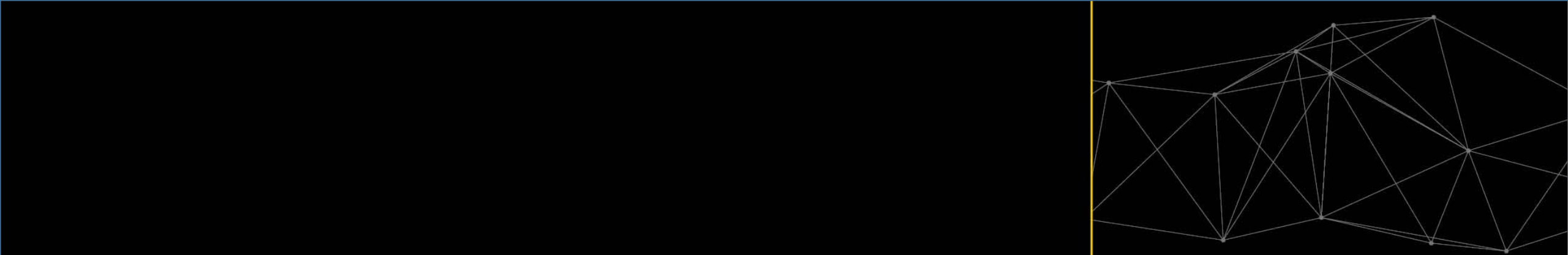
Kibernetinis saugumas ir asmens duomenų apsauga

Jonas Skardinskas
Kibernetinio saugumo valdymo departamento direktorius



Nacionalinis
Kibernetinio
Saugumo
Centras

Ar kibernetinis saugumas garantuoja asmens duomenų saugumą?

Kibernetinis saugumas neabejotinai prisideda prie asmens duomenų saugumo, bet jokiu būdu jo negarantuoja.

Asmens duomenų saugumas yra daug platesnė sąvoka ir apima duomenų valdymą, jų inventorizaciją, gyvenimo ciklo valdymą, duomenų sunaikinimą, personalo mokymą ir kitus dalykus.

Tam, kad kibernetinis saugumas maksimaliai padėtų apsaugoti duomenis jis turi būti integrali įmonės rizikų, tęstinumo valdymo bei asmens duomenų politikos dalis.

Geriausia pradžia – duomenų inventorizavimas

- Duomenų inventorizavimas yra gera pradžią atsakingam duomenų valdymui ir kibernetinio saugumo priemonių pasirinkimui. Juk jei nežinai, kad kažką turi – kaip galėsi tai apsaugoti?
- Vadovams svarbu suprasti skirtumus tarp fizinio ir skaitmeninio turto praradimo.
- Skaitmeninio turto kiekis ir forma dažnai keičiasi žymiai greičiau nei fizinio, todėl reikalingos automatizuotos priemonės palaikyti tinkamą jo apskaitą.
- Inventorizacija padeda nustatyti rizikingiausias skaitmeninio turto rūšis, rasti tinkamas priemones rizikoms valdyti

Skaitmeninis turtas asmeniniame ir tarnybiniame kompiuteryje

Tarnybinė informacija kompiuteryje (klientų, gamybos, prekių judėjimo duomenys, intelektinė nuosavybė, pokalbiai, dokumentai ir pan.);

e-bankininkystės prisijungimo duomenys, piniginės lėšos;

Facebook, Gmail, iCloud, Twitter, Amazon, PayPal ir kt. paskyros, kurių pagalba galima pasiekti įvairią informaciją

Asmens duomenys, kurių pakanka tapatybei pavogti (asmens kodas, dokumentų numeriai, soc. draudimo numeris);

Šantažavimas grasinant informacijos užšifravimu ir/arba paviešinimu;

Kompiuterio resursų išnaudojimas;

Kas organizacijoje atsakingas už kibernetinį saugumą?

- ✓ **Įstaigos vadovas:** užduočių ir resursų skyrimas, atskaitomybės reikalavimas iš pavaldžių asmenų (pagal KSĮ neša administracinę atsakomybę)
- ✓ **IT specialistai:** saugių prieigų valdymas, tinklo segmentavimas, atnaujinimų diegimas, veiklos tęstinumo užtikrinimas
- ✓ **Informacijos bei kibernetinio saugumo specialistai:** rizikos vertinimas, darbuotojų mokymai, pažeidžiamumų paieška, anomalijų sistemose stebėjimas, vadovybės informavimas apie problemas/kibernetinio saugumo rezultatus
- ✓ **Darbuotojai:** informavimas apie kibernetinius incidentus, informacijos bei kibernetinio saugumo reikalavimų laikymasis

Duomenų saugos priemonės

Šifravimas

Prieigos valdymas

Ugniasienės ir įsibrovimo aptikimo/prevencijos sistemos:

Atsarginių kopijų darymas ir tęstinumo planai.

Reguliarūs saugos vertinimai

Darbuotojų švietimas ir sąmoningumas

Teisės aktų ir reguliavimo laikymasis

Reguliarus duomenų stebėjimas ir efektyvi duomenų politika

Kritinis mastymas – sėkmės prielaida

- Svarbių duomenų ir dokumentų kopijos turi būti saugomos atskirai nuo sistemos
- Sudėtingų slaptažodžių naudojimas ir jų periodiškas keitimas nenaudokite tų pačių slaptažodžių skirtingose sistemose
- Visada įvertinti informacijos jautrumą prieš jos siuntimą paštu ar įkėlimą į „ debesį“
- Neteikite perteklinės asmeninės informacijos internete ar socialiniuose tinkluose
- Jei kolega staiga atsiuntė netikėtą prašymą ar prašo veiksmų , kurie gali būti lemtingi pvz .: pervesti pinigų) pasitikslinkite paklausdami jį telefonu
- Atsiminkite , kad išmanieji telefonai maži kompiuteriai, jie paveldi visas kompiuterių kibernetines grėsmes
- Naudotojai visada turėtų būti atsargūs ir truputį paranojiški (bet kuris gautas laiškas , dokumentas ar nuoroda gali būti kenksminga)
- Niekada niekam neduokite savo slaptažodžių administratoriai niekada to jūsų neklaus, nes jie turi aukštesnio lygmens teises

Kelias į priekį

Kokia situacija Jūsų organizacijoje? To galima paklausti saugos įgaliotinio, prašant pateikti Jūsų informacinių išteklių atitikties vertinimo ataskaitą, rizikos vertinimą, kibernetinių/informacijos saugos incidentų suvestinę?

Ką darytumėte jeigu Jūsų sistemos būtų užšifruotos? Reikia įvertinti ar žinote kur yra Jūsų veiklos tęstinumo valdymo planas? Ar žinote kada paskutinį kartą jis buvo išbandytas? Kas atsakingas už Jūsų sistemų atstatymą?

Ar Jūsų organizacijoje yra stebimos anomalijos? Pasiteiraukite, kaip dažnai Jūsų kibernetinio saugumo specialistai analizuoja žurnalinius įrašus (tai turi būti daroma nuolatos), ar juos koreliuoja su informacija kompiuteriuose, mobiliuosiuose telefonuose, ar tai tik informacija iš ugniasienės? Jeigu ne jūs net nežinote kad pas jus vyksta kibernetiniai incidentai.

Ar pasitikite paslaugų teikėjais? Ar organizacijos teikiančios Jums IT paslaugas prisijungia po darbo valandų? Kas atlieka paslaugos teikėjų veiksmų analizę, kad pastarieji nevykdo kenkėjiškos veiklos?