Kapitola 7

Bezpečnostní analýza (analýza rizik)

Po prostudování kapitoly budete umět:

- základní pravidla a smysl analýzy rizik, tj., bezpečnostní analýzy informačního systému.

Klíčová slova:

Analýza rizik, aktivum, hrozba, zranitelnost, riziko.

7.1 Úvod do problematiky

Důležitým atributem navrhovaných systémů je správa bezpečnosti informací. Pro základní analýzu rizik se vychází z přístupů uvedených v metodice, která je v souladu s normami:

- ČSN ISO/IEC 27001:2014 – Systémy řízení bezpečnosti informací
- ČSN ISO/IEC 27002:2014 – Soubor postupů pro řízení bezpečnosti informací
- ČSN ISO/IEC 27005:2009 – Řízení rizik bezpečnosti informací

Postup, který je ve shodě s bezpečnostními normami ČSN/ISO, je klíčovým zorným úhlem při řešení analýzy rizik.

7.1.1 Definice pojmů[4]

Aktivum

Aktivum je vše, co má pro subjekt hodnotu, která může být zmenšena působením hrozby. Základní charakteristikou aktiva je hodnota aktiva, která je založena na objektivním vyjádření obecně vnímané ceny nebo na subjektivním ocenění důležitosti (kritičnosti) aktiva pro daný subjekt, popřípadě kombinaci obou přístupů. Hodnota aktiva je relativní v závislosti na úhlu pohledu hodnocení.

Při hodnocení aktiva se berou v úvahu především následující hlediska:

a) pořizovací náklady či jiná hodnota aktiva,
b) důležitost aktiva pro existenci či chování subjektu,
c) náklady na překlenutí případné škody na aktivu,
d) rychlost odstranění případné škody na aktivu,
e) jiná hlediska (mohou být specifická případ od případu).

Hrozba

Hrozba je síla, událost, aktivita nebo osoba, která má nežádoucí vliv na bezpečnost nebo může způsobit škodu.

[4] Smejkal, V., Rais, K. Řízení rizik ve firmách a jiných organizacích. 4., aktualizované a rozšířené vydání. Praha: GRADA, 2013, 488 str., ISBN 978-80-247-4644-9

Škoda, kterou způsobí hrozba při jejím působení na určité aktivum, se nazývá dopad hrozby. Základní charakteristikou hrozby je její úroveň. Úroveň hrozby je definována jako pravděpodobnost výskytu hrozby.

Zranitelnost

Zranitelnost je nedostatek, slabina nebo stav analyzovaného aktiva (případně subjektu nebo jeho části), který může hrozba využít pro uplatnění svého nežádoucího vlivu. Tato veličina je vlastností aktiva a vyjadřuje, jak citlivé je aktivum na působení dané hrozby.

Zranitelnost vznikne všude tam, kde dochází k interakci mezi hrozbou a aktivem. Základní charakteristikou zranitelnosti je její úroveň. Úroveň zranitelnosti aktiva odpovídá pravděpodobnosti, že se hrozba vyplní.

Opatření

Opatření je postup, proces, procedura, technický prostředek nebo cokoliv, co bylo speciálně navrženo pro zmírnění působení hrozby (její eliminaci), snížení zranitelnosti nebo dopadu hrozby. Opatření se navrhují s cílem předejít vzniku škody nebo s cílem usnadnit překlenutí následků vzniklé škody.

Z hlediska analýzy rizik je opatření charakterizováno efektivitou a náklady.

Do nákladů na opatření se započítávají náklady na pořízení, zavedení a provozování opatření. Společně s efektivitou opatření jsou tyto náklady důležitými parametry při výběru opatření.

Riziko

Ve smyslu předchozích definic riziko vyjadřuje míru ohrožení aktiva, míru nebezpečí toho, že se uplatní hrozba a dojde k nežádoucímu výsledku vedoucímu ke vzniku škody. Velikost rizika je vyjádřena jeho úrovní.

Při návrhu opatření se používá pravidlo, které stanovuje, že náklady vynaložené na snížení rizika musí být přiměřené hodnotě chráněných aktiv s cílem dosažení referenční úrovně rizika, pod kterou se riziko prohlásí za zbytkové a nepodnikají se žádná opatření.

