Kybernetická a informační bezpečnost (ale kdyby jenom to)

Ing. Aleš Špidla

Prezident Českého institutu manažerů informační bezpečnosti
ales.spidla@cimib.cz
Specialista pro kybernetickou bezpečnost CENDIS, s.p.
ales.spidla@cendis.cz

Program

- Kybernetická a informační bezpečnost jako součást bezpečnostní kultury firmy
- Proč je kybernetická a informační bezpečnost základní prvkem pudu sebezáchovy firmy
- Jak uchopit hodnotu informací a jak s ní pracovat
- Jak zavést a řídit kybernetickou a informační bezpečnost ve firmě
- Současné trendy

Kybernetická a informační bezpečnost jako součást bezpečnostní kultury firmy

- Co to je bezpečnostní kultura firmy
  - BOZP
  - Požární bezpečnost
  - Fyzická bezpečnost
  - Kybernetická bezpečnost
  - Informační bezpečnost
    - Ochrana know-how
    - Ochrana osobních údajů
    - …
    - …
  - Ochrana značky
  - Ochrana dobrého jména
  - Zajištění legislativní shody
  - A celá řada dalších

Kybernetická a informační bezpečnost jako součást bezpečnostní kultury firmy

- Jednotlivé složky bezpečnostní kultury firmy neexistují odděleně
- Jsou navzájem více či méně úzce propojené
- Jsou na sobě závislé
- Vzájemně se podporují a posilují

Proč je kybernetická a informační bezpečnost základní prvkem pudu sebezáchovy firmy

- Protože je součástí bezpečnostní kultury firmy
- Protože v informatizovaném světě jsou informace a informační služby mnohdy nejcennějšími aktivy (informačními) – ISO/IEC 27001, Zákon o kybernetické bezpečnosti
  - Primární aktiva
  - Podpůrná aktiva
  - Zranitelnosti
  - Hrozby
  - Rizika
- Protože kyberprostor je nebezpečný
- Protože škůdci s nejrůznější motivací a jejich nástroje jsou stále silnější a propracovanější
- Protože zuří kyberkonkurenční boj
  - Kyberšpionáž
  - Přímé ohrožení chodu firmy
- Protože zuří kybernetický terorismus a kybernetické války
- Protože žádný obor není uchráněn

Jak uchopit hodnotu informací a jak s ní pracovat

- Důvěrnost, Dostupnost, Integrita, Nepopíratelnost – to je to oč tu běží
- Nejdůslednější a nejpřesnější vyčíslení hodnoty informačních aktiv nastane po jejich ztrátě, poškození, zničení, krádeži
  - Náklady po výše uvedené zahrnují m.j.
    - Náklady na znovuobnovení
      - Ztráty způsobené výpadkem
      - Náklady na nákup technologií pro obnovu
      - Čas odborníků pracujících na obnově
      - Výkupné
      - Pokuty
      - Náklady na znovuobnovení dobrého jména
      - Atd.
  - Ale to už je pozdě
- Úvaha – analýza (rizik) musí být provedena v okamžiku, kdy zvažuji vznik, využití informačních aktiv
- Jaká rizika (nejen finanční) hrozí mému byznysu v případě porušení bezpečnostní mantry - Důvěrnost, Dostupnost, Integrita, Nepopíratelnost informačních aktiv

Jak uchopit hodnotu informací a jak s ní pracovat

PROTOŽE !!!!!!

Jak zavést a řídit kybernetickou a informační bezpečnost ve firmě

- Vyhodnotit základní kontexty
- Zpracovat katalog informačních aktiv, jejich zranitelností, hrozeb a z toho plynoucích rizik
- Prioritizovat – klasifikovat informační aktiva
- Navrhnout a implementovat odpovídající organizační a technická opatření
  - Zvážit jestli na to máme sílu
- Nikdy se nezastavit
- Neustále vyhodnocovat, napravovat, vzdělávat, trestat
- Vzít si jako vzor ZoKB, VKB
- Nezapomenout na provázanost s GDPR a elektronickou identitou

Současné trendy

- Útoky na všechno co se v kyberprostoru hýbe
- Svět IoT – internet věcí
- Průmysl 4.0
- Využití umělé inteligence (obávám se, že na obou stranách)

ČIMIB

DĚKUJI ZA POZORNOST

Ales.spidla@cimib.cz
Ales.spidla@cendis.cz