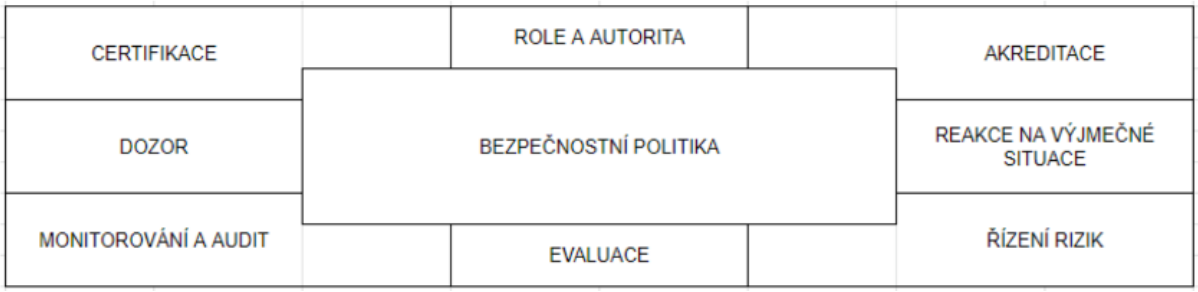
15. Bezpečnostní politika – druhy, základní části a pojmy, auditní postup

Bezpečnostní politika

- Soubor zásad a pravidel s jejichž pomocí organizace chrání svá aktiva.
  - Organizace – s.r.o., akciová společnost, …
  - Aktiva – peníze, materiál, movitosti, nemovitosti, finance, pohledávky, čas, lidi, know-how
  - Pasiva – dluhy, závazky, úvěry, …

Druhy



Rozdělení v závislosti na (zásady)

- Počet uživatel
- Kritičnost systému
- Interaktivita práce

Základní typy politiky

Promiskuitní

- Vše dovoleno
- Domácí PC

Liberální

- Vše povoleno, kromě napsaných podmínek (naše společnost).
- Střední organizace, nekritické systémy

Konzervativní

- Co je povoleno, je výslovně uvedeno.
- Pro kritické systémy.
- Velký počet interaktivních uživatelů.

Paranoidní

- Je zakázáno vše, až na omezené akce (přesné výjimky).
- Veřejné terminály

Základní části a pojmy

Certifikace

- Proces ohodnocení atestace, zkoušení a testování jakosti, ale i způsobilosti pracovníků podle daných norem.
- Certifikační autorita
    - Důvěryhodná instituce, který vydává svým zákazníkům certifikáty.
    - Př. Městských 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 politiku přípustného použití aktiv.
    - Hodnotí uskutečnění.
    - Vynucuje bezpečnostní opatření.
- Bezpečnostní manažer
    - Řídí implementaci rozhodnutí bezpečnostní rady.
- Bezpečnostní správce
    - Výkonný orgán.
- Bezpečnostní auditor
    - Hlavní kontrolní orgán.

Monitoring a Audit

- Nepřetržitý proces realizující:
    - Kontrola a dodržování defensivních opatření (využití firemní pošty pro osobní účely).
    - Vyhodnocení záznamu v auditních a logovacích souborech.
    - Log (kdo/kdy přišel) audit (kolikrát co se kdy stalo).
    - Aktualizace dokumentace

Auditní postup

1. Detekce – Zjištění události mající vliv.
2. Rozlišení
    - Určuje prioritu opatření.
    - Zapsání v auditním záznamu, nebo spuštění bezpečnostního poplachu.
3. Zpracování bezpečnostního poplachu – Vysvětlení a opatření k události.
4. Analýza
    - Posouzení události v kontextu předchozích událostí a možných dopadů.
    - Dominový efekt
    - Synergetický efekt (více malých → jeden velký)
5. Agregace
    - Distribuované záznamy → jeden
    - Součet, počet, nejmenší, největší, seskupit.

        - Vyhodnocení dominových a synergetických efektů.
    6. Generování zprávy – Z auditních záznamů vypracování auditní zprávy.
    7. Archivace – Uchování záznamu o události a přijatých opatřeních.

Evaluace

- Pravidelné periodické (minimálně 3 roky) hodnocení bezpečnosti informačního systému.
- Základ pro změnu bezpečnostní politiky (hodnocení rizik).
    - 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).

Auditní postup

1. **Detekce**
    - Zjištění události mající vliv.
2. **Rozlišení**
    - Určuje prioritu opatření.
    - Zapsání v auditním záznamu, nebo spuštění bezpečnostního poplachu.
3. **Zpracování bezpečnostního poplachu**
    - Vysvětlení a opatření k události.
4. **Analýza**
    - Posouzení události v kontextu předchozích událostí a možných dopadů.
    - Dominový efekt
    - Synergetický efekt (více malých → jeden velký)
5. **Agregace**
    - Distribuované záznamy → jeden
    - Součet, počet, nejmenší, největší, seskupit.
    - Vyhodnocení dominových a synergetických efektů.
6. **Generování zprávy**
    - Z auditních záznamů vypracování auditní zprávy.
7. **Archivace**
    - Uchování záznamu o události a přijatých opatřeních.