizováno dle stanoveného postupu.

1.2 Východiska

Pro užití této metodiky organizace samostatně vypracuje a připraví podklady a vstupy pro analýzu rizik, jmenovitě:

- vymezení rozsahu SŘBI,
- dekompozice aktiv,
- hodnocení zranitelností,
- hodnocení hrozeb,
- hodnocení dopadů.

Tato metodika hodnocení rizik vychází z doporučení norem ISO 27005 a ISO 31000 pro oblast řízení rizik. Dále tato vychází z požadavků zákona č. 181/2014 Sb., o kybernetické bezpečnosti (ZoKB), v rozsahu požadavku jeho prováděcího předpisu, vyhlášky č. 316/2014 Sb., § 4, odstavce 1, písm. a).

Postupy jsou uvedeny v tomto dokumentu, který dává v několika bodech možnost volby a nastavení systému organizací samotnou. Výsledný způsob (konkrétní metodika přístupu k jednotlivým činnostem) ale musí být jednoznačně dokumentován, aby podle něj mohlo být postupováno a byla umožněna kontrola správného provedení činností.

1.3 Dotčení pracovníci

Tento dokument je určen pro všechny „role“ zainteresované na správě aktiv IS VaVaI, tzn. zejména manažera KB IS VaVaI, Garanty aktiv IS VaVaI (primárních a podpůrných) a další bezpečnostní role řízení rizik KB IS VaVaI.

- Manažer KB IS VaVaI (této role se problematika týká hlavně v oblasti kontroly procesů řízení rizik a začlenění do kontextu řízení rizik ÚV ČR)
- Garant aktiva IS VaVaI (primární role, odpovědná za provedení analýzy rizik, aplikaci stanovených opatření a následné provádění procesu řízení rizik)
- Garanti podpůrných aktiv (role dotčená zejména v oblasti provádění analýzy rizik a následně provádění stanovených preventivních a kontingenčních opatření)
- Další pracovníci (dalších pracovníků se problematika týká hlavně v oblasti identifikace aktiv)

Poznámka: role využívané při správě a zajištění bezpečnosti IS VaVaI jsou definovány v interním předpisu „Příručka ISMS“.

1.4 Související dokumenty a výstupy

Související dokumenty:

- Metodika identifikace a hodnocení aktiv IS VaVaI
- Výstupy z procesu identifikace a hodnocení aktiv
- Příručka ISMS IS VaVaI
- Politika bezpečnosti informací IS VaVaI

Dále se jedná o

- Metodiku stanovení kritérií přijatelnosti rizik, včetně kritérií pro určení přijatelné míry zbytkového rizika.

Výstupní dokumenty:

V procesu řízení rizik na základě této metodiky jsou vypracovány (resp. aktualizovány) následující dokumentované informace:

- Přehled a hodnocení identifikovatelných rizik
- Zpráva z analýzy a hodnocení rizik
- Prohlášení o aplikovatelnosti

které obsahuje přehled vybraných a zavedených bezpečnostních opatření,

- Plán zvládání rizik

který obsahuje cíle a přínosy bezpečnostních opatření pro zvládání rizik, určení osoby zajišťující prosazování bezpečnostních opatření pro zvládání rizik, potřebné finanční, technické, lidské a informační zdroje, termín jejich zavedení a popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními.

1.5 Seznam zkratek

Zkratka	Význam
KB	Kybernetická bezpečnost
ÚV ČR	Úřad vlády České republiky
RVVI	Rada pro vědu, výzkum a inovace, poradní orgán Vlády České republiky
IS VaVaI	Informační systém výzkumu, vývoje a inovací
ZKB	Zákon o kybernetické bezpečnosti
ISMS	Systém řízení bezpečnosti informací
Sb.	Sbírka zákonů České republiky
ČR	Česká republika
VIS	Významný informační systém
NCKB	Národní centrum kybernetické bezpečnosti
RACI	Matice odpovědností
IT	Informační technologie
EU	Evropská unie
ISO	Mezinárodní organizace pro standardizaci
IEC	International Electrotechnical Commission

