

# OUCH!

## Ebben a kiadásban...

- Áttekintés
- Felhőszolgáltató választása
- Adatvédelem

## A felhő biztonságos használata

### Áttekintés

A „felhő” olyan hatékony technológia, amelyet mind a vállalatok, mind a magánszemélyek egyre többen használnak. A „felhő” a különböző emberek számára mást-mást jelent, de általánosságban elmondhatjuk, hogy olyan szolgáltatások, amelyeket az Internet segítségével veszünk igénybe, például adatok tárolására és kezelésére. A felhő alapú szolgáltatásoknak nem csak az az előnyük, hogy az adataink könnyen hozzáférhetőek különböző eszközökről a

világ bármely pontjáról, hanem az is, hogy azt azzal tudjuk megosztani, akivel csak akarjuk. A szolgáltatást azért nevezzük „felhőnek”, mert általában nem tudjuk, hogy az adataink fizikailag hol találhatóak. Az ismert felhő alapú szolgáltatások között olyanokat találhatunk, mint például dokumentumok készítése a Google Docs segítségével, fájlok megosztása a Dropbox-on, saját szerver telepítése az Amazon Cloud-on, és az Apple iCloud-ba feltöltött képek vagy zenék. Az ilyen szolgáltatások segítségével lényegesen javíthatjuk a saját produktívitásunkat, azonban vannak kockázatok is. Az e havi hírlevél bemutatja, hogyan lehet biztonságosan kihasználni a felhő adta lehetőségeket.

### A szerzőről

Dave Shackelford ([@daveshackelford](https://twitter.com/daveshackelford)) egy profi tanácsadó, a Voodoo Security tulajdonosa, és számos SANS kurzus szerzője, mint például a SANS Security 579: Virtualizáció és privát Felhő biztonság, illetve Security 524: Felhő biztonsági alapok.

### Felhőszolgáltató választása

A felhő nem jó vagy gonosz, hanem egy olyan eszköz, amellyel megoldhatjuk a feladatainkat otthon vagy a munkahelyünkön. Azonban az ilyen szolgáltatások használatakor a saját adatainkat kezelés, tárolás céljából átadjuk másoknak, és elvárjuk, hogy tartsák biztonságos körülmények között, illetve, hogy mindig elérhetőek legyenek. Mivel biztosra kell mennünk a döntésünk bölcsességét illetően, kérdezzük meg a rendszergazdát, hogy a munkahelyi számítógépen, illetve a céges adatokkal kapcsolatosan használhatunk-e felhő alapú szolgáltatást. Ha van lehetőségünk felhő szolgáltatás igénybevételére, akkor győződjünk meg arról, hogy melyiket és milyen feltételekkel használhatjuk. Ha személyes célra akarjuk használni, akkor az alábbiakat vegyük figyelembe:

1. **Támogatás:** kaphatunk segítséget a felmerült problémákkal vagy kérdésekkel kapcsolatban? Van telefonos ügyfélszolgálat vagy email cím, ahova fordulhatunk? Esetleg van nyilvános fórum vagy a Gyakran Ismételt Kérdéseknek fenntartott rész a szolgáltatás weboldalán?

## A felhő biztonságos használata

2. **Egyszerűség:** mennyire egyszerű használni a szolgáltatást? Az összetettebb szolgáltatások használata esetén könnyebb hibázni, ami akár az adatok elvesztéséhez is vezethet. Olyan szolgáltatást válasszunk, amely könnyen érthető, használható, és konfigurálható!
3. **Biztonság:** milyen személyes adatot gyűjtenek a felhasználóról? Titkosított csatornán jut el a számítógépen tárolt adat a felhő szolgáltatóhoz? A szolgáltató szerverén titkosított formában tárolják a feltöltött adatokat, és ha igen, akkor ki tudja visszafejteni a titkosítást?
4. **Általános szerződési feltételek:** szánjunk egy kis időt az ÁSZF elolvasására (gyakran meglepően könnyű elolvasni)! Tudjuk meg, kinek van hozzáférése az adatainkhoz, és milyen jogaink vannak, illetve milyen biztonsági felelőssége van a szolgáltatónak és a felhasználónak!



*A felhő segít abban, hogy az információink könnyebben hozzáférhetőek legyenek, ami javíthat a produktívitásunkon, de legyünk óvatosak az állományok tárolásával és megosztásával kapcsolatban.*

## Adatvédelem

Miután kiválasztottuk a számunkra megfelelő szolgáltatást,

a következő lépés annak megfelelő használata lesz. Az, hogy hogyan férünk hozzá, és hogyan osztjuk meg az adatainkat, gyakran sokkal nagyobb hatással van az adataink biztonságára, mint bármi más, ezért az alábbiakat vegyük figyelembe:

1. **Hitelesítés:** használjunk erős és egyedi jelszót a felhőszolgáltatáshoz. Ha a szolgáltató lehetőséget ad a kétfaktoros (kétfaktoros) hitelesítésre, akkor ajánlott igénybe venni azt. Talán ez a legfontosabb lépés, ami a fiókunk biztonságát garantálja.
2. **Fájlok és mappák megosztása:** a felhőben könnyen megy a megosztás. Talán túlságosan is. A legrosszabb esetben véletlenül a teljes Internet számára megosztunk bizonyos fájlokat vagy mappákat. A védekezés legjobb módja, ha alapértelmezésként senkivel nem osztjuk meg az adatainkat. Ha szükséges, akkor egyedileg határozzuk meg, hogy kik (személyek vagy bizonyos csoportok) férhetnek hozzá az adott állományhoz vagy mappához. A későbbiekben, amikor valakinek már nincs szüksége a megosztásra, akkor vonjuk vissza a jogosultságait. A szolgáltatók lehetőséget biztosítanak arra, hogy könnyedén nyomon kövessük, kik fértek hozzá az állományainkhoz és mappáinkhoz.
3. **Megosztott fájlra és mappára mutató hivatkozások:** a felhő szolgáltatások egyik leggyakoribb alkalmazása az állományainkra és mappáinkra mutató hivatkozások készítése. Ezen funkció használatával egyszerűen meg tudunk osztani bármit egyetlen hivatkozás készítésével. Azonban ennek a megoldásnak komoly biztonsági hátrányai vannak, mivel a hivatkozás birtokában bárki hozzáférhet a személyes adatainkhoz. Miután elküldtük valakinek a linket, az bármikor továbbküldheti másoknak, de akár egy keresőben (például Google) is tárolásra kerülhet. A későbbiekben,

