SECURITY 2011

19. ročník konference o bezpečnosti v ICT

Efektivní řízení rizik ISMS

Luděk Novák, Petr Svojanovský

ANECT a.s.

Obsah

- Proč řízení rizik ICT?
- Základní prvky řízení rizik ICT
- Příklady ohodnocení
- Potřeby řízení rizik ICT
- Registr rizik ICT
- Závěr

Motto:

Kdo chce vyřadit každé riziko, ten také zničí všechny šance.

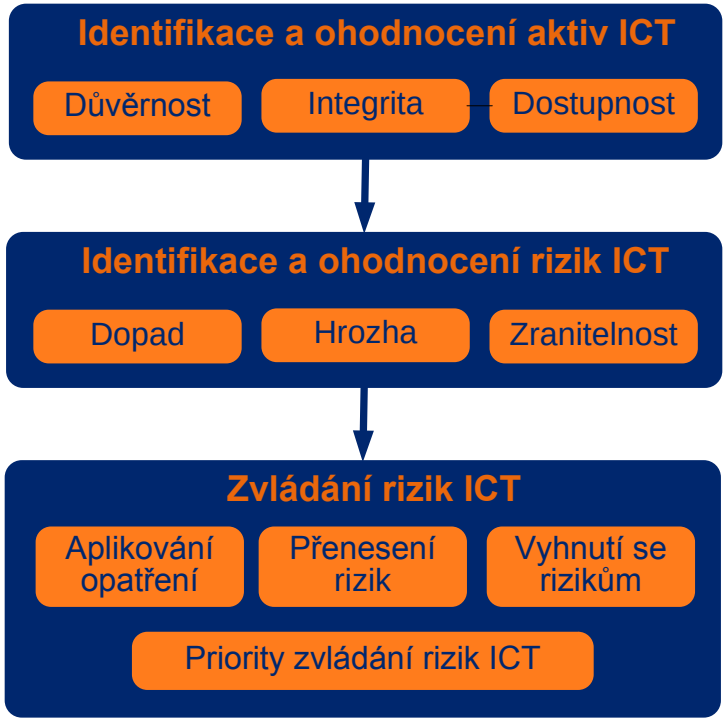
Proč řízení rizik ICT?

- Vzrůstá míra využití ICT pro uspokojování potřeb organizací
- Roste závislost fungování organizací na chodu ICT
- Trvale klesají odborné znalosti obsluhy ICT
- Stále vzrůstá složitost ICT

- Existuje příliš mnoho méně patrných závislostí, které mohou mít podstatný vliv na fungování systémů
- Další úspěšný rozvoj je podmíněn znalostí rizik ICT

Základní prvky řízení rizik ICT

- Ohodnocení aktiv ICT
  - Posouzení hodnoty aktiv z pohledu organizace
  - Ideální je vycházet z katalogu služeb ICT
- Ohodnocení rizik ICT
  - Identifikování možných hrozeb a jejich dopadů
  - Určení účinnosti existujících opatření
  - Posouzení jednotlivých rizikových scénářů
- Zvládání rizik ICT
  - Určení nezbytnosti a způsobu snižování rizika
  - Výběr vhodných bezpečnostních opatření
  - Sladění potřeb a možností – **určení priorit**
- Kvalita řízení rizik ICT rozhoduje o účelnosti řízení informatiky



Příklady ohodnocení aktiv

- Aplikační server 10.26.26.234
  - Důvěrnost: vysoká
  - Integrita: vysoká
  - Dostupnost. vysoká
- Operační systém
  - Důvěrnost: vysoká
  - Integrita: kritická
  - Dostupnost: střední
- Centrální router
  - Důvěrnost: střední
  - Integrita: střední
  - Dostupnost: střední
- PDA ředitele
  - Důvěrnost: nízká
  - Integrita: kritická
  - Dostupnost: kritická
- Služba: Service desk
  - Důvěrnost: 2 – pomocné informace
  - Integrita: 3 – slouží jako báze znalostí
  - Dostupnost: 3 – podpora činností IT max. výpadek 8h
- Databáze zákazníků
  - Důvěrnost 4 – osobní údaje
  - Integrita 4 – osobní údaje
  - Dostupnost 3 – výpadek v řádu jednoho pracovního dne nezpůsobí vážnější potíže