1.6 Terminologie z oblastí řízení rizik

aktivum – primární aktivum a podpůrné aktivum

primární aktivum – informace nebo služba, kterou zpracovává nebo poskytuje informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury nebo významný informační systém,

podpůrné aktivum – technické aktivum, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému,

technické aktivum – technické vybavení, komunikační prostředky a programové vybavení informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému a objekty, ve kterých jsou tyto systémy umístěny,

riziko – možnost, že určitá hrozba využije zranitelnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému a způsobí poškození aktiva,

hodnocení rizik – proces, při němž je určována významnost rizik a jejich přijatelná úroveň,

řízení rizik – činnost zahrnující hodnocení rizik, výběr a zavedení opatření ke zvládání rizik, sdílení informací o riziku a sledování a přezkoumání rizik,

hrozba – potenciální příčina kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, jejímž výsledkem může být poškození aktiva,

zranitelnost – slabé místo aktiva nebo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami,

přijatelné riziko – riziko zbývající po uplatnění bezpečnostních opatření, jehož úroveň odpovídá kritériím pro přijatelnost rizik,

bezpečnostní politika – soubor zásad a pravidel, které určují způsob zajištění ochrany aktiv orgánem a osobou uvedenou v § 3 písm. c) až e) zákona č. 181/2014 Sb., o kybernetické bezpečnosti,

garant aktiva – fyzická osoba pověřená orgánem nebo osobou uvedenou v § 3 písm. c) až e) zákona č. 181/2014 Sb., o kybernetické bezpečnosti, k zajištění rozvoje, použití a bezpečnosti aktiva,

uživatel – fyzická nebo právnická osoba anebo orgán veřejné moci, která využívá primární aktiva,

administrátor – fyzická osoba pověřená garantem aktiva zajišťující správu, provoz, použití, údržbu a bezpečnost technického aktiva.

2 PROCES POSUZOVÁNÍ RIZIK BEZPEČNOSTI INFORMACÍ

Proces posouzení rizik vychází z obecných principů hodnocení rizik uváděných v normě ISO 31000. Metodika identifikace a vyhodnocení rizik je založena na pravidlech a postupech definovaných normou ISO 27005. Stupně hodnocení rizik vychází z doporučení Vyhlášky č. 82/2018 Sb., příloha č. 2.

3 PROCES POSUZOVÁNÍ RIZIK

Proces posuzování rizik bezpečnosti informací vychází z doporučení normy ISO 27005 a zahrnuje níže uvedené fáze:

1) Stanovení kontextu hodnocení rizik
2) Identifikace a hodnocení aktiv
3) Identifikace rizik
4) Analýza rizik
5) Vyhodnocení rizik

Obsah činností a výstupy z jednotlivých fází jsou popsány v následujících kapitolách.

3.1 Fáze I – Stanovení kontextu řízení rizik

Účel: kontext pro posouzení rizik je stanoven na základě vyhodnocení všech relevantních informací pro řízení rizik, zejména **účelu hodnocení rizik, r**ozsah a hranice systému, v němž budou posuzována rizika.

Dále jsou v této fázi upřesněna **kritéria hodnocení rizik**:

I. Kritéria pro hodnocení rizik bezpečnosti informací – příloha č.3
II. Kritérium pro posuzování dopadů, hrozeb a zranitelností – příloha č.4
III. Kritérium pro akceptaci rizik – postup pro akceptaci rizika, příloha č.5
IV. Seznam relevantních hrozeb – referenční seznam hrozeb, příloha č.6
V. Seznam relevantních zranitelností – referenční seznam zranitelností, příloha č.7.

3.2 Fáze II – identifikace a hodnocení aktiv

Účel: posouzení hlavních „procesů“ zpracování informací v systému (organizaci) s cílem identifikovat „primární aktiva“, dále podpůrná aktiva a jejich vzájemné vazby. Všechna aktiva jsou hodnocena z hlediska požadavků na důvěrnost, integritu a dostupnost.

Postup identifikace a hodnocení aktiv je stanoven metodikou „Identifikace a hodnocení aktiv“.

