ANECT

Řízení rizik ICT účelně a prakticky?

Luděk Novák, Petr Svojanovský, ANECT a.s.

ISSS

12. – 13. dubna 2010, Hradec Králové

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 informačních a komunikačních systémů pro uspokojování potřeb organizací**
- **Roste závislost fungování organizací na chodu informačních a komunikačních systémů**
- **Trvale klesají odborné znalosti obsluhy informačních a komunikačních systémů**
- **Stále vzrůstá složitost informačních a komunikačních systémů**

- **Existuje mnoho málo zřetelných závislostí, které mohou mít podstatný vliv na fungování systémů**
- **Další úspěšný rozvoj je podmíněn znalostí rizik ICT**

ANECT

ZÁKLADNÍ PRVKY ŘÍZENÍ RIZIK ICT

- **Ohodnocení aktiv ICT**
  - Posouzení hodnoty a přínosů 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 informačních rizik**
  - Určení nezbytnosti a způsobu snižování míry rizika
  - Výběr vhodných bezpečnostních opatření
  - Sladění potřeb a možností – **určení priorit pro zvládání**

- **Kvalita analýzy a zvládání informačních rizik rozhoduje o účinnosti a efektivnosti řízení informatiky**

ANECT

PŘÍKLADY OHODNOCENÍ AKTIV

- **Aplikační server 10.26.26.234**
  - Důvěrnost: vysoká
  - Integrita: vysoká
  - Dostupnost. vysoká
- **Operační systém linux/windows**
  - Důvěrnost: vysoká
  - Integrita: kritická
  - Dostupnost: střední
- **Centrální router**
  - Důvěrnost: střední
  - Integrita: střední
  - Dostupnost: střední
- **PDA tajemníka úřadu**
  - Důvěrnost: nizká
  - 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
- **Obecní databáze občanů**
  - Důvěrnost 4 – osobní údaje
  - Integrita 4 – osobní údaje
  - Dostupnost 3 – výpadek v řádu 1 pracovního dne nezpůsobí vážnější potíže

ANECT

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 úřadu
  - Hrozba 3 – podezření na úniky údajů v minulosti (nebylo prokázáno)
  - Zranitelnost 2 – identifikace uživatele, omezení přístupových práv, důsledné logování činností, namátkové kontroly
  - Riziko 2 – potřeba prohloubit program bezpečnostního povědomí

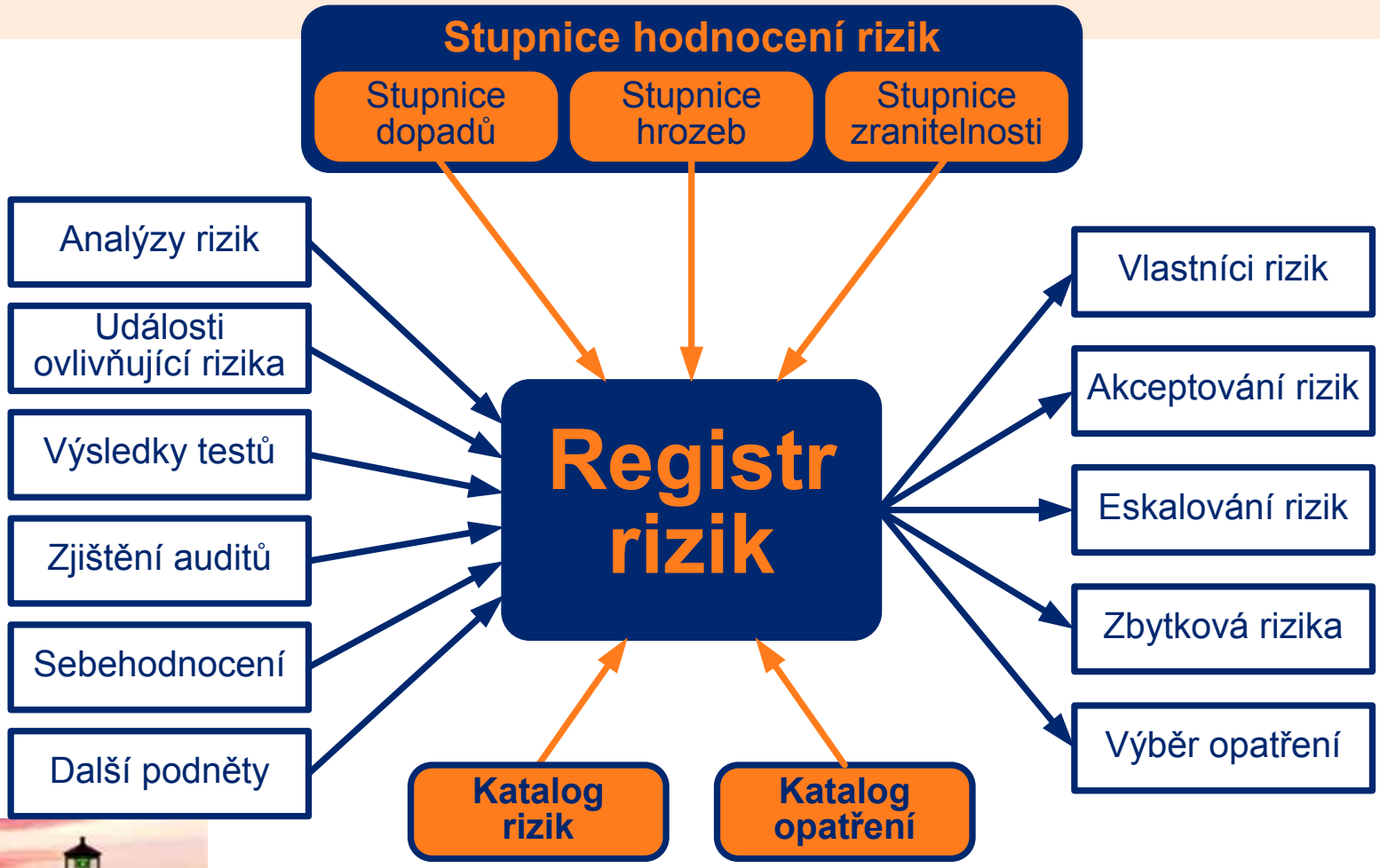
ANECT

CO DNES VLASTNĚ POTŘEBUJEME?

- **Každodenní řízení rizik**
  - 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 informačních rizicích
  - Informace získávané během prověřování stavu informatiky
  - Metody sebehodnocení (management, uživatelé, informatici)
  - Podněty všech zainteresovaných osob apod.
- **Přehled a evidenci informačních rizik**
  - Určování priorit pro zvládání rizik
  - Efektivní práce s riziky a sledování jejich vývoje
  - Pravidelné přehodnocení systému řízení informačních rizik

ANECT

REGISTR RIZIK – JÁDRO SYSTÉMU ŘÍZENÍ RIZIK



ZÁVĚR

- **Řízení rizik ICT prohlubuje efektivní řízení informatiky**
- **Řízení rizik ICT umožňuje účinněji využít výhod soudobých možností informačních a komunikačních technologií**
- **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**

Děkuji za pozornost!

ludek.novak@anect.com
petr.svojanovsky@anect.com

ANECT