# Plánování v rámci ISMS

František Steiner
Západočeská univerzita v Plzni



## Agenda

- Základní pojmy
- Ustavení ISMS
- Management rizik
- Analýza rizik
- Metody analýzy rizik



## Základní pojmy

- Aktivum – cokoliv, co má pro organizaci cenu
- Hrozba – potenciální příčina incidentu, která může mít za následek poškození systému nebo organizace
- Zranitelnost – slabá stránka aktiva nebo skupiny aktiv, která může být využita jednou nebo více hrozbami

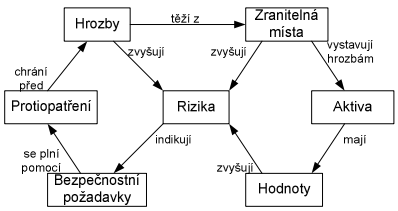


## Základní pojmy

- Riziko – je potenciální možnost, že daná hrozba využije zranitelností aktiv nebo skupiny aktiv a způsobí tak ztrátu nebo zničení aktiv
- Riziko – kombinace pravděpodobnosti výskytu události a jejich následků

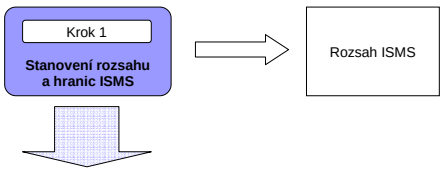


## Vzájemné vztahy při správě rizik

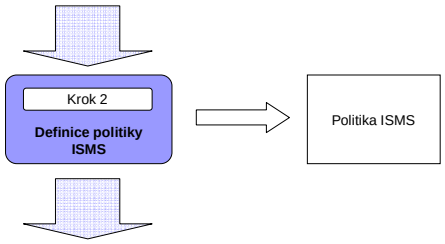





## Ustavení ISMS

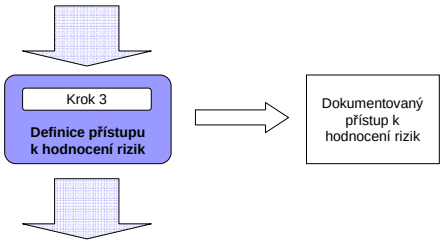


## Ustavení ISMS



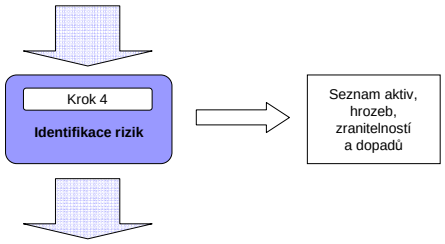

7

## Ustavení ISMS



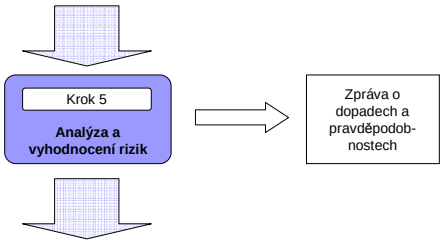

8

## Ustavení ISMS



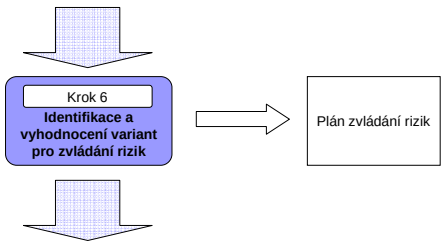

9

## Ustavení ISMS



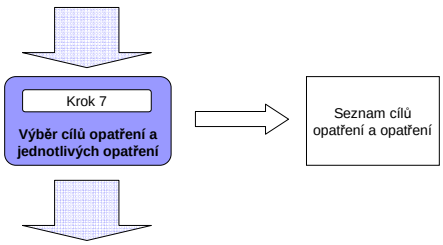

10

## Ustavení ISMS



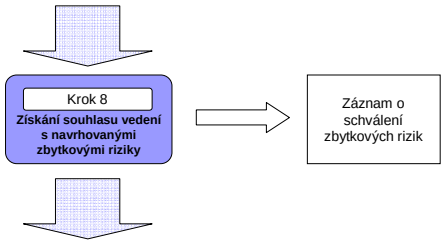

11

## Ustavení ISMS



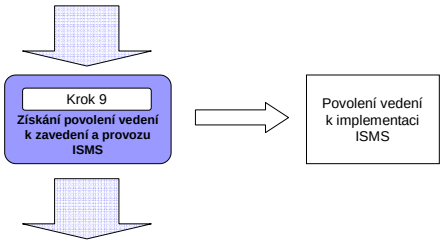

12

## Ustavení ISMS



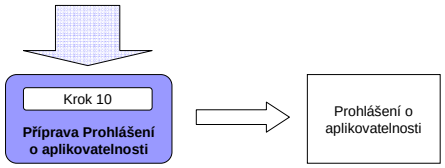

13

## Ustavení ISMS




14

## Ustavení ISMS

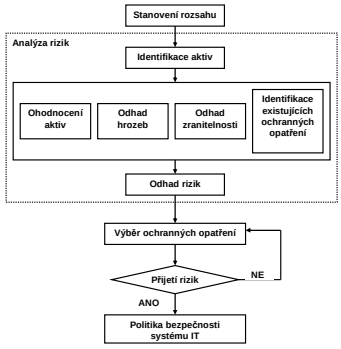



15

## Management rizik (ČSN ISO/IEC TR 13335 )

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

16




17

## Management rizik (BS 7799-3)

- Posouzení a hodnocení rizik
- Výběr, implementace a provoz nástrojů řízení pro ošetření rizik
- Monitorování a přezkoumání rizik
- Udržování a zlepšování nástrojů řízení rizika

18

## 100 % bezpečnost ?

***Bezpečný systém*** je pouze takový, který je vypnut a odpojen, uzamčen ve vyztuženém titanovém trezoru, který je zabetonován v bunkru a obklopen nervovým plynem, a to vše je střeženo velmi dobře placenými ozbrojenými strážci.