Výstupem z této fáze jsou seznam primárních a podpůrných aktiv, včetně určení jejich garantů:

I. Seznam primárních aktiv + jejich garanti + hodnocení důležitosti těchto aktiv
II. Seznam podpůrných aktiv + jejich garanti + hodnocení důležitosti těchto aktiv

Výše uvedené údaje jsou uloženy v tabulce **„VAVAI_AKTIVA“ (tabulka Excel).**

3.3 Fáze III – Identifikace rizik

Účel: Identifikace a hodnocení hrozeb a zranitelností a jejich dopadů na aktiva organizace. V průběhu identifikace rizik jsou využívány předem odsouhlasené seznamy relevantních hrozeb a zranitelností. Poznámka – u každého aktiva se posuzuje úroveň hrozby, zranitelnosti a možných dopadů.

V rámci této fáze se jedná o:

a. **Identifikaci a posouzení hrozeb** – identifikace hrozeb (příp. jejich příčiny) vůči jednotlivým primárním aktivům. Hrozby se „vybírají“ ze stanoveného referenčního seznamu hrozeb. Hrozby se hodnotí dle kritérií pro hodnocení hrozeb.
b. **Identifikaci stávajících opatření** – identifikace a zadokumentování stávajících bezpečnostních opatření. Cílem je usnadnit posouzení zranitelnosti aktiv vůči konkrétním hrozbám a dále aby nedocházelo k „duplikování“ opatření, která by byla navrhována k ošetření rizik.
   Poznámka – tento krok není nezbytný v případě využitelné dokumentace nebo při opakované analýze.
c. **Identifikaci a posouzení zranitelností** – identifikace zranitelností, které by mohly být zneužity hrozbami – s dopadem na aktiva. Zranitelnosti se „vybírají“ ze schváleného referenčního seznamu zranitelností. Zranitelnosti se hodnotí dle kritérií pro hodnocení zranitelností.
d. **Identifikace a posouzení dopadů** – hodnocení případných dopadů (následků) v případě uplatnění identifikovaných hrozeb a zranitelností v případě bezpečnostního incidentu. Dopady se hodnotí dle tabulky pro hodnocení dopadů.
e. **Výpočet rizika** – na základě údajů týkající se dopadů, hrozeb a zranitelností je provedeno stanovení rizika. Zpravidla se použije následující funkce (vzorec) pro výpočet rizika:

   R = Ha x Zr x Do x Hr

   kde je R ….. míra rizika
   Ha ….. hodnota aktiva
   Zr ……. zranitelnosti
   Do ……. dopad
   Hr ….. hrozba

Výstupy z této fáze procesu hodnocení rizik jsou následující:

I. Stanovení úrovně dopadů, hrozeb a zranitelností (pracovní data)
II. Určená míra rizika bezpečnosti informací pro jednotlivá aktiva

Výše uvedené údaje jsou uloženy v tabulce **„VAVAI_RIZIKA“ (tabulka Excel, samostatný soubor).**

3.4 Fáze IV – Analýza rizik

Účel: posouzení všech údajů získaných v předchozích fázích, analyzovat identifikovaná rizika bezpečnosti informací. Analýza rizik probíhá v souladu s kritérii pro hodnocení rizik.

Poznámka – úroveň rizika též ovlivňuje pravděpodobnost vzniku incidentu, tj. uplatnění hrozby a případné následky (dopady) v daném scénáři incidentu, berou s v úvahu informace o primárních aktivech, o procesech organizace a případně další relevantní informace.

V rámci této fáze se jedná o:

a. **Analýzu rizik ve vztahu k primárním a podpůrným aktivům** – na základě identifikované míry rizika se posuzují pravděpodobné scénáře incidentů a jejich možné dopady na organizaci. Stanovují se priority mezi riziky, řadí se podle jejich významnosti.

3.5 Fáze V – Vyhodnocení rizik

Účel: posouzení jednotlivých rizik a jejich porovnání s kritérii hodnocení rizik a závěrů z analýzy rizik. Hodnocení probíhá v souladu s kontextem řízení rizik, berou se v úvahu cíle společnosti, možné

následky, pravděpodobnost uplatnění hrozby a další faktory, např. větší množství malých rizik může vyústit v daleko větší celkové riziko.

Manažer KB IS VaVaI schvaluje vyhodnocení rizik a akceptuje zbytková rizika.

Výstupem z této etapy je:

a. **Hodnocení rizik** – jsou vyhodnocena rizika z hlediska jejich závažnosti, stanovena jejich priorita, ….
b. **Zpráva z hodnocení rizik** – výstupní dokument z procesu hodnocení rizik.

