OIXIO rekomendacijos kaip padidinti atsparumą kibernetinėms grėsmėms

Pavadinimas	Aprašymas	Konkretūs rekomenduojami veiksmai
Techniniai		
Prieigų apribojimas	Užtikrinama, kad tik tam tikriems asmenims būtų suteikiamas prieigos leidimas prie jūsų IT infrastruktūros (neatsižvelgiant į tai ar vartotojas vidinis ar išorinis). Tai apima vartotojų paskyrų valdymą, prieigos kontrolę, duomenų šifravimą ir kitas priemones.	a. Audituokite dabartines prieigas. b. Iš naujo įvertinkite prieigų lygius ir modifikuokite pagal poreikį. c. Kur įmanoma, suteikite prieigą su ribotu laikotarpiu, t. y. kad prieiga būtų nutraukta automatiškai pasibaigus atitinkamam laikotarpiui.
Atsarginių kopijų funkcija, darymas ir lokacija	Atsarginės kopijos yra svarbios, nes jos padeda išsaugoti duomenis net ir po sistemos sutrikimų arba atakų. Atsarginės kopijos turėtų būti daromos reguliariai ir saugomos atskirame saugyklų įrenginyje, kuris yra fiziškai nutolęs nuo pagrindinės infrastruktūros. Jos taip pat turi būti reguliariai testuojamos, jog galėtumėte būti ramūs, kad nelaimei nutikus jos veiks tinkamai ir duomenys bus atkurti be trikdžių.	a. Susikurkite aiškų planą (dažnumas, lokacijų kiekis) priklausomai nuo duomenų kritiškumo ir vertės jūsų verslui b. Nuolat testuokite atsargines kopijas, t. y. būkite tikri, kad kilus poreikiui galėsite atkurti reikiamus duomenis.
Programinės įrangos versijos ir jų naujinimas	Reikia periodiškai tikrinti ir atnaujinti programinę įrangą, kad būtų užtikrintas saugumas ir funkcionalumas. Tai apima saugumo pažeidimų pašalinimą, naujų funkcijų diegimą ir t. t.	a. Pasitelkite centralizuotus Remote Monitoring & Management įrankius. Su tokiu įrankiu galėsite lengvai stebėti ir valdyti programinės įrangos versijas bei jų naujinimus.
Operacinės sistemos versijos ir jų naujinimas	Panašiai kaip su programine įranga, reikia periodiškai tikrinti ir atnaujinti operacinę sistemą, kad būtų užtikrintas saugumas ir funkcionalumas. Tai apima operacinės sistemos atnaujinimą, atnaujinimų diegimą ir t. t.	a. Pasitelkite centralizuotus įrankius tokius kaip WSUS arba Azure patch management ar kt.
IT Valdymas ir stebėsena:		
Antivirusinės ir kt. prevencinės priemonės	Antivirusinės programos, ugniasienės ir kitos prevencinės priemonės yra būtinos užkirsti kelią virusų, kenkėjiškų programų ir kitoms grėsmėms atakuojant jūsų IT infrastruktūrą.	a. Pasirūpinkite antivirusinės apsaugos priemonėmis, kurios turėtų centralizuotą stebėsenos funkcijas, EDR (Endpoint detection and response) funkcionalumą ir kt. b. Valdykite prieigą prie jūsų vidinės infrastruktūros pasitelkiant ugniasienę, t. y. leiskite tik autorizuotiems asmenims turėti prieigą prie jūsų vidinių resursų. c. Reguliariai rūpinkitės antivirusinės programos bei ugniasienės atnaujinimais.
IT infrastruktūros stebėsena ir analizė	Visi sistemos įrašai turėtų būti saugomi ir tikrinami siekiant nustatyti galimus saugumo pažeidimus ar kitus nukrypimus. Šios analizės tikslas yra užtikrinti, kad sistemoje nėra jokių neįprastų veiksmų ar potencialių saugumo grėsmių.	a. Pasitelkite SIEM (Security information and event management) įrankius į pagalbą surenkant ir analizuojant IT infrastruktūros sistemų įrašus. b. Apsvarstykite SOC (Security Operations Center) teikiamas paslaugas. c. Pasirūpinkite, kad sistemų įrašai būtų saugomi atsižvelgiant į veiklos specifiką, tai gali būti nuo 1 mėn. iki 1 metų.

Pavadinimas	Aprašymas	Konkretūs rekomenduojami veiksmai
Administracines privilegijas turinčių paskyrų valdymas	Administracinės paskyros suteikia pilną teisę prieiti prie jūsų IT infrastruktūros ir ją valdyti. Reikia užtikrinti, kad administracinės paskyros būtų naudojamos tik reikiamuose atvejuose, kad jų turėtojai žinotų savo atsakomybę ir kad privilegijos būtų suteikiamos tik reikiamu lygiu.	a. Kasdien naudojamos vartotojų ir administracines teises turinčios paskyros turėtų būti atskirtos. b. Suteikite prieigos lygius tik reikiamu lygiu ir atitinkamam laikotarpiui. c. Reguliariai iš naujo įvertinkite ir keiskite prieigos lygius.
Vartotojų budrumo ugdymas		
Periodiniai neplanuoti budrumo „patikrinimai“	Mes nuolat siunčiame įtartinus pranešimus ir žiūrime kaip vartotojai reaguoja, atliekame vis sudėtingesnes el. pašto atakų simuliacijas, kad budrumo lygis nuolat kiltų. Tikriname vartotojų budrumą, atitinkamai, modifikuojame mokymų strategiją bei pateikiame ateities rekomendacijas vartotojams.	a. Pasitelkite Microsoft 365 įrankius reguliariai imituoti „phishing“ atakas ir dalinkitės gautais rezultatais bei tobulinkite mokymų strategiją. b. Nuolat dalinkitės naudinga informacija, patarimais vartotojams apie saugumą ir didinkite jų budrumą.
Naujausios versijos turėjimas		
Migravimas į naujas versijas	Naujos versijos dažnai turi paskutinius saugumo patobulinimus ir pašalina ankstesnių versijų pažeidžiamumus. Permigravus į naujas versijas užtikrinama, kad jūsų sistema būtų atnaujinta ir geriau apsaugota nuo kibernetinių grėsmių. Tai ypatingai svarbu atsižvelgiant į nuolat besikeičiančias ir vis sudėtingesnes kibernetines atakas.	a. Identifikuokite senas sistemų versijas. b. Įsivertinkite ar yra galimybių jas migruoti į naujesnes versijas. c. Apsivarstykite migravimo į naujausią versiją variantus. d. Neturint galimybės permigruoti senos sistemos į naują versiją, pasirūpinkite papildomais įrankiais saugumui užtikrinti. e. Pradėkite formuoti sistemų gyvavimo žemėlapius ir ruoštis sistemų versijų kėlimui tinkamu laiku.

Kibernetinis saugumas yra kritiškai svarbus organizacijų sėkmei ir tvarumui. Jis turi būti nuolat tobulinamas, kad organizacija būtų atspari naujoms kibernetinėms grėsmėms.
Jei Jums reikalinga pagalba šiais klausimais, prašome nedvejoti ir susisiekti su mumis.