Havi biztonság tudatossági hírlevél számítógép felhasználók számára

OUCH!

Ebben a kiadásban...

A felhő biztonságos használata

Áttekintés

A „felhő” olyan hatékony technológia, amelyet mind a vállalatok, mind a magánszemélyek egyre többet 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 produktivitásunkat, azonban vannak kockázatok is. Az e havi hírlevél bemutatja, hogyan lehet biztonságosan kihasználni a felhő adta lehetőségeket.

A szerzőről

Dave Shackleford (**@daveshackleford**) egy profi tanácsadó, a Voodoo Security tulajdonosa, és számos SANS kurzus szerzője, mint például a SANS Sexcurity 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 produktivitásunkon, 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 kétlépcsős (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 szermélyes adatainkhoz. Miután elküldtük valakinek a linket, az bármikor továbbküldheti másoknak, de akár egy keresőben (például Google) is tárolásra kerülhet. A későbbiekben,

A felhő biztonságos használata

amikor már nincs szükség a hivatkozással megosztott fájlok vagy mappák elérésére, akkor tiltsuk le a hivatkozást, vagy legalább használjunk jelszót a linkhez.

4. **Beállítások**: értsük meg a szolgáltató által felkínált biztonsági szolgáltatásokat. Például ha megosztunk valakivel egy állományt vagy mappát, az továbboszthatóe másokkal a mi beleegyezésünk nélkül? Továbbá, van-e lehetőség arra, hogy lássuk, ki tekintette meg az általunk megosztott tartalmakat. Tudjuk-e a megosztásnál korlátozni a jogokat pl. „csak olvasásra” az „olvasás és szerkesztéssel” szemben, amikor más felülírhatja a fáljainkat?
5. **Vírusvédelem**: mindig telepítsük a legújabb verzióját az antivírus szoftverünket azokra az eszközökre, amelyekről használjuk a felhőszolgáltatást. Ha az általunk megosztott fájl vírussal fertőzött, akkor másokat is megfertőzhet, ha hozzáférnek.

További Információ

Iratkozzon fel a havi rendszerességű OUCH! biztonságtudatossági hírlevélre, férjen hozzá az OUCH! archívumhoz, tudjon meg többet a SANS biztonságtudatossági megoldásairól a securingthehuman.sans.org/ouch/archives weboldalon keresztül.

Magyar Kiadás

Kormányzati, távközlési és informatikai szolgáltatóként, Magyarország egyik stratégiai fontosságú gazdasági társasága a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. Társaságunk kiemelt feladata a kormányzati infrastruktúra működtetése, az e-közigazgatási megoldások támogatása, valamint kormányzati szintű informatikai szolgáltatások nyújtása. További információ a http://www.nisz.hu oldalon olvasható.

Hivatkozások

A kétlépcsős hitelesítésről:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201509_hu.pdf
A jelmondatokról:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201504_hu.pdf
A jelszókezelő programokról:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201510_hu.pdf
A káros szoftverekről:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201504_hu.pdf
A biztonsági mentésekről:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201603_hu.pdf

Szerkesztette: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Fordította: Birkás Bence