3.6 Fáze VI – Ošetření rizik

Účel: na základě vyhodnocení rizik bezpečnosti informací je navržen způsob ošetření jednotlivých rizik a následně stanovena konkrétní opatření. Viz kapitola „Ošetření rizik“.

4 ZPRÁVA Z HODNOCENÍ RIZIK

Zpráva z posouzení rizik obsahuje níže uvedené údaje (šablona je uvedena v samostatném souboru):

1) Způsob a účel provedení hodnocení rizik
2) Rozsah hodnocení rizik
3) Použitá metodika hodnocení rizik (odkaz na …)
4) Identifikovaná primární a podpůrná aktiva (odkaz na přílohu …)
5) Identifikovaná rizika (odkaz na tabulku …)
6) Hodnocení rizik (výsledky hodnocení
7) Doporučení k ošetření rizik
8) Doporučení k akceptaci „zbytkových“ rizik
9) Závěr
10) Přílohy (tabulka aktiv, tabulka rizik, metodika – dle konkrétní potřeby).

Šablona zpráva z hodnocení rizik je uvedena v samostatném souboru

5 DOPORUČENÍ K OŠETŘENÍ RIZIK

Ošetření rizik je samostatný proces, který navazuje na výsledky hodnocení rizik, resp. z něj vychází. Hlavním cílem tohoto procesu je navrhnout způsoby ošetření jednotlivých rizik na základě posouzení významu rizika a možností organizace na ošetření rizika.

Dalším krokem při ošetření rizik je, na základě rozhodnutí o způsobech ošetření rizik, bezpečnostních potřeb a výsledků hodnocení rizik, navržení konkrétních bezpečnostních opatření, která jsou souhrnně uvedena v **Prohlášení o aplikovatelnosti**, obsahující přehled vybraných a zavedených bezpečnostních opatření v organizaci.

Pro nově identifikovaná a nepřijatelná rizika se zpracuje a následně realizuje **plán zvládání rizik**, který obsahuje:

- Bezpečnostní opatření ke zvládání určených rizik,
- určení osob zajišťující prosazování bezpečnostních opatření,
- potřebné finanční, technické, lidské a informační zdroje,
- termín jejich zavedení,

Do plánu zvládání rizik jsou nově přijímaná opatření průběžně doplňována a již zavedená opatření jsou při aktualizaci či re-analýze rizik přesunována do prohlášení o aplikovatelnosti.

Na základě výsledků vyhodnocení rizik bezpečnosti informací jsou definovány **cíle bezpečnosti informací**, které mají být dosaženy v rámci ISMS. Pro každý cíl bezpečnosti informací se určí: co má být dosaženo, předpokládané zdroje k jejich naplnění, kdo bude odpovědný, plánovaný termín splnění. Z definování cíle bezpečnosti musí být zřejmé, jakým způsobem bude hodnoceno dosažení cíle.

Formulář pro zaznamenávání cílů je uveden v příloze č. 9.

6 PŘÍLOHY

Příloha č. 1 – Rozsah a hranice hodnocení rizik

Příloha č. 2 – Kritérium pro hodnocení rizik

Příloha č. 3 – Kritéria pro akceptaci rizik

Příloha č. 4 – Kritéria pro posuzování hrozeb, zranitelností a dopadů

Příloha č. 5 – Referenční přehled hrozeb

Příloha č. 6 – Referenční přehled zranitelností

Příloha č. 7 – Seznam primárních aktiv (šablono údajů)

Příloha č. 8 – Seznam podpůrných aktiv (šablona údajů)

Příloha č. 9 – Cíle bezpečnosti informací

Příloha č. 1 – Rozsah a hranice hodnocení rizik

Rozsah posouzení rizik bezpečnosti informací, příp. i rozsah systému řízení bezpečnosti informací, se se doporučuje definovat uvedením potřebných skutečností (tzn. „co spadá do rozsahu“) v následujících oblastech:

1. **Z hlediska organizační struktury organizace** – organizační součásti, které spadají do řízení rizik.
2. **Z hlediska hlavních procesů (činností) organizace** – procesy, které spadají do systému řízení rizik.
3. **Z hlediska místa dislokace (lokality)** - lokality (přesnou adresou), které spadají do systému.
4. **Z hlediska informačních systémů** – IS využívaných poskytování služeb koncovému uživateli.
5. **Z hlediska informačních technologií** – ICT technologie (sítě, servery, datová úložiště, komunikační sítě, …), padající do systému, tzn., jsou potřebné pro podporu výše uvedených procesů a primárních aktiv.
6. **Z hlediska služeb externích subjektů** – služby externích subjektů, významné pro bezpečnost informací, spadající do systému řízení rizik.