Příklady ohodnocení rizik

- Požár
  - Dopad: kritický
  - Hrozba: střední
  - Zranitelnost: nízká
  - Riziko: střední
- Selhání zařízení
  - Dopad: kritický
  - Hrozba: střední
  - Zranitelnost: nízká
  - Riziko: střední
- Prozrazení informací
  - Dopad: kritický
  - Hrozba: střední
  - Zranitelnost: vysoká
  - Riziko: vysoké

- **Požár datového centra A46**
  - Dopad: 4 – nefunkčnost primárních serverů (částečné záloha výkonu)
  - Hrozba 2 – náhodné selhání technologie, nedodržování pravidel DC
  - Zranitelnost 1 – požární čidla, zhášení
  - Riziko 2 – pravidelné kontroly DC
- **Prozrazení osobních údajů**
  - Dopad: 3 – porušení zákonných povinností, pokuta
  - Hrozba 3 – podezření na úniky (neprokázáno)
  - Zranitelnost 2 – identifikace uživatele, omezení přístupových práv, důsledné logování činností, namátkové kontroly
  - Riziko 2 – potřeba prohloubit program bezpečnostního povědomí

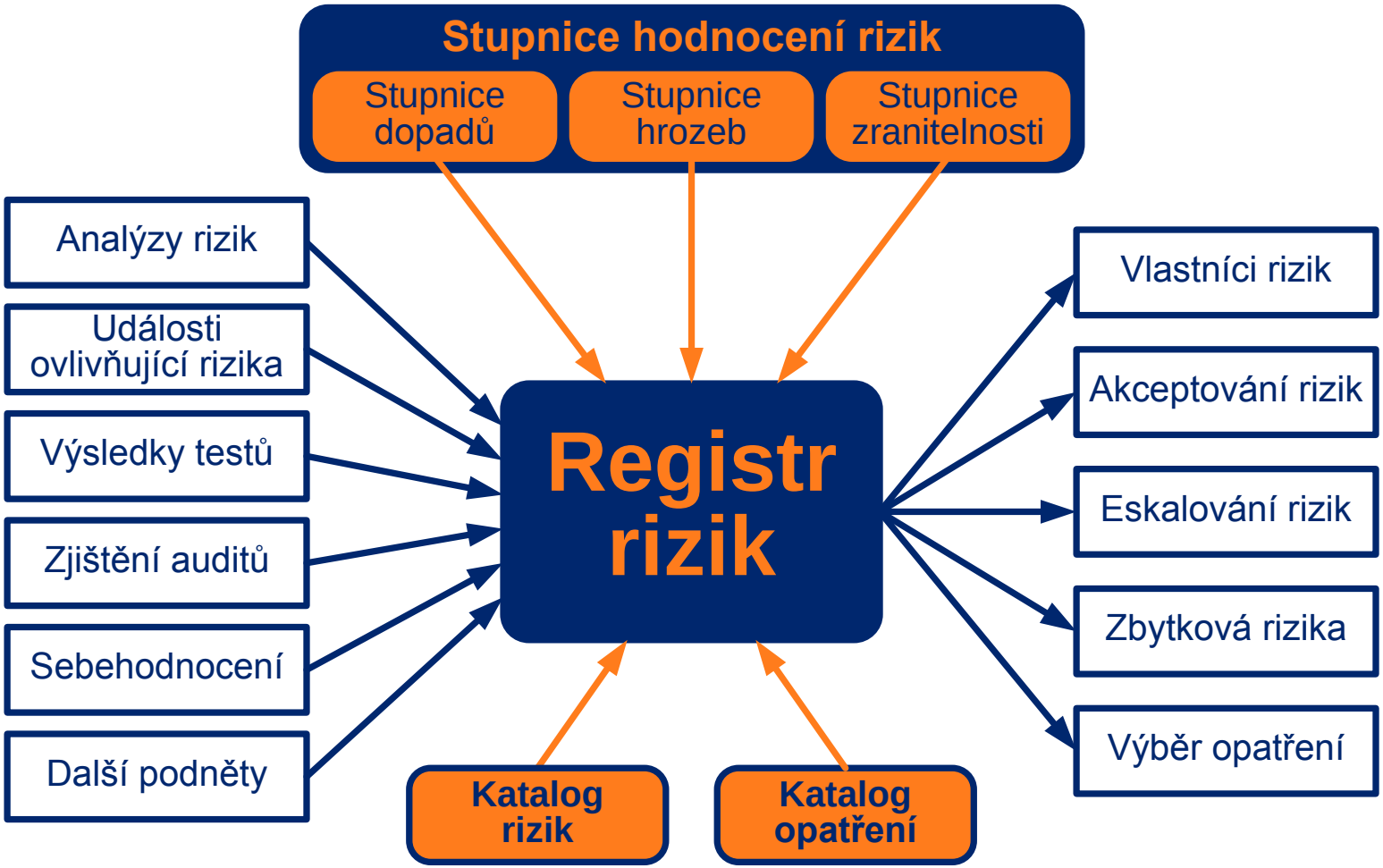
Příklad přehledu rizik

			Stupeň dopadu			Stupeň hrozby			Stupeň zranitelnosti			Stupeň rizika		
001	Porušení pravidel ochrany duševního vlastnictví, využívání nelegálního programového vybavení	Ano	Vysoký	20,0	Porušení právního řádu ČR	Střední	35%	Instalace nelegálního SW	Střední	40%	Není reverzní kontrola licencí	Střední	2,8	Není dostatečné povědomí o pravidlech
002	Nedostupnost informací a služeb ICT, selhání systému	Ano	**Kritický**	**50,0**	**Ohrožení chodu xx**	Střední	50%	Selhání HW nebo komunikačních služeb	Střední	40%	Decentralizovaný charakter systému	Vysoký	10,0	Připravit krizové plány a postupy
003	Rizika spojená se špatnou organizací nebo koordinací managementu bezpečnosti informací včetně nejednoznačně stanovené odpovědnosti	Ano	Vysoký	20,0	Nesoulady při prosazování pravidel bezpečnosti	Střední	35%	Špatná koordinace mezi	Střední	40%	Není důsledně řešeno	Střední	2,8	