Gene Spafford
Computer Operations, Audit, and Security Technology (COAST)
Purdue University

19

## Obecný postup analýzy rizik

- Stanovení hranice analýzy rizik
- Identifikace aktiv
- Stanovení hodnoty a seskupování aktiv
- Identifikace hrozeb
- Analýza pravděpodobnosti hrozeb a zranitelností
- Identifikace používaných opatření
- Výpočet rizika

20

## Aktiva

- Co jsou aktiva?
- Aktivum je něco, co má pro organizaci hodnotu a z tohoto důvodu ho musí organizace chránit
- Musí být relevantní rozsahu systému řízení bezpečnosti informací

21

## Aktiva

- Příklady aktiv spojovaných s informačními systémy jsou:
  - Informační aktiva - datové soubory, uživatelská dokumentace atd.
  - Papírové dokumenty – smlouvy, směrnice atd.
  - Software – aplikační a systémový SW atd.
  - Fyzická aktiva – počítač, média atd.
  - Lidé – zákazníci, personál atd.
  - Image a dobré jméno
  - Služby – komunikační, odborné atd.

22

## Hodnoty aktiv (a potenciální dopady)

- Má organizace identifikované hodnoty jejich informačních aktiv?
- Určení hodnoty každého aktiva je první krok ke stanovení efektivní bezpečnostní strategii
- Jaký systém – 0 až 5 nebo nízká až velmi vysoká
- Jsou životně důležité složky procesu analýzy rizik

23

## Hodnota aktiv

- Dle ISO/IEC 27001, aktiva nemusí nutně zahrnovat všechny věci normálně považované za cenné
- Organizace musí určit, která aktiva mohou svou absencí nebo porušením ovlivnit dodávku produktu/služby

24

## Hrozby

- Potenciální příčina nežádoucího incidentu, který může mít za následek poškození organizace a jejích aktiv
- Úmyslné nebo náhodné, způsobené člověkem nebo vyšší mocí
- Aktiva jsou předmětem mnoha druhů hrozeb, které využívají zranitelností

25

## Příklady hrozeb

| **Lidské hrozby** | | **Hrozby prostředí** |
|---|---|---|
| Úmyslné | Náhodné | |
| Odposlech<br>Změna informace<br>Hacking systému<br>Nepřátelský program<br>Krádež | Chyby a opomenutí<br>Vymazání souboru<br>Nesprávné směrování<br>Fyzické nehody | Zemětřesení<br>Blesk<br>Povodeň<br>Požár |

26

## Zranitelnosti

- Zranitelnost je slabina/díra informační bezpečnosti organizace
- Zranitelnost sama o sobě nezpůsobuje poškození, je to pouze okolnost nebo soubor okolností, které umožní hrozbě ovlivnit aktiva
- Není-li zranitelnost řízena, umožní hrozbě působit na aktiva

27

## Příklady zranitelností

- Absence vedoucího pracovníka
- Nestabilní elektrická síť
- Nechráněná kabeláž
- Nedostatek bezpečnostního povědomí
- Chybně přiřazená přístupová práva
- Nedostatečný bezpečnostní výcvik
- Neinstalovaný firewall
- Nezamčené dveře

28

## Posouzení hrozeb a zranitelností

- Úmyslné hrozby
- Náhodné hrozby
- Minulé incidenty
- Nový vývoj a trendy

29

## 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

30

## Typy analýzy rizik (ČSN ISO/IEC TR 13335 )

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

31

## Typy analýzy rizik (ČSN ISO/IEC TR 13335 )

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

32

## Podrobná analýza rizik

- 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

33

## Kombinovaná analýza rizik

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

34

## Metody analýzy rizik

35

## 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 |

36

## 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 |

37

## 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 |

38

## 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 |

39

## 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* |

40

## 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* |

41

## Analýza rizik vyhodnocující pravděpodobnost incidentu a jeho dopad

| Aktivum | Hodnota | Hrozba | Zranitelnosti | Pravděpodob-nost incidentu | Dopad | Riziko | Opatření |
|---|---|---|---|---|---|---|---|
| Aktivum 1 | 5 | Hrozba A | Zranitelnost 1 | 5 | 4 | 20 | Opatření 1 |
| | | | Zranitelnost 3 | 3 | 2 | 6 | |
| | | | Zranitelnost 5 | 4 | 5 | 20 | |
| | | Hrozba C | Zranitelnost 2 | 1 | 1 | 1 | |
| | | | Zranitelnost 4 | 3 | 2 | 6 | |
| | | | | | | | |
| | | Hrozba D | Zranitelnost 4 | 2 | 3 | 6 | |
| | | | Zranitelnost 5 | 2 | 3 | 6 | Opatření 2 |
| | | | Zranitelnost 6 | 4 | 3 | 12 | |

42

## Softwarové nástroje

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

43