6.1 Příloha č. 2 – Kritérium pro hodnocení rizik

Pro vyhodnocení míry rizika je využita následující stupnice:

Stupnice pro hodnocení rizik		
Úroveň	Číselná hodnota	Popis
Nízké	1–64	Riziko je považováno za přijatelné (akceptovatelné).
Střední	65 (96) - 256	Riziko může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti proti-opatření může být riziko přijatelné.
Vysoké	257 (576) - 2048	Riziko je dlouhodobě nepřípustné a musí být zahájeny systematické kroky k jeho odstranění
Kritické	2049–4096	Riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění.

6.2 Příloha č. 3 – Kritéria pro akceptaci rizik

Metodikou hodnocení rizik jsou stanovena pouze základní kategorie pro akceptaci rizik, které nastavují škály pro úrovně akceptace rizik. Riziko je nezbytné posuzovat dle konkrétního případu, v kontextu s ostatními riziky a jednotlivě zvažovat důvody pro jejich akceptaci.

Kritéria pro akceptaci rizik se mohou v čase lišit, tzn., že mohou být proměnná v různých situacích.

Při akceptaci rizik je nezbytné přihlédnout též k právním a regulačním aspektům pro danou oblast, použitým technologiím, provozním faktorům, ekonomickým faktorům, …

Základní kritéria pro akceptaci rizik (při využití dané metodiky hodnocení rizik) jsou:

a. Hodnota vypočteného rizika u daného aktiva je nižší než 64;
b. Dané riziko nesouvisí s naplněním právních a regulatorních předpisů, resp. jeho akceptace neznamená přímé porušení povinnosti vyplývající z těchto předpisů;
c. Dané riziko nesouvisí s primárním aktivem, jehož hodnota byla v některých aspektech (Důvěrnost/Integrita/Dostupnost) hodnocena jako kritická (číselná hodnota 4);

Návrh na akceptaci rizika podává Manažer KB IS VaVaI; k akceptaci rizika se vyjadřuje Rada VVI. Výsledné rozhodnutí o akceptaci rizika provádí vedení organizace.

6.3 Příloha č. 4 – Kritéria pro posuzování hrozeb, zranitelností a dopadů

Níže uvedené tabulky obsahují kritéria pro hodnocení dopadů, hrozeb a zranitelností ve vztahu k primárním a ostatním aktivům.

A) Stupnice pro hodnocení dopadů			
Úroveň	ID	ZKB	Obecná kritéria
Nízký	1	Dopad je v omezeném časovém období a malého rozsahu a není závažný na činnost systému. Rozsah případných škod nepřesahuje finanční nebo materiální ztráty řádově tisíce Kč.	Dopad na aktivum/organizaci je zanedbatelný. Z hlediska: - organizačního – nevýznamný - poškození aktiva = do 1-5% - výpadku služby = do 1-3 hodiny - finančního = řádově tisíce Kč Kritérium dostupnosti: nedostupnost je akceptována do 1 týden
Střední	2	Dopad je omezeného rozsahu a v omezeném časovém období. Rozsah případných škod se pohybuje do 10–100 tis. Kč, nemá závažný vliv na činnost společnosti a poskytování služeb.	Dopad na aktivum je znatelný až přechodné problémy, neposkytování služby v plném rozsahu. Z hlediska: - organizačního – znatelný, přechodně akceptov. - poškození aktiva = do 10–20% - výpadku služby = do 4-8 hodin - finančního = 10–100 tisíc Kč Kritérium dostupnosti: nedostupnost je akceptována do řádově dny, max. 2-3 dny
Vysoký	3	Dopad je sice omezeného rozsahu, ale trvalý nebo závažný. Rozsah případných škod se pohybuje do 500 tis. Kč anebo představuje závažné omezení poskytování služeb společnosti.	Dopad na aktivum je – krátkodobě vážné problémy, nefunkčnost služby. Z hlediska: - organizačního – přechodné problémy - poškození aktiva = do 50% - výpadku služby = do 1 týdne - finančního = statisíce, max. do 500 tisíc Kč Kritérium dostupnosti: nedostupnost je akceptována do řádově hodin, max. 4–8 hodin
Kritický	4	Dopad je plošný rozsahem, trvalý a velmi závažný. Rozsah případných škod (finančních nebo materiálních) se pohybuje v řádu statisíců Kč anebo představuje závažné až trvalé zamezení poskytování služeb společnosti.	Dopad na aktivum je – dlouhodobé vážné problémy, nefunkčnost a neposkytování služby. Z hlediska: - organizačního – kritický, vážné problémy - poškození aktiva => 50% - výpadku služby => 1 týden - finančního = řádově statisíce, nad 500 tis. Kč Kritérium dostupnosti: nedostupnost je akceptována v řádově minuty, max. 1 hodina

