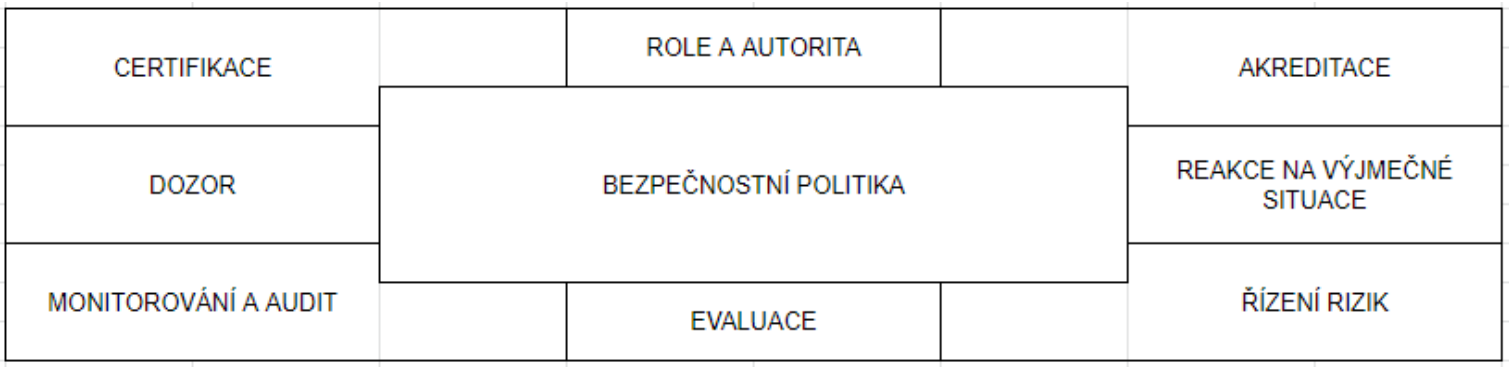
25.

Bezpečnostní politika – druhy, základní části a pojmy, auditní postup

Soubor zásad a pravidel s jejíž užití chrání organizace svá aktiva

Aktiva - Peníze, materiál, know-how, čas, lidi



Základní typy politiky

1. Promiskuitní
   Vše je povoleno
   Př: pc v domácnosti
2. Liberální
   Co není povoleno je výslovně uvedeno
   Př: malá organizace (síťové prostředí)
3. Konzervativní
   Co je povoleno je výslovně uvedeno
   Př: velká organizace
4. Paranoidní
   Vše je zakázáno až na přesné výjimky
   Př: veřejné terminály

CERTIFIKACE

Proces ohodnocení atestace a zkoušení a testování jakosti, ale i způsobilosti pracovníků podle daných norem

Certifikační autorita

- Důvěryhodná instituce, která vydává svým zákazníkům certifikáty
- Př: městský úřad, pošta

AKREDITACE

Proces formálního uznání, že systém splňuje požadavky certifikace
(certifikace pro instituci pro vydávání certifikátu)

ROLE A AUTORITA

Pro zajištění bezpečnostní politiky je v podniku sestavena organizační struktura

Bezpečnostní rada

- Řeší bezpečnostní politiku
- Schvaluje politiky přípustného použití aktiv
- Hodnotí uskutečnění
- Vynucuje bezpečnostní opatření

Bezpečnostní manažer

- Řídí implementaci rozhodnutí bezpečnostní rady

Bezpečnostní správce

- Výkonný orgán

Bezpečnostní auditor

- Hlavní kontrolní orgán

MONITOROVÁNÍ A AUDIT

Nepřetržitý proces realizující:

- Kontrolu a dodržování defensivních opatření (využití firemní pošty pro osobní účely)
- Vyhodnocení záznamu auditních a logovacích souborech
- log(kdo/kdy přišel) audit (kolikrát co se kdy stalo)
- Aktualizace dokumentace

Auditní postup

1. **D**etekce - zjištění události
2. **R**ozlišení - určuje prioritu opatření (audit záznam/poplach)
3. **Z**pracování bezpečnostního poplachu - vysvětlení/opatření
4. **A**nalýza
    - Posouzení události v kontextu předchozích událostí a možných dopadů
    - Dominový efekt
    - Synergetický efekt (více malých -> jeden velký)
5. **A**gregace - distribuované záznamy -> jeden
6. **G**enerování zprávy - z bezpečnostních auditních záznamů je zpracována auditní zpráva
7. **A**rchivace - uchování záznamů a přijatých opatření

EVALUACE

Pravidelné periodické (min. 3 roky) hodnocenní bezpečnosti

Na základě evaluace se upravuje bezpečnostní politika

- Cíl - kompromis mezi rizikem a náklady na protiopatření

DOZOR

Stanovení odpovědných osob za bezpečnostní politiku včetně rozsahu pravomocí a postihů

Doplňuje role a autority v podniku (může být i externí)