Bring Your Own Device

T · · Systems · · ·

Ahogy az okostelefonok és táblagépek használata egyre elterjedtebb, természetes igény, hogy ezeket az eszközöket munkavégzésükhöz is mind többen kívánják használni. A saját eszközök használata hatékonyabbá és kényelmesebbé teszi a munkát.

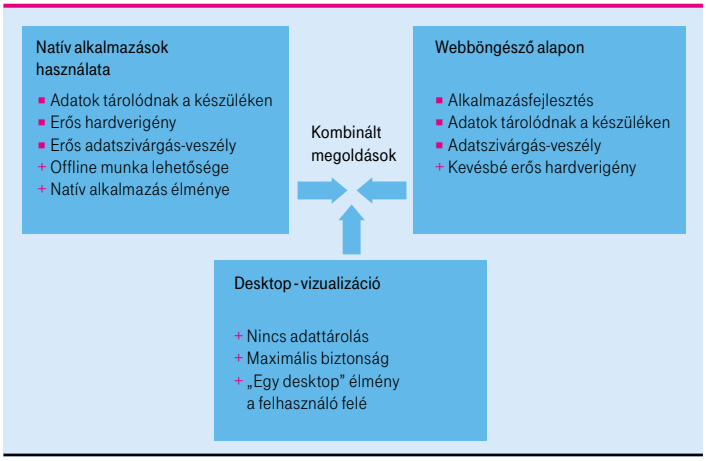
A világon mindenhol okos eszközök milliót használják a dolgozók, hogy segítségükkel megkönnyítsék saját mindennapjaikat. Ezek a hasznos készülékek az alkalmazásaik és könnyű használatuk miatt a magánélet mellett a munkahelyi környezetben is jelentős támogatást tudnak nyújtani, olyannyira, hogy akár képesek helyettesíteni a vállalat által biztosított IT-eszközöket is. **Ez a trend a BYOD (Bring Your Own Device), melynek során a munkavállaló szabadon választhat eszközt a munkájához**, és ez az okos eszköz lehet akár a privát célokra használt darab is. Sokan az IT-eszköz tulajdonosának megváltozását tekintik a trend alappillérének, azonban a jól átgondolt koncepcióban az eszköz tulajdonlása másodlagos. A megoldás akkor lesz sikeres, ha támogatja a munkáltató által biztosított eszközök és a munkavállaló saját eszközeinek használhatóságát is. Egy másik fontos alapkövetelménye egy jó BYOD-megoldásnak, hogy ne csak az okostelefonokra és tabletekre terjedjen ki: a trend magában foglalja a saját tulajdonú PC-k munkahelyi célokra való használatát is.

Az IT-architektúra feladata azt a környezetet biztosítani, amelyben bármilyen eszköz tulajdonostól függetlenül képes a szükséges erőforrások elérésére, természetesen a megfelelő biztonság fenntartásával. Az IT-osztály számára egy BYOD-megoldás bevezetése első ránézésre hatalmas kihívás, hiszen az eddigi eszközparkhoz képest sokszorosára kell növelni a támogatott típusok számát, mindezt úgy, hogy ugyanakkor kevesebb kontrollja van számos eszköz felett.

A főbb stratégiai irányok:

- vállalati alkalmazások futtatása az eszközön,
- webalapú hozzáférés az adatokhoz,
- az okos eszköz megjelenítő legyen.

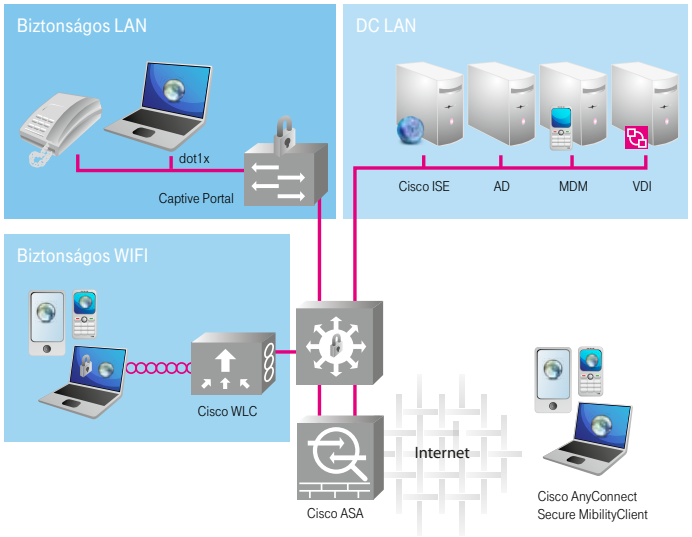
1. ábra BYOD-stratégiák



A biztonsági szint megtartása érdekében meg kell határozni bizonyos követelményeket a hálózatra helyben vagy akár távolról csatlakozó saját eszközökkel szemben is. Ezek lehetnek biztonsági szoftverek telepítésére vagy frissítésére vonatkozó előírások. Az üzleti szervezetek kevesebb mint fele (a nagyvállalatok 47%-a, a kkv-k 38%-a) rendelkezik a vállalati adatok mobil eszközzel történő továbbításáról szóló szabályzattal.

Ezek mellett fontos, hogy a hálózatra csatlakozó minden eszköz felhasználóhoz legyen köthető. **Ezt a csatlakozás során elvégzett hitelesítéssel lehet legjobban biztosítani.** Mivel napjainkban már számos módon lehet csatlakozni a vállalati hálózathoz, olyan BYOD-megoldást kell kidolgozni, amely minden hozzáférési pontot képes megfelelő módon kezelni.

2. ábra BYOD-építőelemek



A szükséges háttér:

- WiFi: modern Cisco kontroller alapú megoldás a funkcióknak megfelelő WiFi-hálózatok megjelenítésére.
- Cisco ISE (Identity Services Engine): az ISE-rendszer képes a központi hitelesítő szerver szerepét ellátni. Emellett biztosítja a magas színvonalú vendégkezelést és a csatlakozó eszközök számára előírt biztonsági szabályrendszer ellenőrzését is.
- Menedzselt LAN: intelligens Cisco switchek, melyek képesek a vezetékes hálózatra csatlakozó eszközök megfelelő kezelésére, hitelesítésére, karantén kezelésére.
- MDM: Mobile Device Management rendszer segítségével garantálható, hogy az eszközök megfelelő biztonsági beállításokkal rendelkeznek az érzékeny adatok tárolásához.
- VDI segítségével elérhető, hogy a saját eszköz a szervezet védendő adatainak csupán a megjelenítésére szolgáljon. Emellett a felhasználó a saját eszközén is a megszokott vállalati platformon dolgozhat, de a saját eszköz nyújtotta mobilitással.
- VPN-hozzáférés biztosítja, hogy a munkavállaló a szolgáltatásokat ne csak a telephelyen érje el, hanem bárhonnan, bármikor, de a megfelelő biztonsággal.
- Megfelelő szabályzás és oktatás.

A felsorolt elemek részben vagy akár teljes egészében manapság már jelen vannak a vállalatoknál. Így a meglévő rendszereket kiegészítve könnyen elérhető egy megfelelő infrastruktúra.

A megoldás releváns lehet, ha:

- a munkavállalók saját eszközöket is használnak,
- a cég hálózatvédelmi NAC-megoldások bevezetését tervezi,
- fontos a vendégek számára biztosított minőségi hozzáférés,
- fontos a mobil eszközök VPN-elérése a központ felé,
- zöldmezős WiFi-kiépítés esetében,
- VDI-környezetet használnak okos eszközökről,
- érzékeny adatok jelenhetnek meg a saját eszközön.

Tekintse meg Bring Your Own Device megoldásunkat Future Zone innovációs központunkban (Budapest XI., Budafoki út 56.)!

Amennyiben felkeltettük érdeklődését, kérjük, keresse szakértő kollégánkat, vagy látogasson el a www.t-systems.hu weboldalunkra.

Batta Norbert
Mobil: +36 30 644 7567
E-mail: : batta.norbert@t-systems.hu

Détári Gábor
Mobil: +36 30 631 5791
E-mail: detari.gabor@t-systems.hu