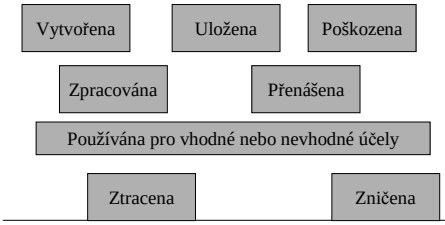
Bezpečnost informací - základní pojmy

Životní cyklus informace

- Informace může být



Druhy informací

- Tištěná nebo psaná na papír
- Elektronicky uložená
- Přenášená poštou nebo elektronicky
- Předváděná např. na videu
- Verbálně sdílená

Co je informační bezpečnost

- Důvěrnost – zajištění, že informace je přístupná pouze osobám autorizovaným pro přístup k nim
- Integrita – zabezpečení přesnosti a úplnosti přenášené informace a metod přenosů
- Dostupnost- zajištění toho, že autorizovaní uživatelé mají přístup k informacím a informačním aktivům kdykoli jej potřebují

Klasifikace podílů na ztrátách

- 50 – 80% ztrát je způsobeno managementem vlastní organizace
- 10 – 30% ztrát je způsobeno vlastními zaměstnanci
- 5 – 8% ztrát je způsobeno „vyšší mocí"
- 0 – 8% ztrát je způsobeno útoky zvenku

Proč zavádět systematickou ochranu dat v manažerských systémech?
Co přináší zavedení systému řízení ochrany dat

- **Výchova personálu k šetrnému zacházení s citlivými daty**
- **Optimalizace sběru , přenosu a ochrany dat**
- **Zvýšení povědomí & zlepšení řídicích mechanizmů**
- **Ochrana existujících dat proti ztrátě nebo zničení**
- **Zajištění shody s právními předpisy**
- **Jaká je současná situace?**
  - **Malá informovanost o rizicích i zranitelnostech v rámci vlastního systému**
  - **Málo řídicích i kontrolních mechanizmů**
  - **Zvýšená rizika prozrazení, zničení a úniku dat**
  - **Riziko ztráty důvěryhodnosti**

Proč se systematicky zabývat nakládáním s informacemi v rámci řízení?

Informace má svou kvalitu, když je

- Dostupná
- Integrovaná
- Dostupná - nezcizitelná

Kde jsou největší ohrožení kvality informací?

Informace s vysokou hodnotou pro podnik musí být chráněny tak

- Aby k nim měly přístup pouze oprávněné osoby
- Aby se dalo zjistit, kdo je vytvořil, změnil nebo odstranil
- Aby nebyly nekontrolovatelným způsobem vyřazeny
- Aby byly dostupné tehdy, když jsou potřebné

Kritické faktory úspěchu

- Politika bezpečnosti zohledňující podnikatelské cíle organizace
- Viditelná podpora a závazek vedení
- Dobré chápání požadavků na bezpečnost, analýzu rizik a management rizik
- Efektivní sdílení bezpečnosti se všemi managery i zaměstnanci

Kritické faktory úspěchu

- Správná míra dokumentace týkající se politiky informační bezpečnosti a požadavků na bezpečnost platná pro zaměstnance a dodavatele a zákazníky
- Správná míra výcviku a vzdělávání
- Vyvážený systém měření pro vyhodnocení výkonnosti managementu informační bezpečnosti a poskytnutí zpětné vazby pro doporučení ke zlepšování

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

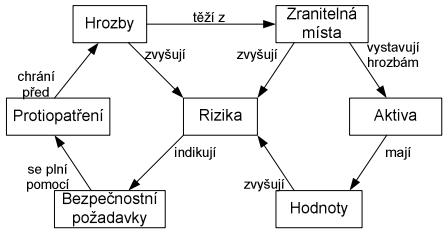
Základní pojmy

- 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



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

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.

