Forpsi Cloud

Riadenie rizík pre bezpečnosť informácií

OBSAH

1 POJMY A DEFINICE

Tato kapitola obsahuje určité definice, které se považují za významné pro prezentaci modelu výpočtu a řízení rizik bezpečnosti informací.

***BIA (Business Impact Analysis – Analýza dopadu na podnikání)*:**

Analýza ekonomických, regulačních a reputačních dopadů na podnikání souvisejících se ztrátou důvěrnosti, integritou a dostupností informací spojených s daným procesem/službou a jejím přerušením.

Dostupnost:

Zajistit, aby v případě potřeby byly k dispozici potřebné informační systémy a údaje.

Řízení rizik pro bezpečnost informací

Soubor činností a obchodních procesů k určení, měření, zmírnění a sledování rizik spojených se ztrátou důvěrnosti, integrity a dostupnosti (CIA) dat a služeb.

Dopad:

Negativní důsledek výskytu jedné nebo více hrozeb pro společnost.

Incident:

Událost související s kybernetickou bezpečností, která má značnou pravděpodobnost ohrožení obchodních operací a bezpečnosti informací.

Integrita:

Jedná se o ochranu údajů a informací před změnami, ať už náhodnými nebo úmyslnými.

Hrozba:

Potenciální příčina (úmyslná nebo náhodná) incidentu, který by mohl poškodit systém nebo organizaci, což by mělo dopad na důvěrnost, integritu a dostupnost informací.

Hrozby mohou být:

- „Kybernetické“ hrozby – mají negativní dopad na společnost tím, že:
  - využívají informačního systému nebo jeho komponent (např.: útok hackerů);
  - provádějí činnosti správy informačního systému (např.: poškození interními pracovníky);
- „Nekybernetické“ hrozby – mají negativní dopad na IT systém společnosti tím, že:
  - mají přímý dopad na poskytování služeb informačních systémů (např. přírodní katastrofy, přerušení podpůrných služeb);
  - ovlivňují způsob řízení informačního systému (např. způsob implementace IT procesů).

Abychom mohli charakterizovat rizika spojená s každou hrozbou, musíme znát:

- Zranitelnosti částí informačního systému nebo místa, kde se mohou vyskytnout hrozby;
- Vystavení komponentů hrozbě, jinými slovy, jak snadné je hrozbu uskutečnit (například server, který poskytuje webovou službu zákazníkům, je více vystaven útokům prováděným přes internet);
- Typy důsledků - vzhledem k tomu, že některé hrozby mohou být „mostem“ pro jiné hrozby (například, neoprávněný přístup k webovému serveru může umožnit útočníkovi zcizení dat, ale také jejich smazání, změnu, provedení podvodů apod.).

Možnost nebo pravděpodobnost výskytu:

Možnost výskytu hrozby je definována jako pravděpodobnost, že dojde k hrozbě ovlivňující jedno nebo více aktiv informačních technologií, s důsledkem negativního dopadu na podnikání, v rámci určitého časového úseku.

Riziko bezpečnosti informací (dále jen „riziko“)

Kombinace pravděpodobnosti výskytu hrozby a dopadu na společnost ve vztahu k aktivům zahrnutým do analýzy. V závislosti na tom, kdy jsou měřena, lze rizika definovat jako:

- Potenciální nebo inherentní riziko (**rRp**):

  Představuje maximální riziko, kterému je dané aktivum vystaveno, pokud jde o možnost vzniku hrozby, která může mít dopad na ztrátu důvěrnosti, integrity nebo dostupnosti informací. Všechny složky zahrnuté do analýzy služby přispívají k určení inherentního rizika: procesy, aplikace, data, infrastruktura a v neposlední řadě také lidský faktor. [3]

  V podstatě je reprezentováno hodnotou, vypočítanou různými způsoby podle toho, která metodika je aplikována, na základě součtu všech hrozeb, kterým je aktivum vystaveno, a to s přihlédnutím k příslušným pravděpodobnostem výskytu a jejich dopadu.

