



**Organizacijos valdymas skaitmeninėje erdvėje:
priklausomybė nuo IT ir kibernetinio saugumo rizikos**



Liudas Ališauskas, Kibernetinio saugumo ekspertas

Temos



Įstaiga skaitmeninėje erdvėje

Kiek įstaigų teikiamos paslaugos ir produktai priklauso nuo technologijų?



IT grėsmių rizikos valdymas

Kodėl turi būti identifikuotos ir valdomos IT ir kibernetinių grėsmių rizikos?



Vidinis pajėgumas ar paslaugos?

Ar, kaip, kokius ir kada priimti sprendimus?

Tikslas: užtikrinti Įstaigos teikiamų paslaugų ir produktų tęstinumą ir atsparumą IT ir kibernetinėms grėsmėms



Šiuolaikinė įstaiga skaitmeninėje erdvėje



Įstaigų priklausomybė nuo IT

Kiek gi mūsų teikiamos paslaugos ir produktai priklauso nuo IT?

- Nebėra „ne IT“ įstaigų
- Galimybės, priklausomybė ir rizika.
- Lankstumas ir prisitaikymas



IT sistemos svarba organizacijos veikloje

Šiuolaikinės technologijos suteikia naujų galimybių, leidžiančių organizacijoms efektyviau vykdyti veiklą, įgyvendinti savo misiją.

- Personalo trūkumas
- Paslaugų efektyvumas
- Viešos paslaugos kokybė



Judėjimas kartu su technologijomis

Organizacijos turi būti lanksčios ir gebėti prisitaikyti prie nuolat kintančių technologinių pokyčių ir sąlygų.

- Kuriantis dirbtinis intelektas
- Debesijos paslaugos
- Inovacijos



IT ir Kibernetinių rizikos valdymas



Kibernetinių atakų poveikis

IT sutrikimai ar kibernetinės atakos gali sukelti asmens duomenų nutekėjimą, praradimą arba trikdyti įstaigos paslaugas.

- Duomenų vagystė ar sunaikinimas
- Įstaigos veiklos paralyžiavimas
- Piliečių nepasitikėjimas viešuoju sektoriumi



IT rizikos valdymo strategijos ir metodai

Tinkamai IT ir kibernetinių rizikų valdymas leidžia išvengti incidentų, užtikrina tinkamą paslaugų tęstinumą ir greitą atkūrimą po incidentų.

- Įstaigos kritinės paslaugos
- Grėsmės ir rizikos
- Tinkamas rizikų valdymas



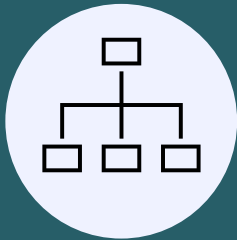
Kibernetinio saugumo gerosios praktikos

Nors visos įstaigos yra unikalios – jų IT ir atsparumo funkcijos puikiai apibrėžtos pasaulinių standartų ir gerųjų praktikų.

- Kibernetinio saugumo įstatymas (OTR)
- IT / Saugos standartai
- Karkasai



Vidinis pajėgumas ar paslaugos?



Vidinių pajėgumų privalumai ir trūkumai

Vidiniai Įstaigos IT pajėgumai leidžia organizacijoms greičiau vykdyti pokyčius, dėl komandos įsitraukimo ir Įstaigos veiklos išmanymo.

- Didesnis komandos įsitraukimas ir kontrolė
- Personalo pritraukimas, auginimas ir išlaikymas
- Naujų technologijų taikymas



IT paslaugų teikėjų naudojimo privalumai ir trūkumai

Platus IT kompetencijų spektras, reikalingas naujų sprendimų kūrimui ir diegimui. Reikalinga stipri sutarties valdymo kompetencija.

- Specializuota patirtis
- Platus sprendimų diegimas
- Mažesnė kontrolė



Kuriuo keliu eiti?

Visais atvejais rekomenduojama atlikti atvejo analizę. Skaičiuojant finansinę dalį kalkuluoti darbo užmokesčio kaštus.

- Poreikiai ir biudžetas
- Trumpalaikiai ir ilgalaikiai tikslai
- Privalumai ir trūkumai



Apibendrinimas

Įstaiga skaitmeninėje erdvėje

Viešojo sektoriaus Įstaiga, kaip ir kitos šiuolaikiškos organizacijos privalo judėti koja kojon su technologijomis.

IT sprendimai privalo būti atsparūs tiek IT tiek kibernetinėms grėsmėms.

IT ir Kibernetinių rizikos valdymas

IT ar kibernetiniai incidentai gali sukelti labai didelės žalos.

Rizikos privalo būti valdomos, kad išvengti incidentų, o nepavykus – gebėti greitai atkurti viešąsias paslaugas.

Rizikos turi būti valdomos Įstaigos rizikų registre.

Kuriuo keliu eiti?

Kelio pasirinkimas privalo būti pragmatiškai apskaičiuotas ir strategiškai suderintas.

Galimas ir realiausias hibridinis variantas.

Perkant paslaugas svarbu turėti sutarties valdymo kompetenciją.

