

A Felhő túloldala: Biztonság

Manapság már a legtöbb cégvezető vagy tulajdonos szívesen áldoz az üzleti biztonságra – nem úgy, mint 10-20 évvel ezelőtt. Tapasztalataink és a gazdasági statisztikák szerint évről évre növekszik a Cloud Computing, azaz a Felhő infrastruktúrát használók tábora, és már tudjuk: **jó okból.**

Emlékszik a közelmúlt óriási IT botrányaira? Hadd említsünk egy példát: a WannaCry ransomware adat titkosító hekkertámadása 2017. májusban több mint 230 000 számítógépet tett használatra alkalmatlanná. A WannaCry áldozatai közül sokan kórházak, bankok, távközlési vállalatok és raktárak voltak több mint 150 országból. Ez is pontosan mutatja azt, hogy áldozat bárki lehet, illetve, hogy milyen könnyen elveszíthetők a számítógépen tárolt információk.



Ma már tudjuk, hogy a megoldás kézenfekvő.

A hagyományos helyi adattárolók könnyű támadhatósága miatt érdemes minden kritikus üzleti információt a Felhőbe költöztetni.



Van **három** okunk, illetve magyarázatunk, hogy miért biztonságosabb az adattárolás a felhőben:

Azok számára, akik nem ismerik
a **Microsoft Azure Cloud**-ot:



Az Azure egy olyan integrált felhő architektúrájú számítástechnikai szolgáltatás, amit bármilyen méretben igénybe lehet venni az alkalmazások telepítésére, az adatok tárolására és a biztonsági mentések védelmére. A szolgáltatás egyszerűen **méretezhető bármilyen üzleti körülményhez** megfizethető költségek mellett, de a legfontosabb kiemelni, hogy használata rendkívül biztonságos.

1.

Hány alkalmazottja van a kibébiztonság intenzív és naprakész ismerstével? Vagy vegyük azt, hogy sok időt szán a számítógépes biztonság megismerésére, és akkor már valóban készen áll egy hekker támadásra? Szerintünk nem. A Microsoft Felhő viszont rendelkezik mindennel, ami Önt és vállalatát hozzásegítheti a legjobb üzleti teljesítmény eléréséhez garantált biztonság mellett. Ráadásul még pénzt is takaríthat meg, mivel nem kell aggódnia a drága informatikai erőforrások bérlése miatt, és nem kell új szerverek és csúcstechnológiát képviselő biztonsági kiegészítők megvásárlásával foglalkoznia.



Szakértők irányítják

2.

Meg tudja akadályozni, hogy alkalmazottainak eszközei, így azon tárolt adatai ne kerüljenek illetéktelen kezekbe?

Mivel az üzleti kritikus adatait ma már nem csak a természeti katasztrófától vagy az elektromos kisléstől kell óvnia, a Felhő megoldás alkalmas arra, hogy fizikailag elválassza a felhasználót és az adatait. A „Controlled Access”, vagyis a szabályozott hozzáférés kifejezés itt azt is jelenti, hogy az adatokat a Felhőben, egy nehezen meghatározható fizikai helyen tárolják, így pl. a munkavállalók és az adataik között nincs fizikai hozzáférési lehetőség. Ez megnehezíti a hekkerek számára, hogy megtalálják az adott felhasználó által kezelt adatokat és visszaéljenek vele. A Microsoft biztonsági protokolljai csak a kívánt hitelesítés után, megfelelő hozzáférési jogosultság birtokában biztosítják az adatok elérését.



Szabályozott hozzáférés

3.

A Fortune 500 cégek 80%-a használja az Microsoft Azure szolgáltatást. Igen, nem Amerikában vagyunk és még az arányok sem stimmelnek, de azért abban van valami megnyugtató, ha az Egyesült Államok legjobban „pörgő” vállalatainak nagyobb része bízik a Microsoft Felhőben, nem? Ha a nagyvállalatok a Microsoft Azure-re bízzák az üzleti információikat, akkor bárki más miért ne követhetné őket? A Felhő megfelel bármilyen üzleti igénynek, ráadásul ugyanazt a biztonsági támogatást nyújtja, mint a Fortune 500 cégek esetében. Kisebb vállalkozásoknak persze nem kell ugyanannyit fizetni, mint nekik.



Elismert platform

Végül, ha adhatunk egy tanácsot:

A cél mindig egy olyan stratégia kifejlesztése és megvalósítása, amelyről Ön, illetve cége úgy érzi, hogy adatai jól menedzselhetők és védett rendszerben vannak eltárolva. Ennek az állapotnak az eléréséhez segítséget nyújthatnak a MultiSoft szakértői. Nem utolsó sorban kollégáink tájékoztatást adnak, hogyan lehet a költségeket alacsonyan tartani.