  Jinými slovy je to riziko, kterému může být aktivum vystaveno kvůli své povaze a hrozbám s ním spojenými. Například počítač vystavený na veřejné síti bez jakýchkoli ochranných opatření.

- Zbytkové nebo konečné riziko (**rRf**):

  Představuje riziko, kterému může být služba vystavena po uplatnění protiopatření ke snížení inherentního rizika.

- Konečné přijatelné riziko (**rRfa**):

  Představuje maximální práh rizika, který je pro společnost přijatelný.

Všechny výše uvedené hodnoty rizika se považují za dynamické, protože se v průběhu času mění a jsou ovlivněny například těmito prvky:

- Vývoj hrozeb;
- Změna parametrů služeb;
- Změny právních ustanovení nebo navazujících předpisů;

- Organizační změny, které mohou mít dopad na slabá místa či na pravděpodobnost uskutečnění se hrozeb, nebo změnit následné dopady;
- Posílení nebo oslabení bezpečnostních opatření.

Základní rizika:

Rozumí se jimi kybernetická rizika bezpečnosti informací spojená s každým aktivem a každým rizikovým scénářem.

Důvěrnost:

Rozumí se jí ochrana údajů a informací za účelem zmírnění rizik spojených s neoprávněným přístupem k informacím nebo jejich používáním.

RPO (Recovery Point Objective – Bod obnovy dat):

Rozumí se jím přijatelná ztráta dat a označuje maximální dobu mezi posledním uložením dat z procesu a událostí, která způsobí zastavení procesu.

RTO (Recovery Time Objective – Doba obnovy chodu):

Rozumí se jí doba po události, během níž:

- musí být produkt nebo služba obnoveny, nebo
- musí být činnost obnovena, nebo
- musí být obnoveny zdroje.

Scénář rizika:

Kombinace dvou nebo více hrozeb, které je umožňují klasifikovat.

Zranitelnost:

Slabá stránka procesu, služby nebo aktiva, která pokud je zneužita jednou nebo více hrozbami, umožní narušení cílů bezpečnosti informací (důvěrnost, integrita a dostupnost). Příklady:

- Neoddělené sítě;
- Používání protokolů, které nejsou chráněny šifrováním;
- Operační systémy, které nejsou pravidelně aktualizovány;
- Databáze s nešifrovanými „citlivými“ údaji;
- Neaktualizované definice virů;
- Nekontrolovaný fyzický přístup;
- Nedostatek automatických protipožárních systémů;
- Nedostatečné záložní energetické systémy;
- apod.

2 HLAVNÍ REFERENČNÍ NORMY

V následujících odstavcích jsou popsané hlavní normy přijaté k zajištění toho, aby prováděné činnosti byly v souladu s mezinárodními osvědčenými bezpečnostními postupy.

2.1 Norma ISO/IEC 27001

Norma ISO/IEC 27001 představuje, jakožto mezinárodní bezpečnostní standard, skutečný příkladový model pro posuzování úrovně bezpečnosti informací, který je schopen analyzovat jak technologické, tak organizační komponenty, které přispívají k definování systému řízení bezpečnosti informací (ISMS).
Norma definuje požadavky na ISMS a pomáhá identifikovat, řídit a minimalizovat množství hrozeb, kterým jsou informace pravidelně vystavovány. Tato norma také stanovuje bezpečnostní kontroly, které mají být přijaty k ochraně informací tím, že je zajistí pro zúčastněné strany, včetně zákazníků organizace.