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

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

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

Příklady hrozeb

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

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

Příklady zranitelností

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

Zranitelnosti organizačního charakteru

- Není definována bezpečnostní politika
- Nejsou definovány odpovědnosti zaměstnanců a dodavatelů
- Nejsou vytvořeny pravidla pro přístup k informacím a nakládání s informacemi a informačními prostředky
  - směrnice,
  - pracovní postupy
  - plány kontinuity
- Není prováděna monitoring a kontrola
- Zaměstnanci nejsou dostatečně a pravidelně proškolování
- Chybí smlouvy s dodavateli nebo neobsahují závazek mlčenlivosti
- Nejsou určena pravidla pro pohyb dodavatelů v budovách
- Požadovaná doba dostupnosti agend neodpovídá době obnovy ostatních aktiv

Zranitelnosti organizačního charakteru (pokračování)

- Neprovádějí se pravidelné zálohy databází
- Management se nezabývá zjišťováním rizik
- Nejsou vedeny záznamy o důležitých činnostech
- Nejsou prověřování zaměstnanci vlastní ani zaměstnanci dodavatelů
- Není omezen přístup k informacím
- Zaměstnanci si neuvědomují význam informací
- Neprovádí se řízené vytváření kopií a skartace
- Používání sdílených účtů a hesel
- Data umístěná na lokálních discích
- Neprovádí se bezpečné skladování a spolehlivá likvidace obsahu nepotřebných paměťových médií a dokumentů

Zranitelnosti technického charakteru

- Nevhodné použití prostor pro spisovny servery, rozvody sítí,
- Nevhodné umístění informačních prostředků
- nevhodné použití nebo uskladnění záložních médií
- Nedostatečná kapacita nebo výkon informačních prostředků
- Nefunkční alarmy, požární detektory a jiné bezpečnostní prvky
- Nespolehlivá dodávka energií
- Bezdrátový přenos není šifrován
- Snadno přístupné kabelové rozvody sítí a dalších prvků sítě (rozvaděče, zásuvky)
- Nedostatečné překážky fyzického vstupu do budov nebo prostor
- Nespolehlivý hardware (překročení životnosti
- Sdílené tiskárny nebo počítače na chodbách
- Absence fyzických překážek pro přístup do prostor s informačními prostředky
- Chybějící HW firewall

Zranitelnosti softwaru

- Chybí antivirový antispyware software nebo neaktualizovaná antivirová databáze
- Zastaralé operační systémy bez omezení přístupu (DIS, Windows 9x)
- Nevhodné databáze pro informační systémy (chybí kontrola integrity)
- Nevhodně použité aplikační systémy
- Chybějící uživatelské účty informačních systémů
- Přístup bez hesla nebo použití slabých hesel
- Používání software neznámého původu
- Používání (instalace) nových verzí IS bez předchozího testování
- Chybějící nebo špatně parametrizovaný SW Firewall
- Chybové aktualizace software

Posouzení hrozeb a zranitelností

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

Mýty a omyly

- Není nutné vytvářet směrnice a dokumentované postupy. Stačí platná legislativa, kterou přece každý musí znát.
- Největším nebezpečím pro organizaci jsou hackeři.
- Pokud se provádí záloha dat a je nainstalován antivirový program, nemůže se nic stát.
- Osobním údajem je rodné číslo, které se na dokladech musí začernit, aby ho nikdo nezneužil.
- atd.

Typické zranitelnosti v praxi

- Přístup cizích subjektů – pronájmy prostor, outsorcing (ostraha, úklid) bez dostatečných kontrol
- Předávání informací dodavatelům – pronájmy serverů, komunikačních linek, apod. bez dostatečných kontrol
- Neznalost a důvěřivost zaměstnanců
- Univerzální klíče od kanceláří, spisoven, serverů
- Nevhodné prostory a podmínky pro archivy
- Nevhodně používaný internet
- Neprovádí se bezpečné skladování a spolehlivá likvidace obsahu nepotřebných paměťových médií a dokumentů