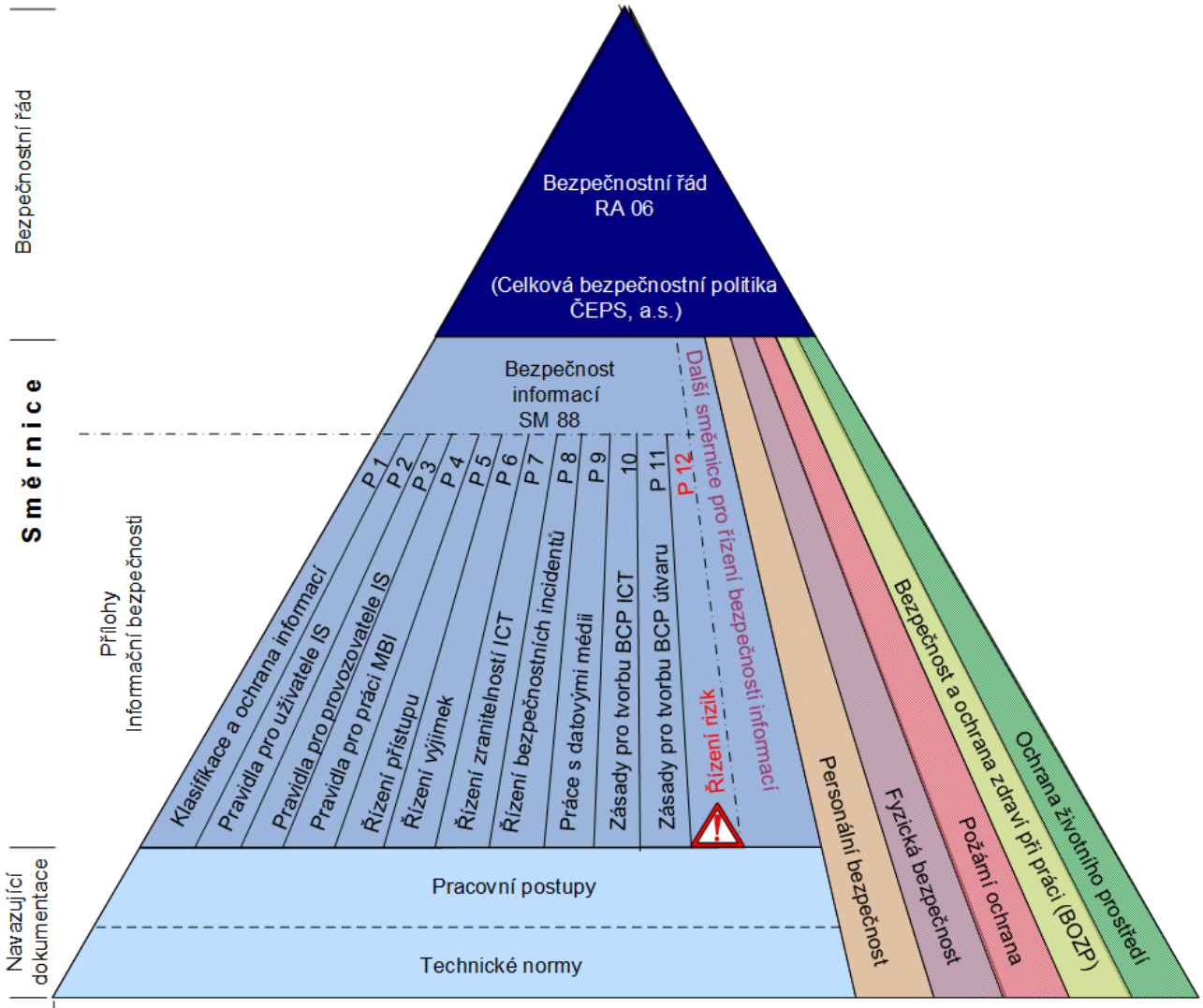
# ŘÍZENÍ RIZIK BEZPEČNOSTI INFORMACÍ

## Zařazení a působnost ve struktuře bezpečnostní dokumentace




| dokument / působnost | Klasifikace a ochrana informací | Pravidla pro uživatele IS | Pravidla pro provozovatele IS | Pravidla pro práci MBI | Řízení přístupu | Řízení výjimek | Řízení zranitelnosti ICT | Řízení bezp. incidentů | Práce s datovými médii | Zásady pro tvorbu BCP ICT | Zásady pro tvorbu BCP útvaru | Řízení rizik |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| uživatel IS | X | X | | | | | | | | | | |
| provozovatel IS | X | X | X | X | X | | X | X | X | X | | X |
| MBI | X | X | | X | X | X | X | X | X | X | X | X |
| vedoucí útvaru | X | X | | | | | | | | | X | X |
| personalista | X | X | | | X | | | | | | | |
| externí subjekt | X | X | X*) | | X*) | | | | | | | |