2.2 Norma ISO/IEC 27002

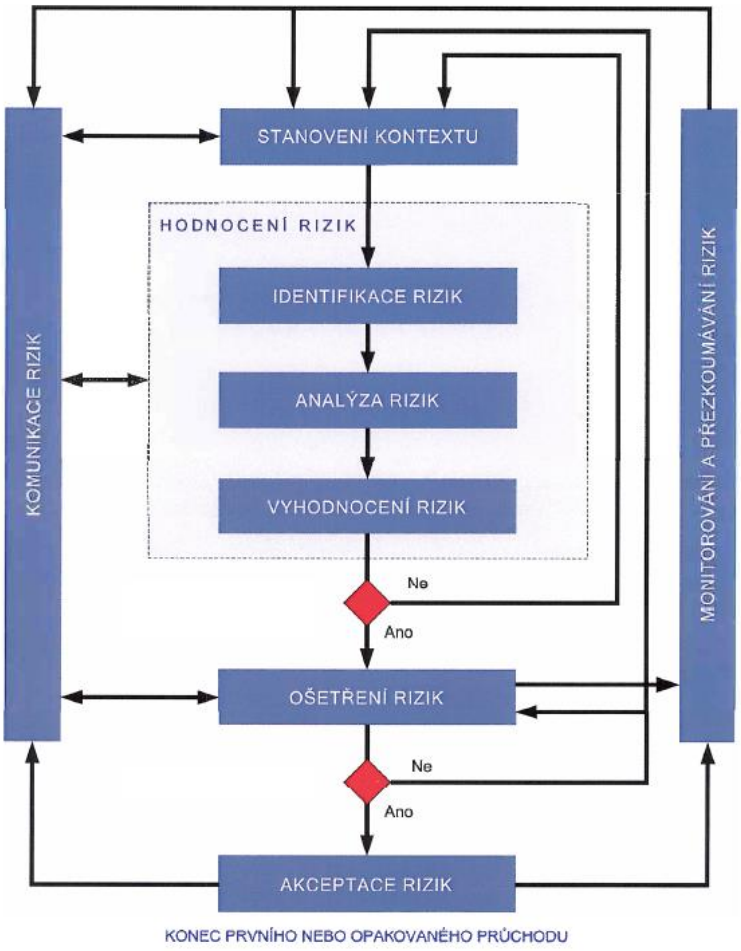
Norma ISO/IEC 27002 definuje směrnice a obecné zásady pro zavedení adekvátního systému řízení bezpečnosti informací v rámci organizace.
Norma ISO/IEC 27002 představuje mezinárodní bezpečnostní normu a skutečný standard pro posuzování organizačních, procedurálních, technologických a regulačních aspektů bezpečnosti informačního systému s cílem:

- Provádět kritické přezkoumání služeb a funkcí, které daný systém již má nebo by měl mít;
- Upozorňovat na zranitelnosti systému;
- Navrhovat vhodná opatření k dosažení úrovně bezpečnosti definované v cílech.

Je třeba poznamenat, že ISO/IEC 27002 identifikuje bezpečnostní kontroly, které by organizace měla zvážit, ale nenahrazuje samotnou analýzu rizik.

2.3 Norma ISO/IEC 27005

ISO/IEC 27005 popisuje proces řízení rizik bezpečnosti informací a související opatření, podporující obecné principy obsažené v ISO/IEC 27001.
Norma (v souladu s normou ISO 31000) je určena k tomu, aby pomohla společnostem řídit rizika v oblasti bezpečnosti informací podobným způsobem, jakým řídí jiné typy rizik.
Obrázek 1 ukazuje schéma procesu řízení rizik navržený normou ISO/IEC 27005:11, které inspiroval model přijatý a vyvinutý Skupinou Aruba.



Obrázek 1 – ISO/IEC 27005: Proces řízení rizik

3 METODIKA ŘÍZENÍ RIZIK V OBLASTI BEZPEČNOSTI INFORMACÍ

Pro Skupinu Aruba představuje informace aktivum, jehož pečlivé řízení je strategické pro ochranu a rozvoj podnikání společnosti.