7.2 Identifikace aktiv, vytvoření modelu aktiv informačního systému

V rámci této fáze je provedeno rozdělení aktiv do kategorií:

1. datová aktiva – informace, data,
2. fyzická aktiva – počítačové vybavení, komunikační zařízení, úložná media, další technická zařízení (napájecí zdroje, klimatizační zařízení),
3. aplikační programová aktiva – aplikační a systémové programové vybavení, vývojové nástroje a utility,
4. informační aktiva – databáze, datové soubory, systémová dokumentace, uživatelské manuály, školící materiály, archivované informace
5. služby koncovému uživateli – procesy, přístupy k datům,
6. prostory – lokality, budovy, místnosti,
7. lidé – dovednosti, zkušenosti,
8. nehmotná aktiva – pověst, image organizace.

Při zpracování analýzy rizik je výhodné i některá aktiva sdružovat do skupin. U všech aktiv pak je stanovena i jejich hodnota, závislá na hodnocení výše uvedených typů aktiv a vazeb plynoucích z vybraných aktiv. V návaznosti na stanovení hodnoty aktiv bude definována úroveň hrozeb a zranitelností pro všechna aktiva. K tomuto účelu jsou využity výsledky z řízených interview se specialisty Zadavatele. Odpovídající opatření k ošetření jednotlivých rizik vycházejí z hodnot aktiv a úrovní hrozeb a zranitelností, resp. ze zjištěné míry rizika. Dále jsou zohledněny i dostupné informace z této oblasti včetně zkušeností zpracovatelského týmu.

7.3 Stanovení zranitelnosti informačního systému, hodnocení rizik (stanovení míry rizika)

Obecně chápeme riziko jako možnost, že s určitou pravděpodobností dojde k události, jež se liší od předpokládaného stavu či vývoje. Riziko by nicméně nemělo být směšováno, respektive redukováno na pouhou pravděpodobnost, neboť zahrnuje, jak samotnou pravděpodobnost, tak kvantitativní rozsah dané události (dopad). Nejčastěji se riziko uvádí v souvislosti s negativním dopadem (i když

obecně může být odchylka i kladná, ale kladný výsledek nelze většinou považovat za riziko. Proto je nejvíce adekvátní definicí ta, podle níž riziko je situace, v níž existuje možnost nepříznivé odchylky od žádoucího výsledku, ve který doufáme nebo ho očekáváme.

V souvislosti s řízením IS/IT projektů je tedy třeba posoudit:

- jaká rizika projektu hrozí,
- jak je lze zcela eliminovat nebo alespoň snížit jejich úroveň.

Řízení rizik je proces, při němž se subjekt řízení snaží zamezit působení již existujících i budoucích faktorů a navrhuje řešení, která pomáhají eliminovat účinek nežádoucích vlivů, a naopak umožňují využít příležitosti působení pozitivních vlivů. Součástí procesu řízení rizik je rozhodovací proces, vycházející z analýzy rizika. Po zvážení dalších faktorů, zejména ekonomických, technických, ale i sociálních, politických a jiných, management pro řízení rizik vyvíjí, analyzuje a srovnává možná preventivní a regulační opatření. Posléze z nich vybere ta, která existující riziko minimalizují.

Zpracovaná analýza rizik není konečným dokumentem, rizika musí být následně dále upřesňována, zejména z pohledu reakce na ukončení vývoje systémů podniku a reflektovat na nové požadavky vyplývající z rutinního provozu.

Lze konstatovat, že základní analýza již vymezuje bezpečnostní požadavky na realizaci systému a poskytuje podklady pro podrobnou analýzu rizik, prováděnou před nastavením systému do rutinního provozu.

V daném případě je u analytických prací výhodné využít zkušeností s postupem využívajícím řízených interview, tj. „Facilitated Risk Analysis Process“ (FRAP)[5]. Tento proces byl vypracován CSI (Computer Security Institute a vychází z metodiky Delphy, tedy z postupu založeném na řízené diskusi se zástupci Zadavatele. Hlavní důraz při jejím provádění je kladen na řízená jednání expertů a pracovníků Zadavatele jakož i Zpracovatele a na komunikaci s těmito pracovníky, kteří se na provádění analýzy podílejí.

Přitom metoda vychází z předpokladu, že obdržené výsledky analýzy jsou na úrovni odpovídající odborné fundovanosti a znalosti prostředí IS jednotlivých zúčastněných pracovníků.

S ohledem na tyto skutečnosti je třeba daný přístup považovat za první krok, kdy je třeba řešit základní požadavky spojené se stanovením bezpečnosti systému, přičemž podrobná analýza rizik může být provedena v dalším kroku (před nasazením do rutinního provozu).

[5] Thomas Peltier, Information Security Risk Analysis, CRC Press, 2001 - Počet stran: 296 ISBN: 0-8493-0880-1.

7.4 Návrh opatření – prevence proti identifikovaným hrozbám a rizikům

Metody a postupy reflektují doporučení bezpečnostních norem.

7.4.1 Fáze analýzy rizik

1. Identifikace aktiv
   Identifikace aktiv systémů v rámci podniku a jejich základní členění na:

   - informační aktiva
   - podpůrná aktiva
   - aktiva technické infrastruktury,
   - fyzická aktiva,
   - personál.

2. Ohodnocení aktiv.
   Zde jsou stanoveny hranice analyzovaného systému a definují se aktiva spravovaná v systému, kdy se u identifikovaných aktiv systému určí jejich hodnoty a ohodnotí závažnost dopadů bezpečnostních incidentů (Business Impact Analysis) podle identifikátorů hodnocení a se stanovením požadavků na obnovu aktiv v případě havárie (BCP – Business Continuity Plan), tedy zajištění nepřetržitosti provozu.
3. Analýza hrozeb a zranitelností dle metodiky stanovené v ČSN ISO/IEC 27005:2008.
4. Stanovení rizik dle vztahu:

   Riziko = funkce f (dopad hrozby, pravděpodobnost výskytu hrozby)

7.4.2 Aktiva informačního systému

Stanovení odpovědnosti za aktiva je nutnou podmínkou pro dosažení odpovídající bezpečnosti informací.

Musí být stanoven vlastník každého identifikovaného aktiva nebo skupiny aktiv a vlastníkovi musí být přiřazena odpovědnost za udržování příslušných nástrojů řízení bezpečnosti. Odpovědnost za

implementaci nástrojů řízení bezpečnosti může být delegována, ačkoliv zodpovědnost musí zůstat u určeného vlastníka aktiva.

Při tomto postupu základní analýzy můžeme aktiva seskupovat do kategorií, což umožňuje zjistit a popsat způsoby jejich zpracování. Informační aktiva zobrazují významné komponenty informačního systému s bezprostředním vlivem na informační bezpečnost.

Dané skutečnosti jsou posuzovány z pozice nejhorších případů spojených s dopady, které by mohly vyplynout zejména z následujících skupin důsledků:

- nedostupnosti dat,
- prozrazení dat,
- modifikace dat,
- zničení dat.

Bližší posouzení standardně vychází ze čtyř hlavních bezpečnostních hledisek, týkajících se i aktiv informačního systémů podniku, tj.:

- narušení důvěrnosti dat – ze strany uživatelů neoprávněných, ale i ze strany uživatelů překračujících rozsah svého oprávnění;
- modifikace dat nebo programů – vlivem chyb, poruch systému a/nebo aktivní (úmyslnou) či nedbalostní činností uživatelů;
- zničení dat nebo programů – vlivem chyb (hardware, software, správy IS nebo uživatelů, a to rovněž aktivní (úmyslnou) či nedbalostní činností);
- nedostupnost – zamezení přístupu oprávněných uživatelů do systému nebo datům.

Při základním posuzování aktiv je zásadou pomíjet stávající realizovaná opatření, aby nedošlo ke zkreslení výsledku díky jejich stávající účinnosti.

7.4.3 Ohodnocení aktiv

U všech aktiv je stanovena i jejich hodnota, závislá na hodnocení výše uvedených typů aktiv a vazeb plynoucích z kategorií aktiv.

Informační aktiva, která jsou předmětem zkoumání v této etapě projektu, byla identifikována na základě úvodních pohovorů, kdy se dané skutečnosti posuzovaly z pozice nejhorších případů, které by mohly vyplynout zejména z následujících skupin důsledků:

- nedostupnosti dat,
- prozrazení dat,

- modifikace dat,
- zničení dat.

Každé z výše uvedených hledisek je třeba hodnotit z konkrétních dílčích hledisek:

- v případě nedostupnosti je nutné hodnotit alespoň tři časové úseky specifikující dobu nedostupnosti, kdy dojde k určité formě dopadů a následků – od pouhých nepříjemností přes vážný problém až po nezvratné změny.
- u zničení se zvažuje, zda se jedná o totální zničení bez možnosti náhrady, či o zničení s možností obnovy z náhradních zdrojů – tj. v našem případě informačních aktiv o pořízení dat z náhradních zdrojů.
- v případě chybné funkce se jedná o rozlišení ve vztahu k alespoň třem časovým úsekům specifikujícím dobu chybné funkce, kdy dojde k určité formě dopadů a následků – od pouhých nepříjemností až vážným problémům.
- u modifikace je hodnocena chyba nebo úmysl.

Jelikož se ukazuje dosti obtížné, přiřadit jednotlivým aktivům finanční hodnotu, efektivní cesta k ocenění, resp. ohodnocení významu aktiv spočívá v odhadu důležitosti posuzovaných aktiv v rámci navrženého systému.

Numerické údaje tedy nevyjadřují hodnotu nebo kvantitu veličiny, ale příslušnost do dané oblasti. Tím, že se pracuje s veličinami, které spadají do definovaných intervalů, se do jisté míry eliminuje různá kvalita (různá úroveň hodnocení) získaných podkladů.

Obvyklými důsledky naplnění hrozeb jsou dopady finanční (vícenáklady, ušlý zisk, náklady na soudní spor, náhrada škody apod.). Ale mohou to být i dopady společensko-politické (neschopnost organizace zajistit určitou činnost, vyplývající ze zákona nebo z vlastního rozhodnutí příslušného orgánu veřejné moci), jakož i dopady právní (porušení zákona – např. na ochranu osobních údajů).

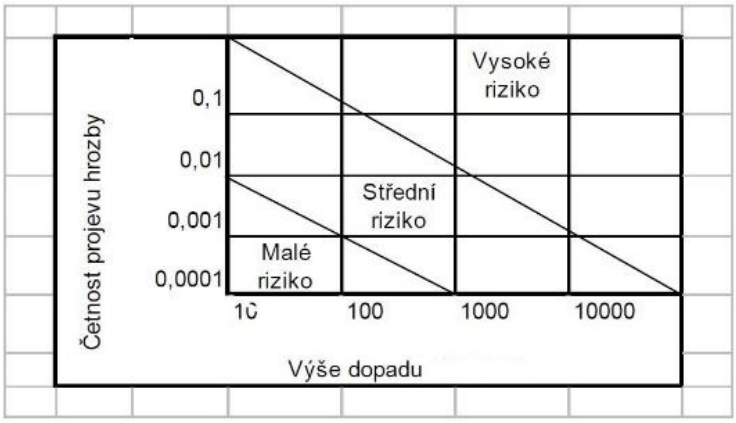
Některé lze kvantifikovat (zejména z oblasti finanční), některé nikoliv a v takovém případě nám přijde vhod výše popsaný kvalifikovaný odhad na pětistupňové stupnici.

Za klíčové dopady lze považovat již výše uvedené:

- pořizovací náklady či jiná hodnota aktiva,
- důležitost aktiva pro existenci či chování subjektu,
- náklady na překlenutí případné škody na aktivu,
- rychlost odstranění případné škody na aktivu,
- jiná hlediska (mohou být specifická případ od případu)

Hodnoty z tabulek, tj. pravděpodobnost vzniku hrozby, hodnota aktiva a zranitelnost daného aktiva jsou podkladem k výpočtu rizik. Vypočtenou míru rizik pak můžeme vyjádřit ve formě matice

rizik. Zde můžeme identifikovat pásma rizika definovaná hranicemi pro nízká (přijatelná), střední a vysoká rizika takto (měřítko je ilustrativní):



Obrázek 7.1 Matice rizik

Při identifikování hlavních informačních aktiv se vychází z procesního řízení a stanovuje se výše každého případu v rozsahu od stupně „velmi nízký“ do „kritický“.

V návaznosti na zhodnocení vlivu hrozeb na řešené prostředí informačního systému vyplývá i obsah tabulky (viz příloha), kde jsou, ve vztahu na nedostupnost či chybnou funkci aktiva, hodnoceny tři časové úseky specifikující dobu nestandardní situace, kdy dojde k určité formě dopadů a následků – od pouhých nepříjemností přes vážný problém až po nezvratné změny.

7.4.4 Analýza hrozeb a zranitelností

Pro provedení analýzy rizik je hodnota identifikovaných aktiv základním vstupem. V širším pojetí zahrnujeme do informačních aktiv i aktiva, která souvisejí s technickou infrastrukturou posuzovaných informačních systémů, i personální a objektovou oblastí.

Úroveň hrozby stanovujeme jako pravděpodobnost výskytu hrozby a úroveň zranitelnosti odpovídá pravděpodobnosti, že se hrozba vyplní s tím, že se hodnotí důležitost aktiva napadeného hrozbou.

Princip odhadu hrozeb a zranitelností

Vzhledem k množství faktorů, které mohou zapříčinit dopad hrozby na informační systém, byly jednotlivé hrozby a zranitelnosti strukturovány podle názvu příslušných aktiv, přičemž bylo dodrženo členění normy ČSN ISO/IEC 27001. Takto zvolený přístup umožnil postihnout celou šíři hrozeb a zranitelností, potenciálně směrovaných na prostředí informačního systému.

Důležité je, aby se vždy hodnocení soustředilo na možné projevy vyplývající mj. z následujících nestandardních situací a činností s ohledem na charakter daného informačního systému, zejména na:

- logická infiltrace (neoprávněný přístup, zneužití oprávněného přístupu, neoprávněné použití aplikace, viry apod.),
- infiltrace komunikace (aktivní narušení komunikace, zneužití logického propojení apod.),
- chyby lidského faktoru (chyby uživatelů, administrátorů, operátorů apod.),
- provozní závady IS,
- fyzické hrozby (krádež, úmyslné poškození, terorismus).

Posuzuje se, do jaké míry by působením hrozeb ve vztahu k identifikovaným zranitelnostem utrpěl informační systém, resp. podnik významnou újmu či případní narušitelé získali významný prospěch.

Metrika hrozeb a zranitelností

Pro stanovení úrovně hrozeb i zranitelnosti byla zvolena pětibodová stupnice, na rozdíl od tříbodové metriky použité v metodice CRAMM. Tato diference vyplynula ze zvolení jiného postupu při výpočtu míry rizika, kdy v našem případě jsou východiskem doporučení a postupy uvedené v normě ČSN ISO/IEC 27005.

Vyjádření úrovní hrozeb a zranitelností je uvedeno v následujících stupních významnosti takto:

Tabulka 7.1 Matice hrozeb a zranitelností

Hrozby	
1	velmi nízké
2	nízké
3	střední
4	vysoké
5	kritické

Zranitelnost	
1	velmi nízká
2	nízká
3	střední
4	vysoká
5	kritická

Použitá metoda stanovení míry rizik[6]

V našem případě byla zvolena metoda analýzy rizik využívající matice aktiv, hrozeb a zranitelností.

Při této analýze rizik se využívají následující tabulky:

- tabulka, obsahující identifikovaná aktiva spolu s jejich hodnotou;

[6] Viz též Smejkal V., Rais K., Řízení rizik ve firmách a jiných organizacích. 4. vydání, Praha Grada Publishing. 2013

- tabulka, obsahující identifikované hrozby a pravděpodobnost možnosti jejich realizace;
- tabulka zranitelností systému.

Hodnoty z tabulek, tj. pravděpodobnost vzniku hrozby, hodnota aktiva a zranitelnost daného aktiva jsou podkladem k výpočtu rizik. Vypočtenou míru rizik pak můžeme vyjádřit ve formě matice rizik.

Míru rizika lze zjistit výpočtem dle vztahu:

Riziko = funkce (pravděpodobnost výskytu hrozby, výše dopadu na aktivum)

S ohledem na hodnotu aktiva je pak stanoven bezpečnostní profil pro aktiva zahrnutá do analýzy rizik a návazně pak budou definována příslušná opatření k ošetření rizik. Lze již nyní poznamenat, že srovnání bezpečnostního profilu a stávajících opatření přijatých v daném informačním systému dává relevantní podklady k vytvoření bezpečnostního modelu maturity (úrovně bezpečnostní zralosti) systému.

Ke stanovení míry rizika bude využito principů definovaných v normě ČSN ISO/IEC 27005:2009 Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací) Grafické znázornění míry rizika je v daném případě velmi přehledné a lze jej dobře využít pro zpracování souborů návazných plánů pro ošetření jednotlivých rizik, jakož i podklady pro sledování navržených akčních plánů.

V návaznosti na doporučení normy ISO/IEC 27005:2008 a z pohledu efektivnosti řešení rizik v informačních systémech podniku (jakož i s ohledem na charakter získaných podkladových materiálů) je zvolena metoda využívající tedy dvou základních parametrů, kdy míra rizika je funkcí pravděpodobnosti výskytu incidentu a dopadu uskutečnění hrozby ve vztahu k příslušnému aktivu.

Nejdříve je ke každému aktivu přiřazena jeho hodnota. Tato hodnota vyjadřuje míru nepříznivého dopadu, ke kterému by došlo v případě ohrožení daného aktiva.

Pro určení pravděpodobnosti výskytu této události je možné s výhodou využít empiricky zjištěných hodnot z veřejně dostupných zdrojů.

Tyto hodnoty uvedené v příslušných tabulkách pak vyjadřují pravděpodobnost výskytu dotčené události.

Následně je pak nalezením průsečíku hodnot dopadu na aktivum a pravděpodobnosti výskytu dané události v součtové tabulce je určena míra rizika pro dotčené aktivum. Tabulkou je pak tato operace vyjádřena následovně:

Tabulka 7.2 Matice pravděpodobností

pravděpodobnost	velmi nízká	1–2	**1**
	nízká	3–4	**2**

	střední	5–6	**3**
	vysoká	7–8	**4**
	kritická	9–10	**5**

K hodnocení míry jednotlivých rizik (inherentního, reziduálního a zbytkového) je použita tzv. součtová matice.

V etapě analýzy rizik a před přijetím opatření na jejich eliminaci se realizuje ohodnocení inherentních rizik (tj. bez zohlednění již existujících či uvažovaných opatření v analyzovaném systému). Po implementaci opatření tak musí být provedeno nové hodnocení míry rizik tak, že je stanovena míra rizika reziduálního, tj. s uvažováním dopadu provedených opatření, popř. cílového rizika, které vychází ze strategického manažerského rozhodnutí, kde je stanovena míra daného rizika, která je již plně akceptovatelná.

V tabulkách jsou hodnoty pravděpodobnosti výskytu rizika definovány takto:

Tabulka 7.3 Matice pravděpodobnosti výskytu

Pravděpodobnost výskytu		
Stupeň	% za rok	Slovní vyjádření
1	<0; 5>	prakticky nepravděpodobné
2	<5; 20>	málo pravděpodobné
3	<20; 50>	příležitostné
4	<50; 70>	pravděpodobné až časté
5	<70; 100>	velmi časté

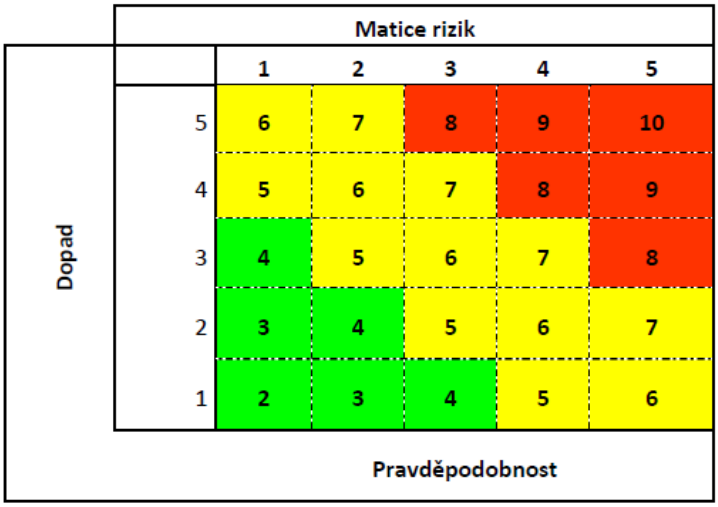
Dopad je ohodnocen mírou následků pro subjekt rovněž ve stupnici 1-5.

Tabulka 7.4 Matice dopadu

Dopad		
Stupeň	Dopad	Následek pro aktiva
1	nevýznamný	Nemá vliv na aktiva nebo je zcela zanedbatelný
2	malý	Nepodstatný, velmi malý vliv na aktiva

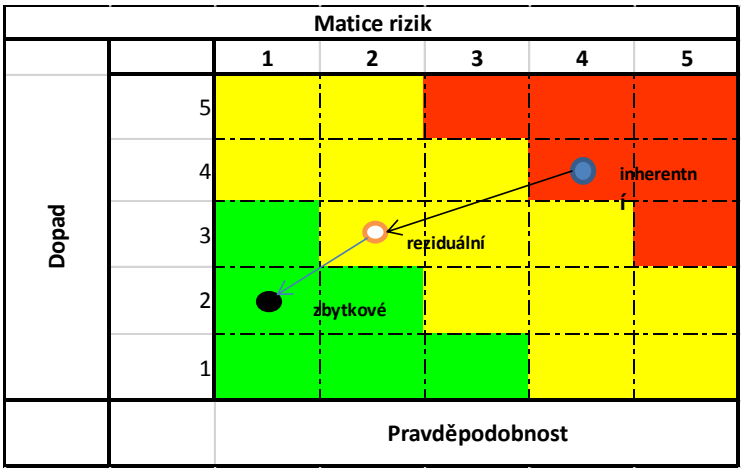
3	střední	Má vliv na aktiva a ztráty jsou řešitelné v rámci stávajících aktiv (Projektu)
4	značný	Má značný vliv na aktiva a ztráty jsou řešitelné pouze mimořádnými opatřeními (zvýšení nákladů, časového harmonogramu atd.)
5	fatální, obrovský	Má kritický vliv na aktiva a potenciální ztráty jsou tak velké, že mohou vést k zrušení Projektu, zakázky, diskreditaci Objednatele apod.

Numerické údaje tedy nevyjadřují hodnotu nebo kvantitu veličiny, ale příslušnost do dané oblasti. Tím, že se pracuje s veličinami, které spadají do definovaných intervalů, se do jisté míry eliminuje různá kvalita (různá úroveň hodnocení) získaných podkladů. V souladu s metodikou uvedenou v ČSN ISO/IEC 27005:2009 jsou evidovaná rizika strukturovaná dle své úrovně do součtové matice rizik uvedené na následujícím obrázku, kde jsou ilustrovány oblasti s danými číselnými hodnotami.



Obrázek 7.2 Součtová matice rizik

Při návrhu odpovídajících bezpečnostních opatření dochází k „posunům“ v tabulkách rizik z úrovně inherentního rizika na úroveň reziduálního rizika, kdy je nutno brát v úvahu účinnost navrhovaných opatření, která jsou v rámci informačního systému implementována. Pro ilustraci je uveden příklad posunu z úrovně inherentního rizika na úroveň reziduálního rizika.



Obrázek 7.3 Eliminace evidovaných rizik

Důležité je zdůraznit, že míru reziduálního rizika neurčují opatření, která jsou teprve uvažována či připravována. Zbytkové riziko je svázáno se strategickým manažerským rozhodnutím, kdy je stanovena míra daného rizika, která je pro podnik v dané situaci akceptovatelná.

Z toho vyplývá, že v systému správy bezpečnostních rizik musí vlastník rizika po jeho zjištění a evidenci stanovit úroveň rizika ve třech základních kategoriích:

- inherentní riziko – míra evidovaného rizika bez implementovaných opatření,
- residuální riziko – aktuální míra evidovaného rizika (při zohlednění implementovaných opatření),
- zbytkové riziko – cílový stav, který nevyžaduje žádné akce na jeho řešení.

Metrika míry rizik

Pro zpracování analýzy rizik v rámci informačních systémů může být zvolena stupnice, kde jsou hodnoty strukturovány do „oblastí“, takže můžeme danou veličinu zařadit po položku:

- 1 = velmi nízké – prakticky nepravděpodobné,
- 2 = nízké – málo pravděpodobné apod.

- Míra rizika 2–4 znamená, že je možné dané riziko akceptovat, toto riziko není vyřazeno z evidence, nejsou přijata žádná opatření, která by vedla k eliminaci tohoto rizika, většinou se jedná o rizika, u kterých by náklady spojené s odpovídajícím opatřením byly vyšší než potenciální dopad uskutečněné hrozby.

- Míra rizika 5–7 značí, že se jedná o riziko, které vyžaduje přijetí adekvátních opatření, v rámci ošetření tohoto rizika je nutné zpracovat plán mitigace (snížení) tohoto rizika a příslušné činnosti budou průběžně sledovány v rámci správy rizik. Dané riziko bude posouzeno při pravidelné kontrole (vesměs se jedná o pravidelné každoroční aktivity).

- Míra rizika 8–10 ukazuje na kritickou oblast a vyžaduje okamžité přijetí nápravy.

Numerické údaje tedy nevyjadřují hodnotu nebo kvantitu veličiny, ale příslušnost do dané oblasti.

V rámci této tabulky jsou následně stanoveny hranice pro nízká (přijatelná), střední a vysoká rizika.

Každé riziko je charakterizováno množinou {úroveň hrozby; úroveň zranitelnosti; pravděpodobnost výskytu rizika; výše škody}, přičemž v rámci návrhu systému bude k takto definovaným rizikům přiřazeno navrhované opatření.

Metodika výpočtu rizika

Míra rizika podle metody postavené na vztahu výše dopadu události (resp. uskutečnění hrozby) na dané aktivum a pravděpodobnosti výskytu takové události je relativní veličina ve stupnici 2–10. Tato hodnota vychází ze závislosti jednotlivých atributů (hrozby, zranitelnosti apod.) stanovených v předchozích etapách analýzy.

Pro další práci s evidovanými riziky systému a další činnosti svázané se správou rizik související s jejich hodnocením ve vztahu ke všem kategoriím rizik (tj. inherentnímu, reziduálnímu a zbytkovému riziku) jsou využity příslušné tabulky uvedené v příloze. Získané hodnoty jsou pak uvedeny v tabulce rizik.

Cílem analýzy rizik je evidence a stanovení míry jednotlivých základních rizik informačního systému podniku Analýza rizik je vždy směrována do výpočtu míry inherentních rizik, tj. rizik systému, kde nejsou uplatněna bezpečnostní opatření.

Dělení evidovaných rizik do příslušných matic rizik se uplatní až při evidenci a stanovení reziduálních rizik, informačních systémů, To umožní jednoznačně sledovat účinnost implementovaných bezpečnostních opatření a využít hodnoty v daných maticích při plánování procesu řízení rizik.

V příslušných tabulkách (maticích rizik) jsou rizika umístěna v závislosti na pravděpodobnost jejich výskytu a dle dopadu na aktiva podniku, které projev tohoto rizika způsobí.

ČERVENÁ OBLAST – pro rizika, která jsou začleněna do této oblasti, musí být navrženo bezpečnostní opatření k jejich zvládnutí a tvorba plánů eliminace těchto rizik má vysokou prioritu.

ŽLUTÁ OBLAST – míra rizika, umístěného v této oblasti umožňuje posouzení nezbytnosti realizace bezpečnostních opatření, jejich rozsahu a časového plánu. Nicméně je třeba zdůraznit, že navržený přístup musí být důkladně zvážen a případná akceptace tohoto rizika musí být zdůvodněna a musí podléhat periodické kontrole.

ZELENÁ OBLAST – vytváří prostor, kde rizika mohou být akceptována, neboť jejich dopad či frekvence jejich výskytu nevyžaduje realizaci opatření. Reakce na tato rizika ve většině případů spadá do organizační úrovně.

Základní analýza rizik informačních systémů podniku je koncipována tak, aby poskytla podklady pro realizaci opatření, adekvátní ke zjištěným hrozbám. Na rizika zjištěná a evidovaná v základní analýze rizik musí reagovat bezpečnostní opatření již následující etapě vývoje. Uplatněná bezpečnostní opatření se pak odrazí v maticích rizik, kdy bude možné poukázat na eliminaci inherentních rizik na hodnoty reziduálního rizika, popř. až na zbytkovou hodnotu rizika.

Kapitola obsahuje souhrnný popis jednotlivých etap analýzy rizik. Jsou zde definice hrozeb a zranitelností informačního systému, Je ukázán postup při oceňování rizik a stanovení následných opatření.

1. Popište jednotlivé kroky analýzy rizik.
2. Vysvětlete pojmy aktivum, hrozba, zranitelnost.
3. K čemu se využívá součtová matice dopadu a pravděpodobnosti?
4. Na základě, čeho jsou oceňována rizika?

Literatura k tématu:

[1] SMEJKAL, V., Rais, K. *Řízení rizik ve firmách a jiných organizacích.* 4. aktualizované a rozšířené vydání. Praha: GRADA, 2013, 488 str., ISBN 978-80-247-4644-9.