primend

Microsoft 365 Premium

Prasmīgs meistars var atvērt jebkuras durvis un logus. Svarīgākais uzdevums Tava uzņēmuma drošībai ir padarīt šādu iespēju pēc iespējas sarežģītāku.

2021. gadā Baltijas valstīs reģistrēti aptuveni 500 000 kiberuzbrukumi, no kuriem 9 000 atstāja kaitniecisku ietekmi. Visnejaukākie uzbrukumi ir kriptovīrusi.

Kibernoziegumi kļūst arvien izsmalcinātāki, un ar vienkāršu pretvīrusu aizsardzību vairs nepietiek, lai būtu drošībā!

Kāpēc izvēlēties M365 Premium?

- **Endpoint Manager**

  Mākoņrisinājums, kas ļauj īstenot centralizētu drošības politiku, nodrošinot vienotu aizsardzību visām ierīcēm, no kurām ir piekļuve uzņēmuma datiem.

  Centralizēta drošības politika visiem datoriem un lietotājiem.

  - **Šifrēti cietie diski (Bitlocker),** kas ir ļoti svarīgi datora zādzības gadījumā. Ja Bitlocker nav ieslēgts, piekļūt datiem cietajā diskā ir iespējams ārkārtīgi viegli.

  - **Daudzpakāpju autentifikācija (MFA),** ir vienkāršākais un ātrākais veids, kā uzņēmumā ieviest stingrāku drošību. Ir svarīgi pārliecināties, ka visi lietotāju konti ir aprīkoti ar MFA un process ir lietotājam draudzīgs.

    Viens no izplatītākajiem kiberdraudiem šobrīd ir pikšķerēšana, zogot lietotāju paroles. Izmantojot MFA, hakeriem paroles ir bezvērtīga informācija, ja vien viņiem nav piekļuves lietotāja mobilajam tālrunim.

- **OneDrive.** Visizplatītākais veids, kā iestatīt OneDrive, ir sasinhronizēt My Documents un darbvirsmu (Desktop) ar MS Cloud. Tas palīdz viegli un ērti pārslēgties uz jaunu datoru, kā arī viegli atgūt datus gadījumā, ja ar datoru kaut kas atgadās.

- ## Defender for Endpoint Business

  Spēcīga pretvīrusu aizsardzība, kas aptur pat tos vīrusus, ar kuriem bezmaksas programmas netiek galā. Ar Premium komplektu ir garantija, ka aizsargāti tiek pilnīgi visi datori. Turklāt, komplektā iekļauts arī reāllaika novērtējums un automatizēti brīdinājumi, ja datora drošībai ir nepieciešami uzlabojumi.

- ## Defender for Office 365

  Pretvīrusu aizsardzība e-pastiem un dokumentiem (OneDrive; SharePoint). E-pasti ir izplatīts vīrusu avots. Izmantojot Defender, tiek nodrošināts, ka neviens no inficētajiem e-pasta ziņojumiem nenonāk iesūtnē.

- ## Limitēta piekļuve un ģeobloķēšana (Geoblock)

  Par uzņēmuma IT drošības politiku atbildīgajam darbiniekam, gluži kā vārtsargam, ir iespēja noteikt, kurš, kā un no kurienes drīkst piekļūt Tava uzņēmuma datiem. Piemēram, pārliecināties, ka neviens nevar lejupielādēt uzņēmuma datus ierīcē, kas nav uzņēmuma pārvaldībā. Izmantojot Geoblock rīku, ir iespējams arī bloķēt piekļuvi savai Office 365 videi no nevēlamām valstīm.

- ## Mobilo datu pārvaldība

  Svarīgi, ka dati ir aizsargāti arī mobilajās ierīcēs (iPhone un Android), lai tiem nevar piekļūt no nevēlamām lietojumprogrammām.

Prasmīgs meistars var atvērt jebkuras durvis un logus. Svarīgākais uzdevums Tava uzņēmuma drošībai ir padarīt šādu iespēju pēc iespējas sarežģītāku.

Nodrošini maksimālu aizsardzību sava uzņēmuma datiem un ierīcēm!

Mārtiņš Jurjāns Primend Latvia vadītājs | martins.jurjans@primend.com

primend

Microsoft Country Partner of the Year
2023
7 Times Winner
2015 / 2016 / 2017 / 2018 / 2020 / 2021