*) *Platí pro externí subjekty v roli správců/administrátorů/vývojářů IS*

*Pozn.: Uvedené názvy nejsou přesnými názvy příloh.*

**OBSAH:**

1 Účel, působnost a odpovědnost ..... 3
1.1 Role, odpovědnosti a pravomoci ..... 3
2 definice základních pojmů a zkratek ..... 3
3 Řízení rizik IS ..... 3
3.1 Metodika RAMSES ..... 4
3.2 Identifikace a rozdělení aktiv ..... 4
3.3 Hodnocení datových aktiv ..... 5
3.4 Hodnocení ostatních aktiv ..... 6
3.5 Hodnocení hrozeb a zranitelností ..... 6
3.6 Výpočet velikosti rizik ..... 7
3.7 Kritéria přijatelnosti rizik ..... 8
3.8 Zvládání rizik ..... 9
3.9 Výjimky bezpečnosti informací ..... 10

# 1 ÚČEL, PŮSOBNOST A ODPOVĚDNOST

Tato příloha ke směrnici „Bezpečnost informací“ zavádí systém řízení rizik bezpečnosti informací (dále v textu také zkráceně „řízení rizik“) a stanovuje metodiku a přístup k jejich identifikaci, hodnocení a zvládání.

Cílem je řízení rizik s ohledem na poslání, cíle a činnosti společnosti.

Účelem směrnice je:

- nastavit efektivní proces a metodiku řízení rizik,
- zajistit identifikaci a rozdělení aktiv,
- zajistit hodnocení aktiv, hrozeb, zranitelností a výpočet velikosti rizik,
- stanovit kritéria přijatelnosti rizik,
- zajistit zvládání rizik.

Tato příloha ke směrnici „Bezpečnost informací“ a popsaný proces řízení rizik bezpečnosti informací vycházející z mezinárodních norem ISO/IEC 27001 a ISO/IEC 27005 je závazná pro všechny zaměstnance ČEPS v roli vedoucích zaměstnanců, vrcholového managementu, členů představenstva, provozovatelů IS a manažera bezpečnosti informací (MBI).

## 1.1 Role, odpovědnosti a pravomoci

Odpovědnosti a pravomoci jsou stanoveny v SM 88.

# 2 DEFINICE ZÁKLADNÍCH POJMŮ A ZKRATEK

**Podpůrné aktivum** – Nastavení SW nebo HW, aby vytvářel auditní záznamy s informacemi o aktivitách aktivních prvků infrastruktury, aplikací a uživatelů, podle nichž mohou být důsledky těchto činností přiřazeny těmto uživatelům, kteří jsou za ně odpovědní.

**Primární aktivum** – Primárním aktivem je informace nebo služba, kterou zpracovává nebo poskytuje významný informační systém.

**Přijatelné (akceptovatelné) riziko** – riziko zbývající po uplatnění bezpečnostních opatření, jehož úroveň odpovídá kritériím pro přijatelnost rizik.

Další související definice jsou uvedeny v SM 88.

# 3 ŘÍZENÍ RIZIK BEZPEČNOSTI INFORMACÍ

Řízení bezpečnosti informací společnosti ČEPS je založeno na řízení rizik bezpečnosti informací.

Celkově je za zajištění fungování procesu řízení rizik odpovědný manažer bezpečnosti informací (MBI). Nezbytnou součinnost musí v jednotlivých fázích poskytovat dotčené subjekty, jedná se především o garanty (vlastníky) aktiv a zaměstnance ustanovené v jednotlivých rolích ISMS. Všichni zaměstnanci společnosti jsou povinni aktivně spolupracovat při provádění hodnocení rizik, tzn. včasně poskytnout vstupní informace pro hodnocení rizik, zejména informace o hodnotách aktiv, hodnocení hrozeb a zranitelností a o aktuálním stavu bezpečnostních opatření.

