YtT Tiina Soininen
Tiedolla johtamisen lehtori

TIEDON JOHTAMINEN (Data management)

Tietoturvallisuus

Aluksi

- Tietoturvassa on tarkoitus suojella informaatioresurssia.
- Eri aloilla on erilaisia määräyksiä
- Sisältää tietoturva menetelmien toteutuksen:
  - prosessit todentamiseen
  - Luvanvaraisuus
  - Tietoon pääsy

Tietoturva koskettaa eri osa-alueita

- Asiakastiedon yksityisyys ja luottamuksellisuus
- Liikesalaisuudet
- Liikekumppanien toiminta
- Yhdistymiset ja yrityskaupat

- Sääntely voi vaikuttaa tietoon pääsyyn
- Varmistaa avoimuutta ja vastuullisuutta
- Ohjaa subjektiivisia käyttömäärittelyjä

- Tietoturvan tulee olla soveltuvalla tavalla
- Tietoturva ei saa olla niin tiukka, että se estää työnteon
- Mahdollisimman pienet toimet, joilla saadaan suurin datan hyödynnettävyys

- Liikesalaisuudet
- Tutkimus ja kehitys
- Asiakastietojen sisällöt
- Liikekumppanuudet ja keskinäiset sopimukset

Karelia

Riskien vähentäminen

- Tunnista ja määrittele sensitiiviset data-varannot
- Määrittele sensitiivisten datojen sijainti koko organisaation osalta
- Määrittele kuinka kutakin data-varantoa täytyy turvata
- Tunnista, kuinka nämä data-varannot on linkitetty liiketoiminnan prosesseihin

Karelia

Tietoturvan tavoitteet ja periaatteet

TAVOITTEET

- Mahdollistaa asianmukainen pääsy tietoihin ja estää asiaton pääsy tietoihin
- Mahdollistaa määräystenmukaisuus ja yksityisyyden suojan, saatavuuden sekä luotettavuuden
- Varmistaa että sidosryhmien yksityisyyden suojan ja luotettavuuden vaatimukset on täytetty

PERIAATTEET

- Yhteistyö
- Liiketoimintalähtöisyys
- Proaktiivinen hallinta
- Selkeät vastuusuhteet
- Metadata lähtöisyys
- Riskin pienentäminen vähentämällä altistumista virheille

Karelia

Uhka ja riski

- Todennäköisyys, että uhka toteutuu ja sen mahdollinen toistuvuuden määrä
- Vahingon tyyppi ja määrä, sisältäen maineen menetyksen
- Vahingon vaikutus liikevaihtoon tai organisaation toiminalle
- Vahingon korjaamisen kustannukset
- Vahingon estämisen kustannukset, sisältäen haavoittuvuuksien korjaukset
- Todennäköisen tietouhkaajan tavoitteet ja tarkoitukset

- Kriittisen riskin data
- Korkean riskin data
- Kohtalaisen riskin data

Karelia

Tietoturvan prosessi

- Tietoihin käsiksi pääsy
- Auditointi
- Todentaminen
- Valtuutus ja oikeuttaminen
- Seuranta

Systeemisiä tietoturvariskejä

- Liiallisten oikeuksien väärinkäyttö
- Legitiimien oikeuksien väärinkäyttö
- Luvaton oikeuksien lisääminen
- Palvelutilien tai jaettujen tilien väärinkäyttö
- Tietohyökkäykset tietovarantoihin
- SQL:n haavoittuvuus
- Oletussalasanat (default passwords)
- Varmuuskopiodatan väärinkäyttö

Karelia

Ulkopuolisia tietoturvariskejä

- Hakkerointi
- Kalastelu
- Haittaohjelmat (lisäohjelmat, vakoiluohjelmat, Troijalaiset, virukset, madot)

Ulkopuolisten tietoturvariskien lähteitä

- Pikaviestimet
- Some sivustot
- Spammi

Ylihuomisen osaamista. Yhdessä.

Karelia ammattikorkeakoulu

LAPIN AMK
Lapland University of Applied Sciences

XAMK PULSE

Jotpa
Jatkuvan oppimisen ja työllisyyden palvelukeskus

Euroopan unionin rahoittama – NextGenerationEU