004	Nerespektování pravidel definovaných v dokumentu Politika bezpečnosti informací	Ano	Vysoký	25,0	Porušení bezpečnostních pravidel	Střední	30%	Nevědomé dodržování pravidel	**Kritický**	**80%**	**Dokument neexistuje**	Vysoký	6,0	Definovat politiku bezpečnosti informací
005	Nedostatečné povědomí pracovníků o bezpečnosti informací	Ano	Vysoký	25,0	Porušení bezpečnostních pravidel	Střední	40%	Nízká znalost pracovníků	**Kritický**	**80%**	**Neprobíhá pravidelná příprava**	Vysoký	8,0	Plán školení o bezpečnosti
006	Ohrožení osobních údajů a jejich nedostatečná ochrana ve smyslu zákona č. 101/2000 Sb.	Ano	**Kritický**	**40,0**	**Poškození dobré pověsti, soudní spory, ohrožení osob**	Vysoký	65%		Vysoký	65%		Vysoký	16,9	Potřeba vymezit a prosadit OOÚ pro všechny zainteresované osoby
007	Nebezpečí a škody způsobené požárem	Ano	Vysoký	30,0	Nefukčnost části systému	Nízký	10%	Nízká pravděpodobnost požáru	Nízký	20%		Nízký	0,6	dáno místními podmínkami, pravidla pro serverovny (umístění, apod.)
008	Nebezpečí a škody způsobené zaplavením vodou	Ano	Vysoký	30,0	Nefukčnost části systému	Nízký	25%	Možnost úniku vody z potrubí, klimatizace	Střední	40%	Někde se problémy objevují	Střední	3,0	dáno místními podmínkami, pravidla pro serverovny (umístění, apod.)
009	Nebezpeční a škody způsobené znečištěním, prachem, chemikáliemi, vibracemi apod.	Ano	Vysoký	20,0	Nefukčnost části systému	Nízký	10%	Prostředí není rizikové	Nízký	20%		Nízký	0,4	dáno místními podmínkami, pravidla pro serverovny (umístění, apod.)
010	Omezení dodávky elektrické energie	Ano	Vysoký	30,0	Nefukčnost části systému	Střední	30%	Střednědobé a dlouhodobé výpadky	Nízký	20%	UPS a diesel standard	Střední	1,8	ověřit připojení všech pracovišť a vyzkoušet funkčnost diesel agregátů
011	Poškození či nedostatečná fyzická ochrana aktiv (zařízení, kabeláž, media apod.)	Ano	Vysoký	30,0	Ohrožení fyzických aktiv	Střední	30%	Ohrožení mobilních prostředků	Střední	30%		Střední	2,7	
012	Neautorizovaný fyzický přístup nepovolaných osob	Ano	Vysoký	30,0	Ohrožení fyzických aktiv	Nízký	10%	Propracovaná fyzická ostraha	Nízký	20%		Nízký	0,6	

