
SICONTACT™
biztonság a digitális világban

\o/ NEM ÉRDEMES SPÓROLNI A BIZTONSÁGON \o/

# Szőr Péter (1970-2013)

- Pasteur víruskereső
- 38 szabadalom
- 2005. The art of Computer Virus Research and Defense
- 2010. A Vírusvédelem művészete

*"Tökéletes védelem sajnos nincs.*
*Ha a felhasználó képzettebb, akkor a védelem is eredményesebb."*

\o/ NEM ÉRDEMES SPÓROLNI A BIZTONSÁGON \o/

# ::Pár szó a nyilvánosságról::


**2008. október**

- A beteg Steve Jobs hamis halálhíre, Apple részvények 10 perc alatt 10%-os esés

**2013. április**

- Az AP hírügynökség Twitter feltörés, Dow Jones ipari átlagindex 150 pontos esése, a Standard and Poor's 500-as indexe 3 perc alatt 136.5 milliárd dollárt veszít

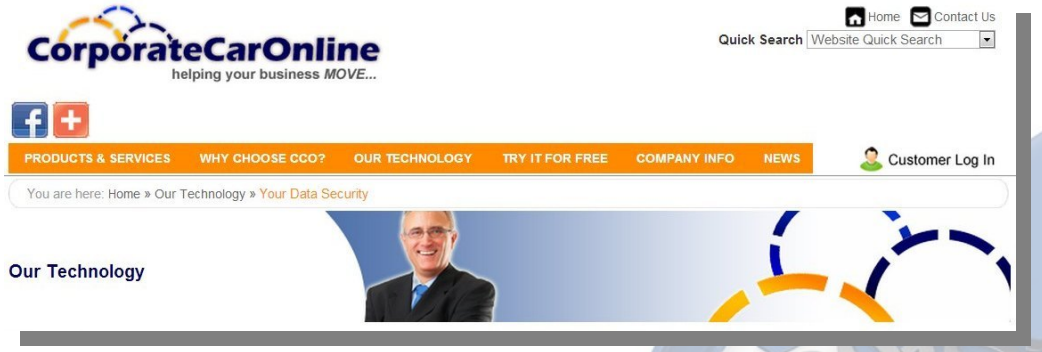
**2015. július**

- Hamis Bloomberg News weboldal: „31 mrd USD Twitter ajánlat”
- A részvény 8.5% meglódul, de a cáfolat után is 3%-kal az előző napi szint felett

*A piac fél, érzékenyen reagál, pump & dump manipuláció, 2007. USA: számítógépes csalásból már több pénz, mint a drogkereskedelemből - 105 milliárd dollár*

\o/ NEM ÉRDEMES SPÓROLNI A BIZTONSÁGON \o/

# ::Adobe incidens - 2013. október::




- Előbb "csak" 2, utána 38 millió ügyféladat, később kiderül, hogy forráskódok is
- Nyilvánosságra kerülnek a jelszavak, plusz a jelszó-emlékeztetőkben egy az egyben

Járulékos áldozat: közös szerveren feltörték a Corporate-Car-Online-t is
- Luxus limuzin kölcsönző, 850 ezer VIP ügyfél, pl. Donald Trump, Tom Hanks, stb.
- Kiszivárgott útvonalak, 241 ezer hitelkártya adata
- Ipari kémkedés, testreszabott APT támadások, célzott adathalászat, stb.