B) Stupnice pro hodnocení hrozeb (výskytu hrozby)		
Úroveň	ID	Popis
---	0	Hrozba není relevantní pro aktivum
Nízká	1	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.
Střední	2	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let, např. jednou ročně.
Vysoká	3	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce či 2 měsíců, např. asi jednou měsíčně.
Kritická	4	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc, např. denně, opakující se, případně trvale.

C) Stupnice pro hodnocení zranitelností		
Úroveň	ID	Popis
Nízká	1	Zranitelnost neexistuje nebo je zneužití zranitelnosti málo pravděpodobné. Jsou zavedena bezpečnostní opatření, které jsou schopna včas detekovat možné slabiny nebo případné pokusy o překonání opatření. Stupeň poškození aktiva – malé až zanedbatelné (1% - 5%)
Střední	2	Zneužití zranitelnosti je málo pravděpodobná až pravděpodobná. Jsou zavedena bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné slabiny nebo případné pokusy o překonání opatření je omezena. Nejsou známé žádné úspěšné pokusy o překonání bezpečnostních opatření. Stupeň poškození aktiva – střední (20%)
Vysoká	3	Zneužití zranitelnosti je pravděpodobná až velmi pravděpodobné. Bezpečnostní opatření jsou zavedena, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známé dílčí úspěšné pokusy o překonání bezpečnostních opatření. Stupeň poškození aktiva – vysoké (50%)
Kritická	4	Zneužití zranitelnost je velmi pravděpodobné až víceméně jisté. Bezpečnostní opatření nejsou realizována anebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známé úspěšné pokusy překonání bezpečnostních opatření. Stupeň poškození aktiva – těžké až úplná destrukce (více jak 80%)

6.4 Příloha č. 5 – Referenční přehled zranitelností

Referenční přehled zranitelností vychází z doporučení vyhlášky č. 82/2014 Sb.

Typ	Zranitelnosti	Poznámka
1.	nedostatečná údržba informačního a komunikačního systému,	
2.	zastaralost informačního a komunikačního systému,	
3.	nedostatečná ochrana vnějšího perimetru,	
4.	nedostatečné bezpečnostní povědomí uživatelů a administrátorů,	
5.	nedostatečná údržba informačního a komunikačního systému,	
6.	nevhodné nastavení přístupových oprávnění,	
7.	nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,	
8.	nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování,	
9.	nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí,	
10.	nedostatečná ochrana aktiv,	
11.	nevhodná bezpečnostní architektura,	
12.	nedostatečná míra nezávislé kontroly,	
13.	neschopnost včasného odhalení pochybení ze strany zaměstnanců.	

6.5 Příloha č. 6 – Referenční přehled hrozeb

Referenční přehled hrozeb vychází z doporučení vyhlášky č. 82/2014 Sb.

Id	Příklady hrozeb	Poznámka
1.	porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů,	
2.	poškození nebo selhání technického anebo programového vybavení,	
3.	zneužití identity,	
4.	užívání programového vybavení v rozporu s licenčními podmínkami,	
5.	škodlivý kód (například viry, spyware, trojské koně),	
6.	narušení fyzické bezpečnosti,	
7.	přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie,	
8.	zneužití nebo neoprávněná modifikace údajů,	
9.	ztráta, odcizení nebo poškození aktiva,	
10.	nedodržení smluvního závazku ze strany dodavatele,	
11.	pochybení ze strany zaměstnanců,	
12.	zneužití vnitřních prostředků, sabotáž,	
13.	dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb,	
14.	nedostatek zaměstnanců s potřebnou odbornou úrovní,	
15.	cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik,	
16.	zneužití vyměnitelných technických nosičů dat,	
17.	napadení elektronické komunikace (odposlech, modifikace).	