Přezkoumání hodnocení rizik musí být prováděno v pravidelných intervalech nejméně jednou ročně, detailní hodnocení rizik pak s maximální periodou tří let nebo v případě podstatných změn v rozsahu ISMS či změn v požadavcích na bezpečnost informací.

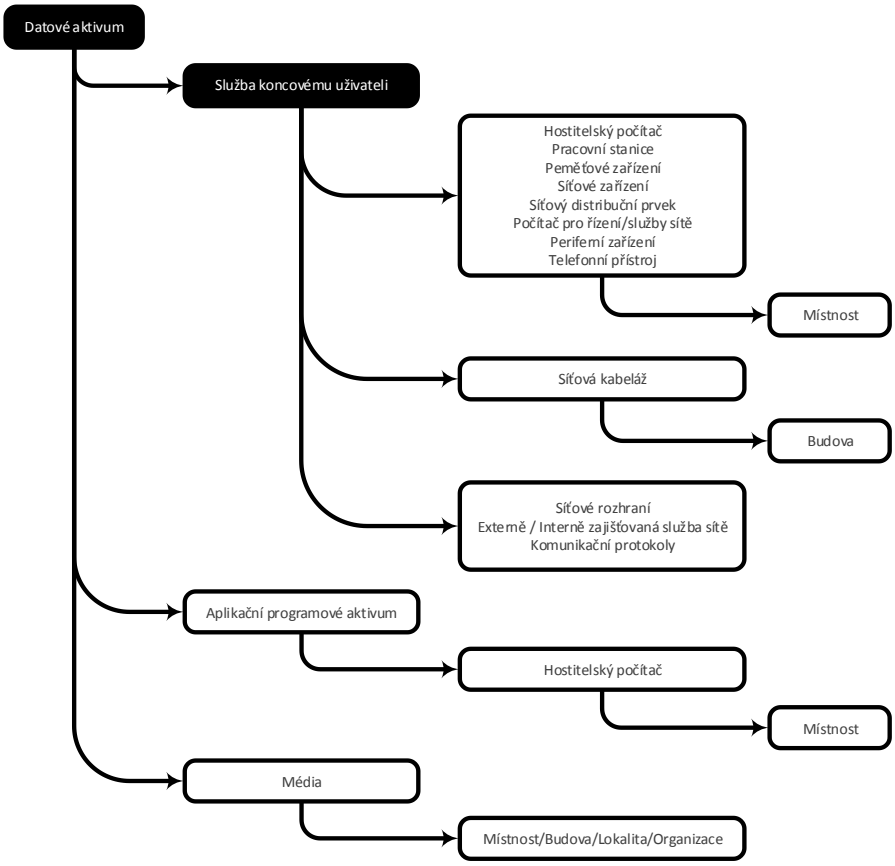
Výsledky hodnocení rizik musí sloužit k volbě odpovídajících kroků a priorit pro řízení bezpečnostních rizik a pro realizaci opatření určených k zamezení jejich výskytu.

## 3.1 Metodika RAMSES

Společnost ČEPS používá pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik včetně stanovení kritérií pro přijatelnost (akceptovatelnost) rizik metodiku RAMSES (metodika RAMSES vychází z mezinárodně uznávané metodiky CRAMM), která zajišťuje, že hodnocení rizik (tj. identifikace, analýza a vyhodnocení rizik) je prováděno komplexně a metodicky správně a výsledky jednotlivých hodnocení rizik jsou porovnatelné a reprodukované v čase. Metodika RAMSES je v potřebném rozsahu promítnuta do metodiky řízení rizik IS ve společnosti ČEPS. Metodika je v souladu s doporučeními ISO/IEC 27005, požadavky certifikační normy ISMS ISO/IEC 27001 a ZoKB. Metodika je také základem webové aplikace RAMSES, která slouží k efektivnějšímu využívání metodiky RAMSES a k prezentaci výsledů hodnocení rizik a stavu bezpečnosti v prostředí ČEPS.

## 3.2 Identifikace a rozdělení aktiv

Základem metodiky RAMSES je rozdělení aktiv na primární a podpůrná.




