Havi biztonság tudatossági hírlevél számítógép felhasználók számára

OUCH!

Ebben a kiadványban...

- **Áttekintés**
- **Felhőszolgáltató választása**
- **Adatvédelem**

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 is 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 OUCH! e havi számában megmutatjuk, hogyan lehet biztonságosan kihasználni a felhő adta lehetőségeket.

A szerzőről

James és Kelli Tarala (@isaudit / @kellitarala) az Enclave Security vezető tanácsadói, valamint számos SANS előadás szerzői, mint például a SANS Audit 566: Implementing and Auditing the Twenty Critical Security Controls és az MGT 415: A Practical Introduction to Risk Assessments.

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:

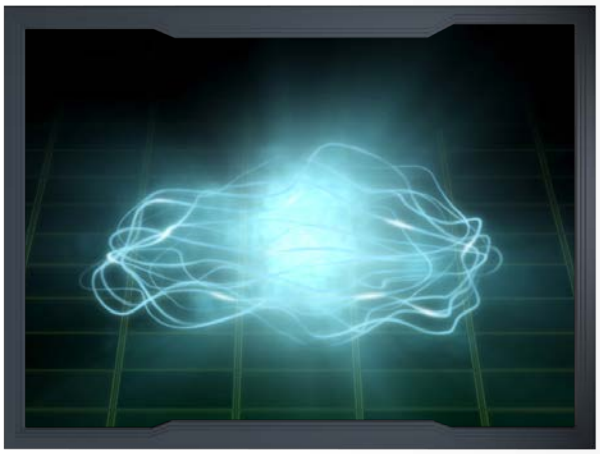
1. **Támogatás**: kaphatunk segítséget a felmerült problémákkal vagy kérdésekkel kapcsolatban? Van telefonos ügyfélszolgálat vagy email cím, ahova fordulhatunk? Esetleg van nyilvános fórum vagy a Gyakran Ismételt Kérdéseknek fenntartott rész a szolgáltatás weboldalán?
2. **Egyszerűség**: mennyire egyszerű használni a szolgáltatást? Az összetettebb szolgáltatások használata esetén könnyebb hibázni, ami akár az adatok elvesztéséhez is vezethet. Olyan szolgáltatást válasszunk,

© The SANS Institute 2014

A felhő biztonságos használata

amely könnyen érthető, használható, és konfigurálható!

3. **Biztonság**: titkosított csatornán jut el a számítógépeden 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!



A felhő segít abban, hogy bárhonnan hozzáférjünk adatainkhoz. Ezáltal produktívabbak lehetünk, 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 két lépcsős (kétfaktoros) hitelesítésre, akkor ajánlott igénybe venni azt.
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, amikor már nincs szükség a hivatkozással megosztott fájlok vagy mappák elérésére, akkor tiltsuk le a hivatkozást, vagy legalább használjunk jelszót a linkhez.
4. **Beállítások**: használjuk a szolgáltató által felkínált biztonsági szolgáltatásokat! Például ha megosztunk valakivel egy állományt vagy mappát, az továbbosztható-e másokkal a mi beleegyezésünk nélkül?

© The SANS Institute 2014

A felhő biztonságos használata

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.
6. **Adatmentés**: bár a felhőszolgáltató is végez adatmentést, mindig gondoskodjunk saját magunk is a biztonsági másolatokról! Nem csak azért fontos ez, mert például megszűnhet a szolgáltató, vagy üzemszünet léphet fel náluk, vagy egyéb más ok miatt válik elérhetetlenné, hanem azért is, mert a nagy mennyiségű adatot sokkal könnyebb egy helyi mentésből visszaállítani, mint a felhőből. Ellenőrizzük azt is, hogy a szolgáltató milyen gyakran menti az adatainkat, adnak-e lehetőséget arra, hogy a módosított fájloknál visszaállítsuk a korábbi állapotot, illetve, hogy mennyi ideig őrzik meg a mentéseket?

További Információ

Iratkozzon fel a havi rendszerességű OUCH! biztonságtudatossági hírlevélre, férjen hozzá az OUCH! archívumhoz, tudjon meg többet a SANS biztonságtudatossági megoldásairól a http://www.securingthehuman.org 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

Jelszavak:	http://www.securingthehuman.org/ouch/2013#may2013
Jelszókezelő megoldások:	http://www.securingthehuman.org/ouch/2013#october2013
Személyes biztonsági mentés és helyreállítás:	http://www.securingthehuman.org/ouch/2013#september2013
Általános biztonsági kifejezések:	http://www.securingthehuman.org/resources/security-terms

OUCH! a SANS Securing The Human program által közzétett hírlevél, amelyre Creative Commons BY-NC-ND 4.0 licensz feltételei vonatkoznak. A hírlevél szabadon terjeszthető vagy felhasználható tudatosító programban, addig amíg az nem kerül módosításra. A fordításért vagy további információért kérjük írjon az ouch@securingthehuman.org címre.

Szerkesztette: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Fordította: Birkás Bence, Benyó Pál, Árvai Gábor

securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus