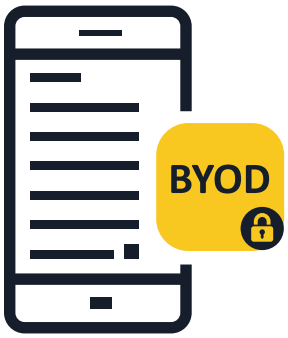
MOBILTELEFONOKON FUTÓ KÁRTEVŐ PROGRAMOK

TIPPEK ÉS TANÁCSOK VÁLLALKOZÁSOKNAK

1 Tájékoztassa a munkatársakat a mobileszközök használatával járó kockázatokról

- A mobileszközöknek köszönhetően mára már igen gyakran összemosódik a különféle eszközök és hálózatok magáncélú és céges felhasználása. A mobileszközökön keresztül a céges hálózatok ellen intézett támadás jelentős kockázattal jár a vállalkozásokra nézve. A mobileszközök is számítógépek, és ennek megfelelő védelmet igényelnek.



2 Vezessen be a cégnél a saját eszközök használatát szabályozó irányelveket (BYOD)

- A céges adatokhoz és rendszerekhez saját eszközeikkel hozzáférő felhasználóknak a céges irányelvek szerint kell eljárniuk, még akkor is, ha az eszközöket csak levelezésre, naptárkezelésre vagy partnerek adatainak kezelésére használják. Körültekintően válassza ki, hogy a mobileszközök kezeléséhez és védelméhez melyik technológiákat alkalmazzák, és hívja fel a munkatársak figyelmét, hogy legyenek mindig óvatosak.

3 A mobileszközökre vonatkozó biztonsági irányelvek legyenek az átfogó biztonsági keretrendszer részei

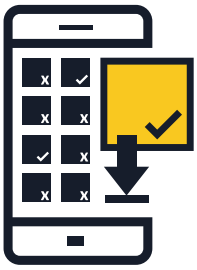
- Amennyiben egy eszköz nem felel meg a biztonsági előírásoknak, azt nem szabad a céges hálózathoz csatlakoztatni, ahogyan a céges adatokhoz sem lehet vele hozzáférni. A vállalatoknak érdemes saját mobileszköz-kezelési (MDM) vagy mobilitáskezelési (EMM) megoldásokat bevezetniük.
- Mindezen intézkedések mellett rendkívül fontos egy mobilfenyegetettség ellen védő rendszer telepítése is. Ezzel a megoldással javul a rendszerek átláthatósága, továbbá könnyebben észlelhetővé válnak a különféle alkalmazás-, hálózat- és operációsrendszer-szintű fenyegetések.

4 Legyen óvatos, ha nyilvános Wi-Fi hálózaton keresztül kíván céges adatokhoz hozzáférni

- Általánosságban elmondható, hogy a nyilvános Wi-Fi hálózatok nem biztonságosak. Ha a cég egyik dolgozója például repülőtér vagy kávézó ingyenes Wi-Fi hálózatán keresztül fér hozzá a céges adatokhoz, azokhoz rosszindulatú felhasználók is hozzáférhetnek. A cégeknek javasolt a „hatékony használatra” vonatkozó irányelvek alkalmazása.

5 Az eszközök operációs rendszere és alkalmazásai legyenek mindig naprakészek

- Javasolja a cég dolgozóinak, hogy telepítsék a mobileszköz operációs rendszerének frissítéseit, amint az eszköz erre vonatkozó üzenetet küld. Különösen az Android rendszerre igaz, hogy érdemes gyakran rákeresni a mobilszolgáltatók és készülékgyártók frissítéseire. A legújabb frissítések telepítésével nemcsak biztonságosabb lesz a készülék, hanem jobban is működik majd.



6 Csak megbízható forrásokból származó alkalmazásokat telepítsen

- A vállalati hálózathoz csatlakozó eszközökre a cég irányelvével összhangban kizárólag hivatalos forrásból származó programok telepíthetők. Hasznos megoldás lehet egy céges alkalmazásbolt kialakítása, ahonnan a felhasználók igény szerint letölthetik az engedélyekkel rendelkező, szükséges alkalmazásokat. A telepítéssel és beállítással kapcsolatban kérje egy biztonsági cég segítségét, vagy hozza létre maga a boltot.

7 Akadályozza meg a szoftvermódosításokat (jailbreak)

- Az operációs rendszerek gyártói különféle biztonsági korlátozásokat alkalmaznak, amelyeket eltávolítva teljes hozzáférést lehet szerezni az operációs rendszerhez, illetve annak funkcióihoz (jailbreak). A készülék biztonsági korlátozásainak eltávolítása (jailbreak) jelentős mértékben csökkentheti a rendszer biztonsági szintjét, mert olyan biztonsági réseket tesz elérhetővé, amelyekről a felhasználó nem is tudhat. Céges környezetben nem szabad olyan eszközt használni, amelyben engedélyezettek a gyökérműveletek.

8 Fontolja meg a felhőbeli tárolás lehetőségét

- A mobileszközök felhasználóival gyakran előfordul, hogy a fontos dokumentumokhoz nemcsak az asztali gépen, hanem az irodán kívül saját telefonjukon vagy táblagépükön keresztül is szeretnének hozzáférni. Céges szinten érdemes megfontolni a felhőalapú tárolási és fájlszinkronizálási megoldások bevezetését, hogy az ilyen és ehhez hasonló igényeket biztonságos módon lehessen teljesíteni.

9 Kérje meg munkatársait, hogy telepítsenek a mobileszközre biztonsági alkalmazást

- A fertőzés kockázata alól egyik operációs rendszer sem jelent kivételt. Amennyiben lehetséges, a felhasználók mindenképpen használjanak a mobilkészüléken valamilyen biztonsági programot, amely észleli a különféle kémprogramokat és rosszindulatú alkalmazásokat és megakadályozza a településüket, valamint több más, kalózkodás-ellenes és lopásgátló funkcióval rendelkezik.

EUROPOL EC3 European Cybercrime Centre

#MobileMalware