6.6 Příloha č. 7 – Seznam primárních aktiv

Seznam primárních aktiv je veden formou tabulky (Excel), která má následující strukturu:

Id.	Položka	Popis položky
1.	Id	Pořadové číslo položky
2.	Název aktiva	Název aktiva
3.	Hodnota – důvěrnost	Uvádí se hodnota požadavků na důvěrnost aktiva – dle kritérií <1–4>
4.	Hodnota – integrita	Uvádí se hodnota požadavků na integritu aktiva – dle kritérií <1–4>
5.	Hodnota – dostupnost	Uvádí se hodnota požadavků na dostupnost aktiva – dle kritérií <1–4>
6.	ID odboru	Označení odboru, do jehož kompetence spadá primární aktivum
7.	Garant aktiva	Jméno vedoucího pracovníka v roli „garanta aktiva“
8.	Hodnota aktiva	Výpočet – součin v položkách 3 x 4 x 5
9.	Používá IS	Uvede se ID SW (1 až n), který je využíván pro zpracování daného aktiva, využívá se seznam z podpůrných aktiv
10.	Přípustné použití aktiva	Odkaz na řídicí dokumentaci, kde jsou dokumentována pravidla přípustného použití aktiva
11.	Využívá lidské zdroje	Odkaz na kategorii lidských zdrojů, související se zpracování daného aktiva. Uvádí se ID ze seznamu v podpůrných aktivech, záložka „Lidé“.

6.7 Příloha č. 8 – Seznam podpůrných aktiv

Seznam primárních aktiv je veden formou tabulky (Excel), která má následující strukturu:

Id.	Položka	Popis položky
1.	Id	Pořadové číslo položky
2.	Název aktiva	Název aktiva
3.	Hodnota – důvěrnost	Uvádí se hodnota požadavků na důvěrnost aktiva – dle kritérií <1–4>
4.	Hodnota – integrita	Uvádí se hodnota požadavků na integritu aktiva – dle kritérií <1–4>
5.	Hodnota – dostupnost	Uvádí se hodnota požadavků na dostupnost aktiva – dle kritérií <1–4>
6.	ID odboru	Označení odboru, do jehož kompetence spadá primární aktivum
7.	Garant aktiva	Jméno vedoucího pracovníka v roli „garanta aktiva“
8.	Hodnota	Výpočet – součin v položkách 3 x 4 x 5

	aktiva	
9.	Dodavatel	Uveden se poskytovatel služby, dodavatel HW / SW, …
10.	Přípustné použití aktiva	Odkaz na řídicí dokumentaci, kde jsou dokumentována pravidla přípustného použití aktiva
11.	Id primárního aktiva	Odkaz na ID primárního aktiva, které je tímto podpůrným aktivem zpracováváno.

Podpůrná aktiva jsou sledována v následujících kategoriích:

1) **Informační systémy,** resp. aplikace, může být dále členěno na:
   - Operační systémy a databázové systémy,
   - Aplikační vybavení (aplikace),
2) **HW –** veškeré HW prostředky pro zpracování dat, mohou být dále členěny na:
   - Servery a další centrální prostředky,
   - Koncová zařízení pro uživatele (pracovní stanice / notebooky)
   - Síťová zařízení – prostředky pro přenos informací, kabeláž
3) **Podpůrná zařízení** (UPS, klimatizace, rozvody elektřiny, …)
4) **Budovy a jejich infrastruktura**
5) **Lidé** (v různých rolích – uživatelé, administrátoři, ….)
6) **Služby** poskytované externími subjekty

6.8 Příloha č. 6 - Cíle bezpečnosti

Formulář pro stanovení cílů bezpečnosti

Cíle bezpečnosti stanovené pro období od …… do…….

Cíl bezpečnosti (formulace)	Cílová hodnota / parametry cíle / zdroje	Vlastník cíle ISMS	Termín / Hodnocení výsledku

Schválil:

Datum: