COLONNADE
A FAIRFAX COMPANY

Home Office tippek

Biztonságos IT rendszerek – otthon is

A koronavírus miatt kialakult vészhelyzet rendkívül gyors reagálást igényelt a vállalatoktól. Sok esetben teljes cégek költöztek át irodaházakból a nappalikba, és akár egyik napról a másikra váltak könnyebben hozzáférhetővé a korábban szigorú szabályok mellett kialakított rendszerek, adatbázisok, így sebezhetőségük is sokkal nagyobb figyelmet érdemel.

Mit tehetünk a biztonságos működésért?

1. Alakítsunk ki felhasználóbarát környezetet a távoli kapcsolódásra! Gondoskodjunk a felhasználók **oktatásáról**, és biztosítsunk lehetőséget a biztonsági **incidensek bejelentésére** is!
2. Gondoskodjunk a **végfelhasználói eszközök** (laptop, tablet, stb.) maximális biztonságáról!
(Pl.: víruskereső telepítése, operációs rendszer frissítése, stb.)
3. Lássuk el **kódvédelemmel** az eszközök adathordozóit!
(Pl.: data encryption)
4. Tegyük biztonságossá minden **adatkapcsolatunkat**, ha az irodai, központi eszközökhöz csatlakozunk! (Pl.: SSL VPN, IPSec VPN)
5. A cég kulcsalkalmazásait biztosítsuk **többtényezős hitelesítéssel**!
6. Állítsuk be az **internetes tartalomszűrést**, és tartsuk távol a nem kívánt online tartalmakat!
7. Tartsuk kontroll alatt az **USB-meghajtók**, és egyéb USB eszközök használatát!
(Pl.: csak titkosított eszközök használatát engedélyezzük)
8. Intézkedjünk a **mobileszközök** biztonságos használatáról!
(Pl.: PIN-kód, ujjlenyomat azonosítás, vagy egyéb azonosítás igénylése)
9. Biztosítsuk a Home Office **IT támogatásához** szükséges eszközöket, alkalmazásokat!
10. Bizonyosodjunk meg arról, hogy a céges VPN megoldás **ki tudja-e szolgálni** egyidőben a sok otthonról bejelentkező felhasználót, és bírja-e a megnövekedett terhelést.
11. Győződjünk meg arról, hogy munkatársaink jogosultak-e a céges eszközeink használatára! Ha nem, akkor biztosítsuk, hogy a **privát eszközök biztonsága** egyenértékű legyen a cégessel.