Principy kybernetické bezpečnosti na úřadu:

Procesy a lidské zdroje

Statutární město Ostrava

- Magistrát
- 23 úřadů městských obvodů
- 160 příspěvkových organizací

- Propojení městskou metropolitní sítí
- Využívání společných aplikací provozovaných v ICT centru
- Outsourcing IT – 100% vlastněná městská akciová společnost Ovanet, a.s.

Systém bezpečnosti:

- Lidé:
  - Každý zaměstnanec
  - Bezpečnostní ředitel
  - Externí bezpečnostní manažer
  - Bezpečnostní fórum
  - Pověřenec
- Procesy (schvalování rolí, hlášení a řešení incidentů, systém vzdělávání)
- Bezpečnostní dokumenty (směrnice, nařízení tajemníka, příručky)
- Infrastruktura (HW, SW)

Lidé a vzdělávání

- Vstupní vzdělávání při nástupu:
  - Příkaz tajemníka k nakládání s prostředky výpočetní techniky, směrnice k zajištění bezpečnostních procesů (povinnosti zaměstnanců, postupy, atd.)
  - Typy útoků, jak je rozpoznat a správná reakce na ně
  - Vysvětlení postupů pro práva a role v SW
  - Vysvětlení principů outsourcingu IT (jak ověřit, že je ajťák z Ovanetu)
  - Jak se chovat k osobním údajům
  - Vysvětlení struktury řízení bezpečnosti (bezpečnostní ředitel, kdo je pověřenec, atd.)
  - Sociální sítě
- Vstupní vzdělávání úředníků
- Průběžné vzdělávání (on-line: institut pro veřejnou správu, dávej kyber od NUKIB, semináře pro vedoucí pracovníky)

Lidé a vzdělávání

- Testování odolnosti (sociotest, podvržený e-mail)
  - Vzdělávání vyhodnocením, zkušeností, zahrnutím do dalšího testovacího vzorku
- Intranet:
  - Bezpečnostní pokyny a dokumentace v samostatné sekci
  - Sekce aktuality: novinky, upozornění, výstrahy
  - Fotografie zaměstnanců a kolegů z Ovanetu
- Call desk
- Fyzická kontrola pracoviště (osobní údaje, technika, apod.)
- On-line prezentace pro ajťáky, vedoucí (kyberčtvrtky Viavis, studio eGovernmentu, apod.)
- Penetrační testování a následná realizace opatření (sledování reakce, kooperativní testování, edukace)
- Pravidelné auditní šetření Interního auditu MMO
- Vše minimálně 1x ročně.

Procesy z pohledu uživatelů IT

- Řízení rolí v IDM
  - Interní uživatelé
  - Externí uživatelé
  - Všechny role, certifikáty, atd.
- Přístup do IS z evidovaných PC, Mobile device managament, příprava multifaktorové autentizace.
- Řízení osobních údajů
  - Adopce nástrojů MS 365 (osobní údaje v cloudových řešeních, kategorizace uživatelů)
  - SW Safetica
- Statut SMO (sjednocení pravidel)
- Ustanovení ve smlouvách s PO pro využívané aplikace (povinnosti PO)

Procesy z pohledu ajťáků

- Sledování varování NUKIB
- Periodické vyhodnocování incidentů Bezpečnosntím fórem a Externím bezpečnostním manažerem
- Plán pro případ „velkého“ bezpečnostního incidentu
  - Posloupnost aktivit
  - Role (kdo co zajišťuje, komu hlásí, tisková mluvčí)
  - Priority pro obnovu
  - Kontakty
  - Je vytištěný

Doporučení:

- Zaveďte pravidelnost a rutinu
- Vytvořte na sebe bič
- Buďte v obraze
- Využijte externí pohled
- Plánujte bezpečnost v rozpočtu