*Obrázek 1 Obecný model aktiv (primární aktiva jsou zvýrazněna černě)*

Analyzované informační systémy ČEPS jsou (v souladu s metodikou RAMSES) tvořeny několika kategoriemi aktiv. Níže jsou uvedeny jednotlivé kategorie aktiv a aktiva, která do kategorií spadají:

- datová aktiva – data a informace,
- služby koncovému uživateli – služby poskytované informačním systémem,
- fyzická aktiva – technické vybavení vč. systémového programového vybavení, komunikace,
- aplikační programová aktiva – programové vybavení,
- prostory – lokality, budovy, místnosti.

Všechna uvedená aktiva mají pro ČEPS určitou hodnotu, která je klíčovým faktorem pro stanovení úrovně bezpečnosti vyžadované pro informační systém(y).

Vztahy, kterými jsou jednotlivá aktiva vázána, jsou definovány pomocí tzv. modelů aktiv (viz *Obrázek 1*). Model aktiv definuje závislosti mezi různými typy aktiv a umožňuje stanovit následně vhodná protiopatření pro datová aktiva, služby informačního systému, fyzická aktiva, aplikační programová aktiva a jejich umístění.

### 3.3 **Hodnocení datových aktiv**

Hodnocení datových (informačních) aktiv probíhá formou interview s garanty aktiv, kteří jsou odpovědní za hodnocená datová aktiva. Interview vede manažer bezpečnosti informací (dále MBI), popř. jím určený zástupce.

Každý respondent je v úvodu interview seznámen s cílem interview. Dále respondent popíše činnosti, v rámci kterých se s daty pracuje. Následně svými slovy popíše dopad na pracovní činnosti v rámci agendy, pokud budou data nedostupná, zničená, prozrazená, modifikovaná viz *Tabulka 1 Význam zkratek jednotlivých typů následků*. Při hodnocení dopadů jsou uvažovány nejhorší možné, ale stále ještě pravděpodobné scénáře.

| Výklad zkratek typů následků (dopadů) | | | |
|---|---|---|---|
| 15M | Nedostupnost dat – do 15 minut | C | Neoprávněné prozrazení smluvním poskytovatelům služeb |
| 1H | Nedostupnost dat – do 1 hodiny | O | Neoprávněné prozrazení cizím osobám |
| 3H | Nedostupnost dat – do 3 hodin | SE | Chyby menšího rozsahu |
| 12H | Nedostupnost dat – do 12 hodin | WE | Chyby většího rozsahu |
| 1D | Nedostupnost dat – do 1 dne | DM | Úmyslná modifikace |
| 2D | Nedostupnost dat – do 2 dnů | In | Vložení falešné zprávy |
| 1W | Nedostupnost dat – do 1 týdne | Or | Popření původu |
| 2W | Nedostupnost dat – do 2 týdnů | Rc | Popření přijetí |
| 1M | Nedostupnost dat – do 1 měsíce | Nd | Nedoručení |
| 2M | Nedostupnost dat – do 2 měsíců a více | Rp | Opakování |
| B | Ztráta dat od posledního zálohování | Mr | Chybné směrování |
| T | Úplná ztráta všech dat | Tm | Monitorování komunikačního provozu |

| Výklad zkratek typů následků (dopadů) | | | |
|---|---|---|---|
| I | Neoprávněné prozrazení identifikovatelným osobám | Os | Narušená posloupnost |

*Tabulka 1 Význam zkratek jednotlivých typů následků*

Záznamy z interview, včetně hodnocení datových aktiv, se zapisují do aplikace RAMSES (*https://ramses.rac.cz*).

Prostřednictvím vodítek hodnocení (viz *Příloha 2*) jsou následně MBI stanoveny hodnoty dopadů pro jednotlivá datová aktiva (kategorie dat a informací). Dopady jsou stanoveny v kvalitativní škále od 1 (nejmenší dopad) do 10 (nejhorší dopad). Výsledné hodnocení dopadů pro jednotlivá datová aktiva je zpracováno formou Zprávy o aktivech a dopadech.

### 3.4 Hodnocení ostatních aktiv

Hodnocení aplikačních programových aktiv – Aplikační programová aktiva podporují práci s datovými aktivy a ke své činnosti potřebují fyzická aktiva. Aplikační programová aktiva zahrnují krabicové, interně vyvíjené nebo zakázkové programové vybavení IS společnosti. Aplikační programová aktiva jsou hodnocena stejným způsobem jako fyzická aktiva, jejich hodnota je vyjádřena náklady na náhradu nebo obnovu.