V tomto kontextu lze kybernetické riziko definovat jako jakoukoli nejistou událost, která by mohla ohrozit jednu nebo více z následujících tří hlavních vlastností informačních aktiv společnosti:

- **D**ůvěrnost (údaje jsou přístupné neoprávněným osobám);
- **I**ntegritu (údaje mohou být předmětem neoprávněných úprav a mohou být změněny);

- **D**ostupnost (informační systém nelze použít);

v závislosti na úrovni závažnosti, která je úzce závislá na typu zasažených informací.

Posouzení rizik zohledňuje tyto možné typy dopadů:

- Ekonomické;
- Regulační;
- Reputační.

Řízení rizik v oblasti bezpečnosti informací je proces, který umožňuje hodnocení vzájemných vztahů mezi aktivy, hrozbami a zranitelnostmi v dané organizaci. Tento analytický proces si klade za cíl identifikovat rizika spojená se zranitelnostmi a hrozbami nalezenými v aktivech a poskytnout základ pro definování efektivního bezpečnostního programu.

Zvažované kategorie rizik musí být v souladu s typy použitelnými v daném kontextu. Zvažovaná rizika proto mohou vyplývat buď z vnitřních, nebo vnějších hrozeb, nebo hrozeb prostředí, jakož i z úmyslného jednání, nebo z nedostatečného organizačního řízení, či z nedbalosti jednotlivců.

Hodnota rizika je chápána jako funkce hodnoty dotyčných aktiv, hodnoty hrozeb a zranitelností.

Výsledky analýzy rizik jsou zdokumentovány a zahrnují:

- Jasné určení hlavních rizik,
- Posouzení potenciálních dopadů, které by každé z určených rizik mohlo mít na podnik;
- Plán doporučených opatření ke snížení rizik a jejich navrácení na přijatelnou úroveň.

Skupina Aruba zavádí model kvalitativní analýzy, protože ten může v krátkém čase poskytnout vysoký stupeň povědomí o hlavních informačně-bezpečnostních rizicích, které ovlivňují dané technologické prostředí.

Přijatá metodika je následující:

- Skupina používá příslušné metody k odhadu hodnoty informací v příslušných procesech a úrovně rizika, kterému jsou vystaveny, aby mohla být přijata vhodná ochranná opatření;
- Použijí se také při vývoji nových infrastrukturních nebo aplikačních řešení, která mají dopad na zabezpečení spravovaných údajů. V tomto případě metodika umožňuje posoudit, jak kritická jsou data a hrozby, kterým jsou vystavena, aby osoby odpovědné za analýzu rizik při vývoji a získávání informačních systémů mohly zavést vhodná ochranná opatření k minimalizaci zranitelností.

Posouzení rizik a analýza korelací mezi aktivy, hrozbami a opatřeními se provádí s podporou interně vyvinutého nástroje s využitím informací shromážděných během konkrétních setkání s různými jednotlivci zapojenými do analyzovaných procesů.

Používaná metodika umožňuje vytvořit obchodní model, kde jsou popsány všechny základní prvky potřebné pro následné analýzy spolu s jejich charakteristikami, jejich hierarchickou strukturou a souvisejícími vazbami.

4 PROCES ŘÍZENÍ RIZIK

Hlavní fáze modelu analýzy pro řízení rizik spojených s bezpečností informací přijaté a uplatňované Skupinou Aruba jsou popsány níže.

4.1 FÁZE 1 – stanovení souvislostí

Definice souvislostí pro analýzu zahrnuje modelování situace společnosti a identifikaci hlavních obchodních služeb, procesů, makro procesů a aktiv.

Při identifikaci zdrojů, jak navrhuje ISO/IEC 27005 „Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací“, se zvažují dva odlišné typy:

- **Primární zdroje** – informace, procesy, makro procesy a podnikatelské služby;
- **Sekundární zdroje nebo aktiva** – hardware, software, personál, síť, umístění a organizace.

