



KIBERNETINĖS SAUGOS

TECHNOLOGIJŲ MATRICA

KATEGORIJOS



KRIPTOGRAFIJA

Kriptografijos raktai, moduliai ir įrankiai naudojami informacijos šifravimui tam, kad informacija atviru (skaitomu) tekstu nebūtų saugoma ar perduodama. Raktai gali būti naudojami e. dokumentų pasirašymui. E. parašo buvimas gali užtikrinti, kad dokumentas yra originalus ir transportuojant ar saugant nėra pakeistas.



BENDROJI SAUGA

Pirminės priemonės, skirtos tinklo, kompiuterių ir bazinių IT paslaugų apsaugai.



RIZIKOS VALDYMAS

IT saugos rizikų mažinimo priemonės.



PRIVATUMAS

Politikų rinkinys ir priemonės, skirtos privačių duomenų saugojimui, perdavimui ir valdymui.



TAPATYBĖS IR PRIEIGOS VALDYMAS

Priemonės, skirtos:
- tapatybės duomenų ir paskyrų saugojimui;
- prieigos teisių suteikimui ir valdymui.



SAUGOS METRIKOS

Priemonės, skirtos saugos produktų veikimo vertinimui ir informacijos bei statistikos apie saugos produktus kaupimui, analizei.



PROCEDŪROS, POLITIKOS, PROCESAI

Taisyklių apie saugos užtikrinimo veiksmus rinkiniai.



SAUGOS PRIEŽIŪRA IR PALAIKYMAS

Kasdienė veikla, užtikrinanti saugų prižiūrimos įrangos veikimą.

NORĖTUMĖTE SUSISIEKTI?



Aivaras Teleiša

„Blue Bridge“ Kompiuterinių tinklų sprendimų vadybininkas

+370 672 28822

aivaras.teleisa@bluebridge.lt

KIBERNETINĖS SAUGOS TECHNOLOGIJŲ MATRICA

Pasiremdama JAV nacionalinio standartų ir technologijų instituto išskirtomis kibernetinės saugos kategorijomis, „Blue Bridge“ sukūrė saugos technologijų matricą. Naudodami šią matricą, pagal savo organizacijos siekiamą saugos brandos lygį galite pasirinkti atitinkamus saugos sprendimus bei technologijas.

aptikimas



apsauga



atkirtis



	BAZINIS SAUGOS LYGIS	PAŽENGĖS SAUGOS LYGIS	SPECIALIZUOTAS SAUGOS LYGIS
Kriptografija / Privatumas	Tinklo srauto šifravimas Viešo-privataus rakto šifravimo infrastruktūra Failo šifravimas Disko šifravimas	E. pašto šifravimas Duomenų bazės šifravimas Rezervinės kopijos šifravimas Saugyklos šifravimas Virtualios mašinos šifravimas	Duomenų saugyklų tinklo (SAN) šifravimas
Bendroji sauga	Tinklo segmentavimas Ugniasienė E. pašto šliuzas Antivirusinė apsauga Aparatinis saugumas	Aplikacijų ugniasienė Serverių antivirusinė apsauga	Naujos kartos antivirusinė apsauga Galinių taškų aptikimas ir atsakas
Tapatybės ir prieigos valdymas	Katalogų tarnyba (AD)	Kelių faktorių autentikavimas Slaptažodžių saugykla Privilegijuotų paskyrų valdymas Tinklo prieigos kontrolė Tapatybės valdymas	Grėsmių analitika
Rizikos valdymas	Pažeidžiamumų valdymas IT infrastruktūros stebėjimas IT auditas	Duomenų nutekimo prevencija Darbuotojų apmokymas	Įrodymų analizė Smėliadėžė Saugos įvykių stebėjimas Apsauga nuo DDoS atakų Grėsmių įžvalgos
Saugos metrikos	Analitika	Analitika	Analitika
Saugos priežiūra ir palaikymas	Naujinimų valdymas Rezervinių kopijų kūrimas Inventoriaus valdymas	Konfigūracijos valdymas	Saugos automatizavimas Dirbtinio intelekto panaudojimas apsaugai
Procedūros, politikos ir procesai	Saugos procedūros	Saugos politikos	Saugos strategija Zero Trust architektūra

ORGANIZACIJOS IT SAUGOS BRANDOS LYGIAI

BAZINIS LYGIS

Šiame lygyje turimos priemonės leidžia apsisaugoti nuo bazinių grėsmių.

PAŽENGĖS LYGIS

Šiame lygyje turimos priemonės apsaugo nuo didelės dalies saugos grėsmių arba apima sritis, kurios neturėjo saugos priemonių baziniame lygyje.

SPECIALIZUOTAS LYGIS

Šiame lygyje turimos priemonės apsaugo nuo specializuotų grėsmių, gali aptikti visai naujas, anksčiau nežinomas grėsmes, taip pat kvalifikuotai atrasti ir analizuoti saugos incidentus, pagelbėti surasti ir panaudoti atsaką tam tikroms grėsmėms. Šios priemonės dažnai reikalingos ir tam, kad organizacija atitiktų tam tikras (teisines, karines ir kt.) reguliacijas.