Hodnocení fyzických aktiv – V metodice RAMSES je termín „fyzické aktivum“ používán pro všechny prvky informačního systému, které nemohou být označeny za datová aktiva ani za aplikační programová aktiva. Fyzická aktiva zahrnují technické vybavení, komunikační zařízení, systémy prostředí a dokumentaci v rámci IS, komunikační protokoly, pronajaté telekomunikační okruhy apod. Ocenění je vyjádřeno náklady na náhradu nebo úplnou obnovu fyzického aktiva. Fyzická aktiva následně nabývají (získávají na důležitosti) hodnoty odvozené z hodnoty datových aktiv a aplikačních programových aktiv, které podporují.

### 3.5 Hodnocení hrozeb a zranitelností

Hodnocení hrozeb a zranitelností je prováděno formou interview s respondenty (garanty aktiv). Jsou zkoumány všechny faktory, jejichž působení na systém může být příčinou určité úrovně hrozby nebo zranitelnosti.

Analýza hrozeb a zranitelností posuzuje mnoho potenciálních oblastí, kde každá může ovlivnit různé části informačních systémů ČEPS. Hrozby jsou seskupeny do následujících kategorií:

- Logické hrozby (6 hrozeb) – Zavedení destruktivních a škodlivých programů, Falšování uživatelské identity identifikovatelnými osobami, Falšování uživatelské identity cizími osobami, Falšování uživatelské identity smluvními poskytovateli služeb, Zneužití systémových prostředků, Neoprávněné použití aplikace,
- Komunikační hrozby (7 hrozeb) – Infiltrace komunikace, Zachycení komunikace, Manipulace komunikace, Odmítnutí odpovědnosti, Selhání komunikace, Začlenění škodlivých programů, Chybné směrování,
- Závady zařízení (12 hrozeb) – Selhání klimatizace, Selhání aplikačního programového vybavení, Selhání systémového nebo síťového programového vybavení, Selhání napájení, Technická závada síťového distribučního prvku, Technická závada síťové brány, Technická závada počítače, Technická závada síťového rozhraní, Technická závada síťové služby, Technická závada tiskového zařízení, Technická závada paměťového zařízení, Technická závada počítače pro řízení/správu sítě,

- Lidské chyby (4 hrozby) – Chyba údržby technického vybavení, Chyba úpravy programového vybavení, Chyba uživatele, Provozní chyba,
- Fyzické hrozby (9 hrozeb) – Požár, Poškození vodou, Přírodní katastrofa, Nedostatek personálu, Krádež provedená identifikovatelnými osobami, Krádež provedená cizími osobami, Terorismus, Úmyslné poškození identifikovatelnými osobami, Úmyslné poškození cizími osobami.

Úroveň hrozby je definována jako četnost výskytu hrozby. Úroveň zranitelnosti jako pravděpodobnost úspěchu hrozby. Úroveň hrozby je vyjádřena prostřednictvím pěti hodnot (viz Tabulka 2), úroveň zranitelnosti pak vyjádřena v níže uvedené třístupňové škále (viz Tabulka 3).

| Úroveň hrozby | Kritéria pro stanovení úrovně hrozby |
|---|---|
| Velmi nízká | Průměrný výskyt incidentu se nepředpokládá častěji než jednou za 10 let. |
| Nízká | Výskyt incidentu se předpokládá v průměru jednou za 3 roky. |
| Střední | Výskyt incidentu se předpokládá v průměru jednou za rok. |
| Vysoká | Výskyt incidentu se předpokládá v průměru jednou za 4 měsíce. |
| Velmi vysoká | Výskyt incidentu se předpokládá v průměru jednou měsíčně. |

*Tabulka 2 Škála pro stanovení úrovně hrozeb*

| Úroveň zranitelnosti | Kritéria pro stanovení úrovně zranitelnosti vůči hrozbě |
|---|---|
| Nízká | V případě incidentu by nebyla pravděpodobnost nejhoršího možného scénáře (stanoveného v průběhu ohodnocení aktiv) vyšší než 33%. |
| Střední | V případě incidentu by byla pravděpodobnost nejhoršího možného scénáře (stanoveného v průběhu ohodnocení aktiv) 33% až 66%. |
| Vysoká | V případě incidentu by byla pravděpodobnost nejhoršího možného scénáře (stanoveného v průběhu ohodnocení aktiv) vyšší než 66% |

*Tabulka 3 Škála pro stanovení úrovně zranitelnosti vůči hrozbě*

Záznamy z hodnocení hrozeb a zranitelností se zapisují do aplikace RAMSES.