4.1.1 Identifikace služeb, procesů a makro procesů

Při určování služeb a procesů organizace se jako výchozí reference používají organizační struktury publikované a zpřístupněné prostřednictvím interního nástroje podnikové komunikace.

Následně jsou jednotlivé procesy, které přispívají k poskytování služeb, seskupeny do makro procesů specifických pro analyzovaný kontext.

4.1.2 Určení aktiv

Abychom zajistili přesné určení aktiv, postupujeme podle následujících kroků:

1. **Určení kategorií** informačních aktiv (např. hardware, software, umístění atd.) podle klasifikačního systému definovaného v normě ISO/IEC 27005;
2. **Vážení kategorií** informačních aktiv podle bezpečnostní strategie společnosti a obchodních, právních a smluvních požadavků;
3. **Identifikace závislostí** mezi kategoriemi aktiv, která byla kategorizována.

4.1.3 Rodičovské vazby mezi makro procesy a aktivy

Jakmile jsou aktiva určena, definují se závislosti mezi nimi a makro procesy.

Tyto závislosti znamenají, že hodnoty dopadu CIA mohou být spojeny s každou kategorií aktiv (určené prostřednictvím rozhovorů BIA), takže lze vypočítat základní kybernetická rizika spojená s každým aktivem.

4.2 FÁZE 2 – Analýza rizik

4.2.1 Posuzování dopadů

Posuzování dopadů (Business Impact Analysis) se provádí v souladu s metodou přijatou jako doplněk k hlavním mezinárodním normám (ISO 27005, ISO 22301) obchodními zástupci.
Během fáze pohovoru BIA a s využitím interně vyvinutého nástroje pro shromažďování informací vedoucí různých oddělení společnosti posuzují ztrátu důvěrnosti, integrity a dostupnosti informací spravovaných v rámci své oblasti působnosti z hlediska ekonomického, regulačního a reputačního dopadu podle definovaných hodnotících stupnic.

Jak je uvedeno ve FÁZI 1, jednotlivé procesy jsou seskupeny do makro procesů specifických pro analyzovaný kontext. Dopady spojené s těmito makro procesy se počítají jako *„nejhorší případ“* jednotlivých dopadů různých procesů, které je tvoří.

4.2.2 Určování a oceňování aktiv

Určení aktiv je výchozím bodem, bez něhož není možné řádně a efektivně řídit zabezpečení společnosti. Inventarizace je ve skutečnosti výchozím bodem pro klasifikaci aktiv společnosti a pro analýzu úrovně rizika, kterému jsou vystaveny.

Účelem této provozní fáze je zajistit sestavení, nebo formalizování na základě již existujících metodik, soupisu informačních aktiv, která společnost považuje za „kritická“ pro dosažení svých obchodních cílů, pro splnění svých smluvních závazků a v neposlední řadě pro dodržení pravidel a právních předpisů, kterým podléhá její činnost.
Centrální hodnota aktiva je obvykle reprezentována informacemi (nebo daty), které systém zpracovává, přičemž úkol zpracování nebo ochrany je ponechán na jiných aktivech.
V tomto kontextu je hodnota přiřazena během rozhovorů BIA pro každé aktivum a pro každou dimenzi CIA (důvěrnost, integrita a dostupnost) bezpečnosti platné pro daný kontext.

Použitím informací shromážděných během rozhovorů je proto možné spojit dopady vyplývající z makro procesů, ve kterých jsou použity, s každým aktivem.

4.2.3 Analýza hrozeb a posuzování pravděpodobností jejich výskytu

Metodika použitá v procesu řízení rizik bezpečnosti informací definuje preventivní postup k určování hrozeb, které ovlivňují daná aktiva. Hrozby představují všechny prvky nebo události, které mohou způsobit poškození aktiva.
Cílem této činnosti je identifikovat hrozby a zranitelná místa ovlivňující určená aktiva zahrnutá do procesu analýzy a řízení rizik a posoudit pravděpodobnost jejich výskytu.
Aby byl seznam hrozeb úplný, odkazuje se na seznam hrozeb v normě ISO/IEC 27005 a úvah vypracovaných a zveřejněných agenturou ENISA na základě studií na toto téma.
Jednotlivé hrozby jsou následně seskupeny do realistických rizikových scénářů pro analyzovaný kontext.

