primend

„Microsoft 365“ debesų saugumo mokymai IT administratoriams

Mokymų trukmė: 2-3 val.
Mokymų kaina: 2000 €

Mokymuose įtraukta klausimų ir atsakymų dalis.
Mokymų programa yra rekomenduojama ir gali būti pritaikyta pagal įmonės poreikius.
Mokymai vyksta anglų kalba.

„Microsoft 365“ debesų aplinkos saugumas apima praktikas, įrankius ir technologijų rinkinį, skirtą „Microsoft 365“ aplinkai ir joje esantiems duomenims, programoms ir tapatybėms apsaugoti. „Microsoft 365“ yra debesies pagrindu sukurtas paslaugų rinkinys, apimantis tokias paslaugas kaip **„Exchange Online“, „SharePoint Online“, „OneDrive for Business“, „Teams“ ir kt.**

Šios aplinkos apsauga yra labai svarbi norint apsaugoti jautrius organizacijos duomenis ir užtikrinti, kad būtų laikomasi reguliavimo standartų. Pagrindinis „Microsoft 365“ debesies aplinkos saugos tikslas yra užtikrinti, kad organizacijos duomenys, tapatybės ir ištekliai „Microsoft 365“ būtų apsaugoti nuo neteisėtos prieigos, duomenų pažeidimų ir kitų saugumo grėsmių.

„Microsoft 365“ debesies aplinkos saugos mokymų IT administratoriams tikslas – suteikti jiems žinių ir įgūdžių, reikalingų norint veiksmingai apsaugoti ir valdyti „Microsoft 365“ aplinką.

primend

- ✔ Dabartinės „Microsoft 365“ nuomotojo ir licencijų būklės įvertinimas kartu su rezultatais pagrįstomis rekomendacijomis.
- ✔ „Microsoft 365“ aplinkos saugos auditas ir „Microsoft Intune“ konfigūracijų peržiūra.
- ✔ Galinių taškų apsauga (Endpoint protection) – kaip efektyviai apsaugoti organizacinius įrenginius, naudojamus duomenų apdorojimui.
- ✔ Kompiuterio valdymas („Windows 11“ ir „Mac“), įskaitant kelių veiksnių autentifikavimą (MFA) ir sąlyginės prieigos strategijas (Conditional Access).
- ✔ Mobiliųjų įrenginių valdymas: programų apsaugos politika (MAM) ir įrenginių valdymas (MDM) – kada naudoti vieną, o kada – abi kartu?
- ✔ Sąlyginės prieigos politika – padidina vartotojų, įrenginių ir duomenų prieigos saugumą.
- ✔ „Microsoft Defender for Office 365“ – saugos sprendimas, skirtas apsaugoti organizacijos el. paštą ir bendradarbiavimo įrankius (pvz., „Microsoft Teams“) nuo kibernetinių grėsmių.
- ✔ El. pašto saugos nustatymai – SPF, DKIM ir DMARC kaip trys pagrindiniai el. pašto autentifikavimo metodai, padedantys apsaugoti domeną ir el. pašto sistemą nuo šlamšto, sukčiavimo ir kitų kibernetinių grėsmių.
- ✔ Tapatybės teikėjas „Microsoft Entra ID“ – debesies pagrindu sukurta tapatybės ir prieigos valdymo paslauga, padedanti organizacijoms saugiai valdyti ir apsaugoti vartotojų tapatybes bei prieigą prie įvairių programų ir išteklių.
- ✔ Duomenų apsauga naudojant „Microsoft Purview“ sprendimus (jautrumo žymėjimas, saugojimo politika, duomenų praradimo prevencija).
- ✔ Registravimas ir stebėjimas debesijos paslaugose.
- ✔ Svečio paskyros prieiga/dalijimasis duomenimis ir bendradarbiavimas su išoriniais partneriais.
- ✔ Saugaus AI naudojimo rekomendacijos.
- ✔ Nuolatiniai klausimai dėl „Microsoft“ debesijos paslaugų.

Susisiekite su mumis:

Tadas Jankauskas | Pardavimo vadovas | tadas.jankauskas@primend.com

bm certification
ISO 9001
ISO 27001
System certification