### 3.6 **Výpočet velikosti rizik**

Míra (velikost) rizik se vypočítává maticovým výpočtem z hodnot aktiv (stanovených jako velikost dopadů v případě narušení bezpečnosti aktiva) a úrovně hrozby a zranitelnosti, viz *Tabulka 4*. Tento výpočet provádí aplikace RAMSES automaticky.

| Hrozba | | Velmi nízká | | | Nízká | | | Střední | | | Vysoká | | | Velmi vysoká | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Zranitelnost | | Nízká | Střední | Vysoká | Nízká | Střední | Vysoká | Nízká | Střední | Vysoká | Nízká | Střední | Vysoká | Nízká | Střední | Vysoká |
| Dopad | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 1 | 2 | 2 | 2 | 2 | 3 |
| | 2 | 1 | 1 | 2 | 1 | 2 | 2 | 2 | 2 | 3 | 2 | 3 | 3 | 3 | 3 | 4 |
| | 3 | 1 | 2 | 2 | 2 | 2 | 3 | 2 | 3 | 3 | 3 | 3 | 4 | 3 | 4 | 4 |
| | 4 | 2 | 2 | 3 | 2 | 3 | 3 | 3 | 3 | 4 | 3 | 4 | 4 | 4 | 4 | 5 |
| | 5 | 2 | 3 | 3 | 3 | 3 | 4 | 3 | 4 | 4 | 4 | 4 | 5 | 4 | 5 | 5 |
| | 6 | 3 | 3 | 4 | 3 | 4 | 4 | 4 | 4 | 5 | 4 | 5 | 5 | 5 | 5 | 6 |
| | 7 | 3 | 4 | 4 | 4 | 4 | 5 | 4 | 5 | 5 | 5 | 5 | 6 | 5 | 6 | 6 |
| | 8 | 4 | 4 | 5 | 4 | 5 | 5 | 5 | 5 | 6 | 5 | 6 | 6 | 6 | 6 | 7 |
| | 9 | 4 | 5 | 5 | 5 | 5 | 6 | 5 | 6 | 6 | 6 | 6 | 7 | 7 | 7 | 7 |
| | 10 | 5 | 5 | 6 | 5 | 6 | 6 | 6 | 6 | 6 | 6 | 7 | 7 | 7 | 7 | 7 |

*Tabulka 4 Matice rizik*

V metodice RAMSES je míra rizika vyjádřena ve stupnici 1 až 7. Hodnoty rizika jsou používány pro zvolení přiměřeného bezpečnostního protiopatření, které pokryje riziko. Míra rizika 1 až 3 znamená, že postačují pouze protiopatření z řady minimálních bezpečnostních opatření. Naopak hodnota 7 znamená, že musí být implementována velmi vysoká úroveň bezpečnosti. Pro slovní ohodnocení rizika je určena následující tabulka:

| Úroveň rizika | Slovní hodnocení rizika |
|---|---|
| 1 - 3 | Nízké až velmi nízké riziko |
| 4 | Střední riziko |
| 5 | Vysoké riziko |
| 6 - 7 | Velmi vysoké riziko |

*Tabulka 5 Úrovně rizik*

### 3.7 **Kritéria přijatelnosti rizik**

Ve společnosti ČEPS jsou stanovena následující kritéria pro přijatelnost (akceptaci) informačních rizik:

- hodnota rizika je v intervalu od 1 do 3 (tj. úroveň rizik, kde odhadované škody jsou natolik malé, že společnost ČEPC je schopná vyrovnávat se s nimi v každodenním provozu),
- náklady na zavedení a provozování opatření přesáhnou potenciální ztráty spojené s možnými následky výskytu rizika,
- velká obtížnost zavedení či provozování opatření,
- nedostupnost zdrojů (finančních, lidských nebo časových) na realizaci opatření,
- zavedení opatření není v souladu s prioritami činností nebo prostředím organizace.

V případech, kdy je naplněno jedno nebo více kritérii přijatelnosti rizika je možné rozhodnout o jeho akceptaci a být připraven vypořádat se s případnými negativními dopady výskytu rizika (nežádoucí události).