4.2.4 Analýza opatření

Cílem této činnosti je určit opatření, která jsou považována za nezbytná k odvrácení rizikových scénářů pro aktiva identifikovaná v předchozím kroku.

Abychom měli jistotu, že je seznam úplný, používá Skupina Aruba seznam opatření založený na osvědčených postupech normy ISO/IEC 27001 přílohy A. V závislosti na typu analyzované služby mohou být hodnocení pro konkrétní subjekty obohacena analýzou dalších kontrol navržených autoritativními zdroji, jako jsou ENISA, AgID (Agency for Digital Italy), NIST atd.

Jakmile je seznam bezpečnostních kontrol definován, mapují se s ohledem na rizikové scénáře, na jejichž základě mohou být provedeny, aby se snížila pravděpodobnost výskytu příslušných hrozeb nebo jejich dopadů.

Protiopatření byla rozdělena na:

- **Reaktivní** (r) – určené ke snížení dopadu;
- **Preventivní** (p) – jeho cílem je snížit pravděpodobnost výskytu hrozby.

4.3 FÁZE 3: Hodnocení rizik

4.3.1 Model a metodika rizik

Hodnota rizika je chápána jako funkce $R = f(A, M, V)$, kde A je hodnotou dotyčných aktiv, M hodnotou hrozeb a V zranitelností. 10

Pomocí FÁZE 2 procesu řízení rizik bezpečnosti informací lze definovat model rizik (*modelování hrozeb*). Jedná se o proces, který se používá k identifikaci potenciálních hrozeb a zranitelných míst, k posouzení jejich pravděpodobnosti ve specifických okolnostech, k jejich seřazení podle priority a ke snížení rizika jejich výskytu zavedením vhodných opatření.

Jakmile jsou definovány základní souvislosti, proces *modelování hrozeb* spočívá ve:

- Vytvoření seznamu potenciálních útoků/zranitelností, který zahrnuje způsoby, jakými by mohla být ohrožena důvěrnost, integrita a dostupnost dat;
- Posouzení nejpravděpodobnějších útoků/zranitelností, vyřazení těch, které jsou nepravděpodobné nebo je téměř nemožné je napravit, a na všechny ostatní aplikovat kontroly nebo opatření, která mohou být buď technická nebo procedurální.

4.3.2 Platné bezpečnostní požadavky a úroveň shody

Jakmile jsou určeny bezpečnostní požadavky, které jsou považovány za relevantní v souvislosti s analýzou (viz oddíl „Analýza opatření“), posuzuje se, do jaké míry jsou splněny požadavky týkající se 14 oblastí uvedených v příloze A normy ISO/IEC 27001.

Rozsah, v jakém je každé bezpečnostní opatření v souladu s nejlepší praxí, je vyjádřen podle definované stupnice hodnot od 0, což znamená, že neexistuje žádné bezpečnostní opatření, do 4, kde bylo bezpečnostní opatření zcela implementováno.

Pro analýzu úrovně souladu kontrol požadovaných přílohou A normy ISO/IEC 27001 se používají informace a důkazy shromážděné prostřednictvím specifických hodnotících činností prováděných interně.

