OUCH! 2021. augusztus

SANS SECURITY AWARENESS

OUCH!

Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

A „felhő” biztonságos használata

Áttekintés

Valószínűleg mindenki hallott már a felhőszolgáltatásokról. Vagyis arról, hogy adatainkat tárolhatjuk különböző szolgáltatóknál, azokat az interneten keresztül, távolról kezelve. Akkor is a felhőt használjuk, ha Google Docs dokumentumot készítünk, a Microsoft Office 365 fiókunkkal levelezünk, a Dropbox segítségével fájlokat osztunk meg, vagy épp ha az iCloudba mentjük a képeket Apple telefonunkról. Miközben adatainkhoz a világ bármely pontján hozzáférhetünk, és azokat többféle eszközön is kezelhetjük, gyakran nem is vagyunk tisztában azzal, hogy azok fizikailag pontosan hol kerülnek tárolásra, és hogy erre valójában nincs is ráhatásunk.

Hogyan válasszunk felhőszolgáltatót?

A felhőszolgáltatások se nem jók, se nem gonoszak. Lehetséges eszközök csupán. Ugyanakkor, ha belegondolunk, az ilyen szolgáltatások igénybevételével bizalmas adatainkat lényegében idegenek kezébe adjuk, akiktől egyszerre várjuk, hogy azokat tartsák biztonságban, de közben tegyék is elérhetővé számunkra. Így hát érdemes alaposan átgondolni, hogy melyik szolgáltatót választjuk. Ha munkáról van szó, mindig egyeztessünk felettesünkkel, hogy szabad-e egyáltalán felhőszolgáltatást használnunk, illetve, hogy melyik az engedélyezett. Ha pedig a felhőszolgáltatást magáncélra vennénk igénybe, fontoljuk meg a következőket:

1. **Bizalom:** Meg tudunk bízni az adott szolgáltatóban? Ez egy jól ismert szolgáltató, amelyet több millióan használnak, vagy esetleg egy kicsi, ismeretlen cég, amit egy olyan országból irányítanak, amelynek a létezéséről sem hallottunk korábban?
2. **Támogatás**: Milyen könnyen kaphatunk segítséget, vagy választ az esetleges kérdéseinkre? Elérhető olyan telefonszám vagy e-mail cím, amin felvehetjük a kapcsolatot a céggel? Kaphatunk támogatást más egyéb módon? Létezik nyilvános fórum, vagy GYIK (Gyakran ismételt kérdések)?
3. **Egyszerűség**: Mennyire egyszerű használni a szolgáltatást? Minél komplexebb egy szolgáltatás, annál valószínűbb, hogy hibázni fogunk, és véletlenül kiszivárogtatjuk, vagy esetleg töröljük adatainkat. Keressünk olyan felhőszolgáltatást, amit könnyű beállítani és kezelni.
4. **Biztonság**: Hogyan kerülnek adataink a szolgáltatóhoz? Alkalmaznak titkosítást a kapcsolat védelme érdekében? Hogyan tárolják az adatokat? Ha tikosítják az adatokat, ki az, aki ezekhez hozzáfér? Ne feledjük, hogy a biztonság közös felelősség, az nem csak a szolgáltatáson, hanem rajtunk is múlik!

5. **Kompatibilitás:** A szolgáltató minden olyan eszközt és operációs rendszert támogat, amelyet használni szeretnénk?
6. **Felhasználási feltételek**: Szánjunk rá egy kis időt, és fusssuk át a szolgáltatás igénybevételének feltételeit! (Meglepő, de sok esetben ezekben egészen könnyű kiigazodni.) Mely ország törvényei érvényesek az adott szolgáltatóra nézve? Legyünk különösen figyelmesek azzal kapcsolatban, hogy a szolgáltató számára mihez adunk engedélyt!

Adataink biztosítása

A következő lépés, hogy megfelelően használjuk a szolgáltatást. Az, hogy hogyan férünk hozzá adatainkhoz, és hogy ezeket hogyan osztjuk meg, sok esetben jóval nagyobb mértékben befolyásolja azok biztonságát, mint bármi más. Néhány kulcsfontosságú lépés ezügyben:

1. **Hitelesítés**: Használjunk erős, egyedi jelszót az online fiókok védelmében! Amennyiben elérhető a kétfaktoros azonosítás, erősen javasolt a használata!
2. **Fájlok és könyvtárak megosztása**: A felhőszolgáltatók leegyszerűsítik az adatok megosztását – esetenként túlságosan is. Előfordulhat, hogy véletlenül nyilvánosságra hozzuk adatainkat. Ettől azonban megvédhetjük magunkat, ha csak bizonyos embereknek vagy csoportoknak adunk hozzáférést adott fájlokhoz vagy mappákhoz. Amikor pedig valakinek már nincs szüksége hozzáférésre, egyszerűen töröljük az adott személy hozzáférését. A választott felhőszolgáltatónak nyomon kell tudnia követni, hogy kinek van hozzáférése fájljainkhoz és könyvtárainkhoz.
3. **Beállítások**: Legyünk tisztában azzal, hogy milyen biztonsági beállítási lehetőségek érhetőek el az adott szolgáltatónál. Például, ha képeket vagy egyéb fájlokat osztunk meg másokkal, ők is továbboszthatják ezeket a tudtunkon kívül?
4. **Megújítás**: Ne felejtsük el időben megújítani az előfizetésünket, mert különben akár el is veszíthetjük a hozzáférést adatainkhoz.

A szerzőről

Tameika Reed (@womeninlinux), a Women in Linux alapítója. Olyan kezdeményezések vezetője, amelyek fókuszában az üzemeltetés, a kiberbiztonság, a DevSecOps és a vezetéstudomány áll. Rendszeresen heti találkozókat szervez különböző témákban, mint például az infrastruktúra üzemeltetés vagy a blokklánc technológia. Előadóként részt vett már az OSCon, a LISA, a Seagl és a HashiConf EU konferenciákon.

Források

Pszichológiai manipulációs támadások: https://www.sans.org/security-awareness-training/ouch-newsletter/2017/social-engineering
Egyszerű jelszókezelés: https://www.sans.org/security-awareness-training/resources/making-passwords-simple
Jelszókezelők: https://www.sans.org/security-awareness-training/resources/making-passwords-simple
A frissítés ereje: https://www.sans.org/security-awareness-training/resources/power-updating

A fordítást készítette: Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI)