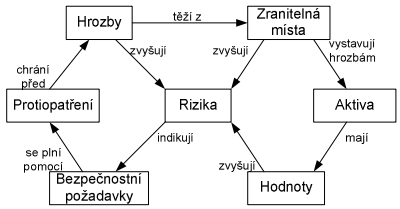
Management rizik

Základní pojmy

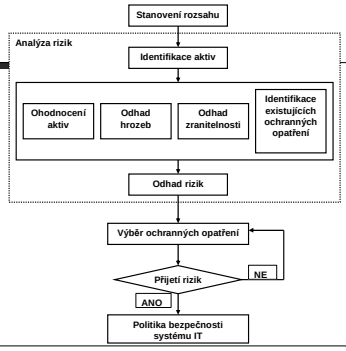
- Aktivum
- Hrozba
- Zranitelnost
- Protiopatření
- Riziko

Vzájemné vztahy při správě rizik



Management rizik

- Část identifikující rizika
  - analýza rizik
- Část hledající odpovídající ochranná opatření
  - zvládání rizik



Obecný postup analýzy rizik

- Stanovení hranice analýzy rizik
- Identifikace aktiv
- Stanovení hodnoty a seskupování aktiv
- Identifikace hrozeb
- Analýza hrozeb a zranitelností
- Měření rizika

Metody analýzy rizik

- Kvalitativní metody
  - Rizika vyjádřena v určitém rozsahu
  - Jednodušší, rychlejší a více subjektivní
  - Problém s kontrolou efektivnosti nákladů
- Kvantitativní metody
  - Založeny na matematickém výpočtu rizika
  - Více exaktní, náročnější na čas a úsilí
  - Poskytují finanční vyjádření rizika

Typy analýzy rizik (ČSN ISO/IEC TR 13335)

- 1) Základní AR
  - Aplikuje tzv. základní bezpečnost
  - Implementace katalogových ochranných opatření
- 2) Neformální AR
  - Využívá znalostí a zkušeností jednotlivců
  - Rychlost a finanční nenáročnost

Typy analýzy rizik (ČSN ISO/IEC TR 13335)

- 3) Orientační AR
  - Většinou součást kombinované AR
  - Určuje vhodný typ AR pro daný systém (základní nebo podrobná)
- 4) Podrobná AR
- 5) Kombinovaná AR
  - Kombinace orientační a podrobné AR

Podrobná analýza rizik – ad. 4)

- identifikace a ocenění aktiv
- nalezení zranitelných míst
- odhad pravděpodobnosti využití zranitelných míst
- výpočet očekávaných ztrát
- přehled použitých opatření a jejich nákladů
- odhad ročních úspor po zavedení vybraných opatření

Kombinovaná analýza rizik – ad. 5)

- Orientační AR
- Identifikace důležitých systémů
- Podrobná analýza u důležitých systémů
- Základní AR u ostatních systémů

Výpočet míry rizika - přístupy

- ***3 faktory***

  R = A x H x Z

R – míra rizika, A – hodnota aktiva, H – pravděpodobnost hrozby, Z - zranitelnost

- ***2 faktory***

  R = PI x D

R – míra rizika, PI – pravděpodobnost incidentu, D – dopad

Matice s předdefinovanými hodnotami

	Úroveň hrozby	Nízká			Střední			Vysoká		
	Úroveň zranitelnosti	N	S	V	N	S	V	N	S	V
Hodnota aktiv	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Odhad hodnoty četnosti a možné změny rizik

Úrovně hrozby	Nízká			Střední			Vysoká		
Úrovně zranitelnosti	N	S	V	N	S	V	N	S	V
Hodnota četnosti	0	1	2	1	2	3	2	3	4

Hodnota aktiv	0	1	2	3	4
Hodnota četnosti					
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

Rozlišení mezi riziky, které je možné a které není možné tolerovat

~~Hodnota~~ dopadu	0	1	2	3	4
Hodnota četností					
0	T	T	T	T	N
1	T	T	T	N	N
2	T	T	N	N	N
3	T	N	N	N	N
4	N	N	N	N	N

Zařazení hrozeb podle míry rizika

Popis hrozby (a)	Hodnota dopadu (aktiv) (b)	Pravděpodobnost výskytu hrozby (c)	Míra rizika (d)	Zařazení hrozby (e)
Hrozba A	5	2	10	2
Hrozba B	2	4	8	3
Hrozba C	3	5	15	1
Hrozba D	1	3	3	5
Hrozba E	4	1	4	4
Hrozba F	2	4	8	3

Analýza rizik využívající matice aktiv, hrozeb a zranitelností (1)

	Popis aktiva	Aktivum 1	Aktivum 2	Aktivum 3	.....	Aktivum Y
	Hodnota aktiva (A)	5	1	4		*Ay*
Popis hrozby	Pravděpodobnost hrozby (T)					
Hrozba A	4	3		2		
Hrozba B	2		3	1		
Hrozba C	5	4	1			
Hrozba D	1	5		3		
.....						
Hrozba X	*Tx*					*Vxy*

Analýza rizik využívající matice aktiv, hrozeb a zranitelností (2)

	Popis aktiva	Aktivum 1	Aktivum 2	Aktivum 3	.....	Aktivum Y
	Hodnota aktiva (A)	5	1	4		*Ay*
Popis hrozby	Pravděpodobnost hrozby (T)					
Hrozba A	4	60		32		
Hrozba B	2		6	8		
Hrozba C	5	100	5			
Hrozba D	1	25		12		
.....						
Hrozba X	*Tx*					*Rxy = Tx . Ay . Vxy*

Softwarové nástroje

- CRAMM
- RA2 Art of Risk
- CORAS
- COBRA
- a další.

Fiktivní firma ***WEB-SHOP***

- zabývá se internetovým prodejem blíže nespecifikovaného zboží.
- Firma má svou kancelář, odkud je řízena, a sklad prodávaného zboží, který se nachází v jiné lokalitě než kancelář.

Fiktivní firma ***WEB-SHOP***

- V kanceláři pracuje majitel firmy spolu se sekretářkou. Kancelář má dvě PC používající operační systém Microsoft Windows XP. Dále je v prostorech kanceláře umístěn server. Tento server je využíván pro provozování www stránek internetového obchodu. Server používá operační systém Microsoft Windows 2000 a databázi Microsoft Access. V budoucnu majitel přemýšlí o přemístění serveru do hostingového centra. Sekretářka kromě běžné agendy vyřizuje i telefonickou podporu zákazníkům. Výpočetní technika je spravována majitelem firmy.

Fiktivní firma ***WEB-SHOP***

- Sklad udržuje dostatečnou zásobu nejlépe prodávaných položek, aby byly splněny požadavky zákazníků. Sklad je přijímacím bodem pro všechny dodavatele, ať se týká přímého dodání k zákazníkovi nebo dodání na sklad. Zboží přichází přes místní kurýrní společnost. Výjimečně mohou být jednotlivé kusy doručeny poštou. Všechny objednávky zákazníků jsou odesílány přímo zákazníkům poštou, s výjimkou určitých velkých nebo těžkých kusů, které jsou zasílány s využitím kurýrní společnosti.

Fiktivní firma ***WEB-SHOP***

- Sklad má jedno PC, které se používá pro záznam položek na skladu a jejich umístění. Také se používá pro vyznačení objednávek, které mají být odeslány a pro zaznamenávání objednávek, které již byly odeslané. PC používá Microsoft Windows 98 jako operační systém a aplikace pro řízení zásob používá databázi Microsoft Access. Dvakrát denně (od pondělí do pátku) se synchronizují záznamy o zásobách a objednávkách se serverem v kanceláři. Přenos souborů a synchronizace je spouštěna z počítače ve skladu. Ve skladu pracují 2 pracovníci a každý z nich může provádět všechny potřebné skladové operace.

Identifikovaná aktiva firmy WEB-SHOP

Typ aktiv	Identifikovaná aktiva	Hodnota aktiva
Informace	Databáze zboží internetového obchodu	5
	Databáze skladu	5
HW	Server	4
	PC	2
SW	Operační systémy	3
	Databázové systémy	3
Služby	Připojení serveru	5
	Připojení PC ve skladu	4

Identifikované hrozby a související zranitelnosti

Identifikovaná hrozba	Pravděpodob-nost hrozby	Příklad související zranitelnosti
Selhání hardware	3	Náchylnost zařízení na vlhkost, prach a ušpinění
Selhání software	3	Nejasné nebo neúplné specifikace pro vývojáře
Zpronevěření aktiv	3	Nedostatek fyzické ochrany budov, dveří a oken
Povodeň	2	Umístění v místech náchylných k povodním
Zlomyslné kódy	5	Nedostatek aktualizací softwaru na ochranu před zlomyslnými kódy
Neúmyslná modifikace	5	Nedostatečný výcvik bezpečnosti
Selhání komunikačních služeb	4	Nechráněná veřejná síťová připojení

Analýza rizik využívající matice aktiv, hrozeb a zranitelností (1)

	Popis aktiva	Databáze zboží internetového obchodu	Databáze skladu	Server	PC	Operační systémy	Databázové systémy	Připojení serveru	Připojení PC ve skladu
	Hodnota aktiva (A)	*5*	*5*	*4*	*2*	*3*	*3*	*5*	*4*
Popis hrozby	***Pravděpodobnost hrozby (T)***								
Selhání hardware	*3*			***2***	***2***				
Selhání software	*3*					***2***	***2***		
Zpronevěření aktiv	*3*			***1***	***3***				
Povodeň	*2*			***1***	***1***				
Zlomyslné kódy	*5*					***2***	***2***		
Neúmyslná modifikace	*5*	***2***	***5***						
Selhání komunikačních služeb	*4*							***5***	***4***

Analýza rizik využívající matice aktiv, hrozeb a zranitelností (2)

	Popis aktiva	Databáze zboží internetového obchodu	Databáze skladu	Server	PC	Operační systémy	Databázové systémy	Připojení serveru	Připojení PC ve skladu
	Hodnota aktiva (A)	*5*	*5*	*4*	*2*	*3*	*3*	*5*	*4*
Popis hrozby	***Pravděpodobnost hrozby (T)***								
Selhání hardware	*3*			***24***	***12***				
Selhání software	*3*					***18***	***18***		
Zpronevěření aktiv	*3*			***12***	**18**				
Povodeň	*2*			**8**	**4**				
Zlomyslné kódy	*5*					***30***	**30**		
Neúmyslná modifikace	*5*	***50***	**12 5**						
Selhání komunikačních služeb	*4*							**100**	**64**

Analýza rizik vyhodnocující pravděpodobnost incidentu a jeho dopad

Aktivum	Hodnota	Hrozba	Zranitelnosti	Pravděpodobnost incidentu	Dopad	Riziko	Opatření
Databáze zboží internetového obchodu	5	Neúmyslná modifikace	Nedostatečný výcvik bezpečnosti	10	5	50	Pravidelné zálohování
Databáze skladu	5	Neúmyslná modifikace	Nedostatečný výcvik bezpečnosti	25	5	125	
Server	5	Selhání hardware	Náchylnost zařízení na vlhkost, prach a ušpinění	6	4	24	
		Zpronevěření aktiv	Nedostatek fyzické ochrany budov, dveří a oken	3	4	12	Umístění v zamčeném prostoru, přístup pouze majitel firmy
		Povodeň	Umístění v místech náchylných k povodním	2	4	8	Umístění serveru v 2. patře
.....	.....	.....	.....	.....	.....	.....	.....