O akceptaci rizik rozhoduje vedení společnosti ČEPS na základě návrhu manažera informační bezpečnosti nebo vlastníka dotčeného procesu či aktiva.

Rozhodující slovo při stanovování přijatelnosti rizika má garant primárního aktiva.

Rizika, která nesplňují kritéria přijatelnosti rizika, musí podstoupit proces zvládání rizik.

Výsledky hodnocení rizik jsou uvedeny ve *Zprávě o analýze rizik*.

### 3.8 **Zvládání rizik**

Na základě zjištění získaných v rámci identifikace a hodnocení aktiv a stanovení velikosti rizika je s pomocí metodiky RAMSES a knihovny opatření RAMSES vytvořen doporučený bezpečnostní profil.

Tento profil je ve formě sady bezpečnostních opatření, jež jsou považována za nezbytná ke zvládání zjištěných rizik, a která jsou použitelná pro analyzované informační systémy ČEPS.

Na nejvyšší úrovni jsou opatření v knihovně seskupena do skupin podle oblastí bezpečnosti následovně:

- IT bezpečnost,
- komunikační bezpečnost,
- personální bezpečnost,
- administrativní bezpečnost,
- fyzická bezpečnost.

Všechna opatření plnící stejnou funkci (např. detekci požáru) jsou obsažena v jedné podskupině. Podskupiny opatření obsahují jak detailní, tak i obecné popisy opatření.

Každé opatření v knihovně RAMSES nese označení úrovně bezpečnosti nebo rozmezí úrovní bezpečnosti (resp. míry rizik, které je schopno pokrývat) na stupnici od 1 (velmi nízká) do 7 (velmi vysoká). Opatření např. mohou podle svého označení odpovídat úrovni (míře) bezpečnosti 1–3 nebo 2–4 nebo 5–7 apod.

Opatření jsou navržena do bezpečnostního profilu organizace, pokud míra rizika odpovídá rozmezí bezpečnostních úrovní příslušných opatření, ovšem za předpokladu, že je opatření vhodné pro daný typ aktiva.

U jednotlivých opatření jsou MBI ve spolupráci s dotčenými garanty aktiv (primárních i podpůrných) prostřednictvím webové aplikace RAMSES identifikovány následující stavy, viz *Tabulka 6*.

| Stav opatření | Popis |
|---|---|
| Zavedeno | Opatření je již zavedeno. |
| Návrh se realizuje | Byla zahájena práce na realizaci protiopatření, avšak nebyla dosud dokončena. |
| Doporučeno k realizaci | Opatření není zavedeno, ale je doporučeno jeho zavedení. |
| Diskutováno | Probíhá diskuze nad tím, zda opatření implementovat či nikoliv. |

| Stav opatření | Popis |
|---|---|
| Přeneseno | Odpovědnost za implementaci a případný provoz protiopatření byla delegována na jinou organizaci (outsourcing). |
| Pokryto jinak | Toto opatření není doporučeno, protože již existují jiná opatření, která odpovídajícím způsobem chrání aktiva proti zjištěným hrozbám. |
| Neaplikovatelné | Protiopatření není pro příslušné aktivum použitelné. |
| Akceptovat úroveň rizika | Přestože existuje doporučení ze strany metodiky RAMSES, bylo rozhodnuto, že opatření nebude implementováno. Důvody pro toto rozhodnutí by měly být zdokumentovány. |

Stav jednotlivých opatření je zaznamenán do *Prohlášení o aplikovatelnosti*.

Plán, kde je uveden harmonogram implementace doporučených opatření, je uveden v *Plánu zvládání rizik*.

### 3.9 **Výjimky bezpečnosti informací**

Situace, kdy stav nebo úroveň bezpečnosti informací řízeně[1] neodpovídá této metodice nebo související dokumentaci, musí být veden jako výjimka s omezenou dobou platnosti a s akceptací rizik plynoucích z této výjimky. Výjimka musí být schválena ředitelem sekce nebo výkonným ředitelem, do jehož působnosti dopady rizika patří. Řízením bezpečnostních výjimek je pověřen manažer bezpečnosti informací (Příloha 6 SM 88).

[1] Nejedná se o bezpečnostní incident, ale o řízený proces s akceptovatelnou mírou rizika.