



CYBERS

„Microsoft 365“ saugumo monitoringas

Bendradarbiaudami su CYBERS galime pateikti savo klientams geriausius saugumo sprendimus.

Kai vartotojai naudojami debesų paslaugomis, labai svarbu, kad būtų taikomos visos priemonės saugumui užtikrinti. Priešingu atveju, tai kelia rimtą grėsmę organizacijoms. Pavyzdžiui, gali kilti pavojus dėl galimybės perimti el. pašto adresą, pavogti asmeninę informaciją ir komercines paslaptis ar net perimti visos organizacijos infrastruktūros ir verslo kontrolę.

Šiuos tikslus galima pasiekti teikiant šias paslaugas:

„M365“ saugumo stebėjimas

Pirmiausia renkame informaciją ir analizuojame debesies nustatymus.



Trumpa esamos padėties apžvalga:

- ✓ Įvertinama, kiek organizacija yra pažeidžiama per galimą debesies ataką
- ✓ Daugiausia dėmesio skiriama kritiniams trūkumams
- ✓ TOP5 saugos problemos ir jų sprendimo būdai
- ✓ Geresnis konfigūravimas pakeitimų, kuriuos galima įdiegti dabartinėje aplinkoje be papildomų išlaidų

„Exchange Online“ stiprinimas

„Exchange Online“ yra populiariaus „Microsoft Exchange“ serverio „Microsoft Cloud“ versija, teikianti el. pašto, kalendoriaus ir kontaktų valdymo paslaugas milijonams verslo vartotojų viešajame debesyje.



Mes patikrinsime šiuos aspektus:

- ✓ „Exchange Online“ prisijungimo politiką
- ✓ Prieigą prie el. pašto per interneto naršyklę
- ✓ „Exchange“ apsaugos politiką
- ✓ Sukčiavimo ir apgavysčių el. paštu prevenciją ir ataskaitų teikimą
- ✓ Priėjimą prie organizacijos duomenų per mobiliuosius įrenginius
- ✓ Bendruosius saugos parametrus, kurie turi įtakos „Exchange Online“ saugumui

„Microsoft 365“ saugumo monitoringas

Norint išvengti galimos žalos, reikia nuolat stebėti debesies aplinką.



Stebėjimo paslauga apima šias funkcijas:

- ✓ Svarbiausių „Microsoft 365“ saugos patobulinimų konfigūravimas
- ✓ Būtinų „Microsoft 365“ žurnalų gavimas ir koreliacija
- ✓ Automatinis pranešimas klientui apie incidentą el. paštu
- ✓ Platformos valdymo stebėsena ir profilaktinės patikros
- ✓ Žurnalo šaltiniai, jungčių valdymas ir stebėjimas
- ✓ Įspėjimų politikos tikrinimas ir atnaujinimas
- ✓ Papildomi konkretaus kliento saugumo naudojimo atvejai
- ✓ Pradinė perspėjimo signalų analizė ir klaidingų teigiamų duomenų pašalinimas
- ✓ Reagavimo į incidentus paslauga ir bendravimas su klientu
- ✓ Mėnesinės ataskaitos ir incidentų analizės