Bezpečnostní politika

- Soubor zásad a pravidel, jejichž pomocí organizace chrání svá aktiva
  - Aktiva – co firma má (značky, finance, nemovitosti)
- Kritické zařízení – věci, bez kterých se neobejdeme
- Základní rozdělení – důležitost
- Rozdělení v závislosti na:
  - Počtu uživatelů
  - Kritičnosti systému
  - Interaktivitě práce

Druhy

1) Promiskuitní
   - Bez ochrany, vše je povoleno
   - Například domácí PC
2) Liberální
   - Je psáno, co se nesmí
   - Například naše zákony
   - **Nevýhoda:** může být špatně napsáno (využití kliček)
   - Užití ve středních organizacích
3) Konzervativní
   - Je psáno, co je povoleno
   - Pro velké systémy s velkým počtem uživatelů
4) Paranoidní
   - Je zakázáno vše až na omezené akce
   - Například čip ve školní jídelně

Certifikace	Role a autorita	Akreditace
Dozor	Bezpečnostní politika	Reakce na výjimečné situace
Monitoring a audit	Evaluace	Řízení rizik

Certifikace

- Proces ohodnocení, zkoušení a testování jakosti i způsobu
- Ověření, že jsme něco dokázali
- **Certifikační autorita** – důvěryhodná instituce

Akreditace

- Že systém splňuje podmínky

Role a autorita

- Bezpečnostní rada:
  - Řeší bezpečnostní politiku
  - Schvaluje politiky
  - Hodnotí uskutečněné politiky
  - Vynucuje opatření
- Bezpečnostní manažer – implementuje rozhodnutí rady
- Bezpečnostní správce – aplikuje implementaci manažera
- Bezpečnostní auditor – bezpečnostní orgán

Monitorování a audit

- Nepřetržitý proces realizující
  - Kontrolu dodržování přijatých opatření
  - Vyhodnocení záznamů v auditních a logovacích systémech

Aktualizace dokumentace

Auditní postup:

1) **Detekce** – zjištění události mající vliv
2) **Rozlišení** – zapsání nebo spuštění poplachu
3) **Zpracování** poplachu – vysvětlení a opatření k události
4) **Analýza** – posouzení kontextu z předchozích událostí
5) **Agregace** – součet, počet, vyhodnocení dominového efektu a synergie
6) **Generování zprávy** – auditní zpráva z auditních záznamů
7) **Archivace** – uchování záznamů o události

Evaluace

- Periodické (minimálně každé 3 roky) – hodnocení IS
- Základ pro změnu BP (hodnocení rizik)

Dozor

- Kontrolní orgán
- Osoby odpovědné za dodržování BP
- Možno i externí

Řízení rizik

- Oblast procesů zabývajících se identifikací, minimalizací, eliminací a řízením rizik

Riziko

- Potencionální možnost že se stane událost, která bude mít vliv na výsledek
- Je potencionální hrozba, lze eliminovat

Hrozba

- Akutně neodvratitelná akce s dopady, lze zmírnit

Identifikace rizika

a) Ohrožení životů, zdraví a životního prostředí
b) Komerční a smluvní vztahy

c) Ekonomické události
d) Politické hrozby
e) Přírodní hrozby – povodně, záplavy, sopka
f) Enviromentální hrozby – emise
g) Fyzické hrozby – požár, kontaminace, poškození vodou
h) Technické hrozby – porucha PC / sítě
i) Technologické hrozby
    a. Externí – viry, závislost na dodavatelích
    b. Interní – nevhodné inovace
j) Lidské hrozby
    a. Neúmyslné – překlep, chyba, zničení, bránění v přístupu (zapomenutí hesla), vyzrazení tajných dat
    b. Úmyslné – interní
        - Zhrzený zaměstnanec s know-how
        - Návštěva
        - Zneužití informace
        - Defraudace – využití cizích peněz
        - Sabotáž – backdoor
    c. Úmyslné – externí
        - Hacker – protože může
        - Špionáž
        - Vandal
        - Terorista – aby se lidé báli
        - Cracker – zpřístupňuje placený software
        - Phishing
        - Blackmailing
k) Ohrožení dobrého jména