Co dnes vlastně potřebujeme?

- Každodenní řízení rizik ICT
  - Úroveň rizika by měla být určena rychle
  - Riziko by mělo být včas předáno k řešení
  - Sledování rizika během procesu jeho zvládání
  - Úzké propojení (splynutí) s řízením informatiky
- Zapojení širokého spektra informačních zdrojů
  - Již existující znalosti o rizicích ICT
  - Informace získávané během prověřování stavu informatiky
  - Metody sebehodnocení (management, uživatelé, informatici)
  - Podněty všech zainteresovaných osob apod.
- Přehled a evidenci rizik ICT
  - Určování priorit pro zvládání rizik
  - Efektivní práce s riziky a sledování jejich vývoje
  - Pravidelné přehodnocení systému řízení rizik

Registr rizik – Jádro řízení rizik



Častá pochybení

- Rizika neodrážení skutečné problémy organizace
- Řízení rizik není práce s přesnými ukazateli, ale pouze více či méně přesnými odhady
- Řešení nevede k vytvoření kvalitního a srozumitelného registru rizik (často nesrozumitelné podrobnosti)
- Výsledkem řízení rizik není stanovení priorit
- Vlastníci aktiv/rizik/opatření netuší, že jsou vlastníci
- Není kladen důraz na skutečné pochopení významu hodnot při hodnocení rizik – chybí jakékoli komentáře
- Často není patrný řetězec „aktivum – riziko – opatření – co udělat – reziduální riziko“

Trendy do budoucna

- Vyšší snaha o řízení „správných“ rizik
  - Zbytečné nízké riziko vede k plýtvání či omezení uživatelů
- Modelování práce s riziky – zatím často intuitivně
  - Modelování skutečné schopnosti opatření redukovat riziko (politika versus hasící přístroj?)
  - Modelování a účelná manipulace s vyspělostí opatření
- Integrování procesu zvládání incidentů
  - Srovnání reálného života s modelem popisujícím rizik

ZÁVĚR

- Řízení rizik ICT prohlubuje efektivní řízení informatiky
- Řízení rizik ICT umožňuje účinněji využít výhod soudobých možností ICT
- Potřeba aplikovaní vhodných metod řízení rizik od strategického plánování po každodenní činnosti
- Využití širokého spektra informačních zdrojů zpřesňuje a snižuje náročnost řízení rizik ICT
- Je důležité nalézt společný jazyk, který umožňuje otevřenou komunikaci o rizicích

SECURITY 2011

19. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Luděk Novák
ANECT a.s.
ludek.novak@anect.com