4.3.3 Výpočet inherentních a zbytkových základních rizik

Během této fáze se vypočítává hodnota inherentních a zbytkových základních bezpečnostních rizik CIA (JAK JSOU, plánovaných a JAK MAJÍ BÝT) spojených s analyzovanou službou.
Inherentní základní rizika pro každé aktivum a pro každý scénář, která jsou spojená podle výše popsané logiky, se vypočítají s ohledem na pravděpodobnost výskytu jednotlivých rizikových scénářů a potenciální dopad, který by mohly mít.
Jakmile jsou zjištěna inherentní rizika, jsou pro získání zbytkových rizik (JAK JSOU, plánovaných a JAK MAJÍ BÝT) zohledněny hodnoty spojené s bezpečnostními protiopatřeními potřebnými k odvrácení identifikovaných rizikových scénářů během fáze interního auditu, a to jak z hlediska snížení pravděpodobnosti hrozeb, tak z hlediska snížení dopadu.

4.4 FÁZE 4 – Náprava rizik[11]

4.4.1 Analýza přijatých rizik

Jedním z konceptů, kterým je třeba se zabývat, pokud jde o řízení rizik, je řízení přijatých rizik. Tento termín obecně odkazuje na rizika, která z nějakého důvodu nemohou být řešena jednoduše nebo vůbec a která jsou tedy akceptována.

Cílem této činnosti je proto definovat kritérium, podle něhož lze jednoduše přijmout páry hrozba-aktivum s nízkým rizikem. Nad rámec jednotlivých případů se proto definuje prahová hodnota, pod níž je určité riziko považováno za náklad, a proto není řešeno.

4.4.2 Výsledky analýzy: zbytkové riziko, JAK JE

Práce spojené s analýzou a hodnocením rizik, s přihlédnutím k použitým protiopatřením (zbytkové riziko), se provádějí podle následujících kroků:

- Posouzení bezpečnostních kontrol s ohledem na osvědčené postupy uvedené v příloze A normy ISO/IEC 27001;
- Analýza dopadu ztráty dostupnosti, důvěrnosti a integrity informací u dotčených služeb;
- Analýza zranitelností a hrozeb pro aktiva;
- Posouzení skutečného rizika v oblasti bezpečnosti informací a určení pořadí podle důležitosti.

4.4.3 Analýza nedostatků a výběr opatření

V návaznosti na provedenou analýzu, za účelem řešení veškerých relevantních rizik/problémů v rámci služeb poskytovaných Skupinou Aruba a s cílem pokračovat v neustálém zlepšování ISMS, jsou údaje získané z analýz provedených nástroji pro analýzu rizik zpracovávány za účelem identifikace rizikových oblastí, pro které je třeba definovat vhodná bezpečnostní opatření.

Za účelem určení opatření považovaných za nezbytná ke zlepšení a snížení rizik se proto čas od času provede analýza nedostatků, jejímž cílem je posoudit nesoulad mezi současnou úrovní uplatňování bezpečnostních opatření a maximální aplikovatelnou úrovní.

4.4.4 Plán napravování rizik – racionalizace intervence

Opatření určená v analýze nedostatků jsou pak seskupena do konkrétních projektových iniciativ a zdokumentována v rámci plánu eliminování rizik

5 FREKVENCE ANALÝZ

Proces řízení rizik v oblasti bezpečnosti informací se provádí každých dvanáct měsíců nebo dříve, dojde-li k významné události, zejména:

12

- Vzniknou nová aktiva, která spadají do oblasti řízení rizik;
- Vzniknou nové hrozby uvnitř i vně organizace, které nebyly posouzeny;
- Vznikne možnost, že nová nebo zvýšená zranitelnost může být zneužita hrozbami;
- Je potřeba přezkoumání již zjištěných zranitelností s cílem určit ty, které mohou být více vystaveny novým nebo znovu se objevujícím hrozbám;
- Nastanou zvýšené dopady nebo důsledky hrozeb na aktiva, zranitelnost a rizika, které společně vedou k nepřijatelné celkové úrovni rizika;
- Nastanou zvláště závažné bezpečnostní incidenty.

Kromě toho mohou být analýzy prováděny s různou četností, například ohledně souladu s konkrétními normami nebo požadavky na certifikaci.