*Többször kozmetikázott beismerés, vétlen szereplők járulékos kára*

\o/ NEM ÉRDEMES SPÓROLNI A BIZTONSÁGON \o/

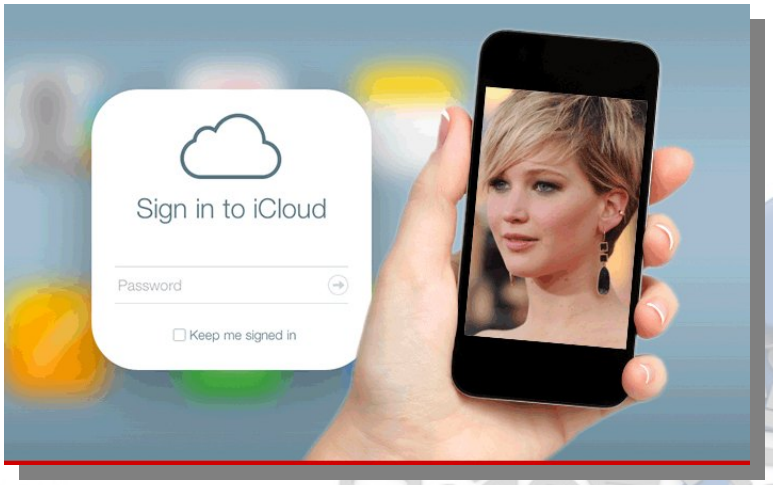
# ::Linkedin incidens - 2012. június::


- 6.5 millió felhasználó adata, jelszava került ki orosz fórumokra, nevek, üzleti kapcsolatok
- 230 ezer akkori magyar felhasználó, szótár alapon gyorsan törhető szimpla SHA-1 hash
- Linkedin spam kampányok: jelszó "megerősítés"
- 2014. szeptember: bejelentkezés kontroll: "click on See where you are logged in", 2FA bevezetése, e-mail értesítés a jelszóváltoztatásokról, adatmentési lehetőség

*Üzemeltetői hibák, primitív SHA-1 hash kezelés (salted) nélkül, késői utólagos hiánypotló fejlesztések*

\o/ NEM ÉRDEMES SPÓROLNI A BIZTONSÁGON \o/

# ::Apple iCloud incidens - 2014. augusztus::

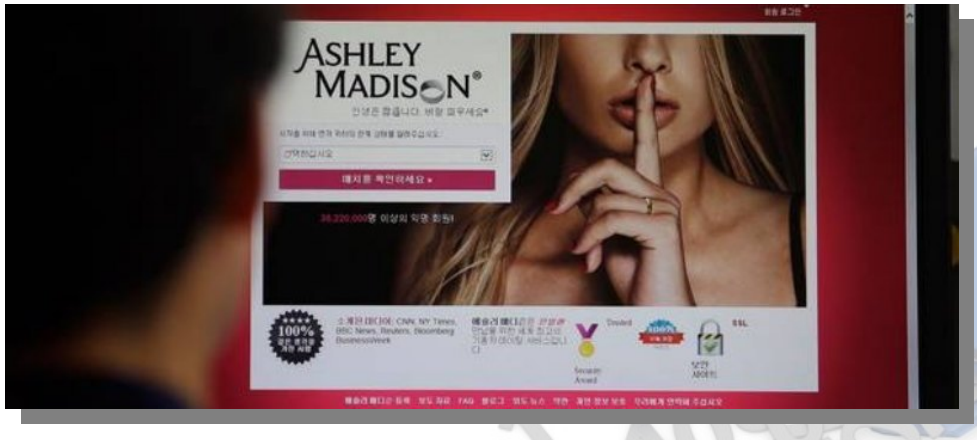



- Hírességek (Jennifer Lawrence, Kate Upton, Avril Lavigne) meztelen képei a Reddit és a 4chan oldalain
- Apple: "Nem az iCloud rendszer hibája"
- NakedSecurity szavazás: "94.59% -> legyen 2FA az iCloud-nál"
- 2014. szeptember: hiányzó brute-force védelem aktiválása a Find My iPhone szolgáltatáson is, 2FA bevezetése, e-mail értesítés a bejelentkezésekről

*Felelősség hárítása, majd utólag elvégzett gyors hiánypotló fejlesztések*

\o/ NEM ÉRDEMES SPÓROLNI A BIZTONSÁGON \o/

# ::Ashley Madison incidens - 2015. augusztus::

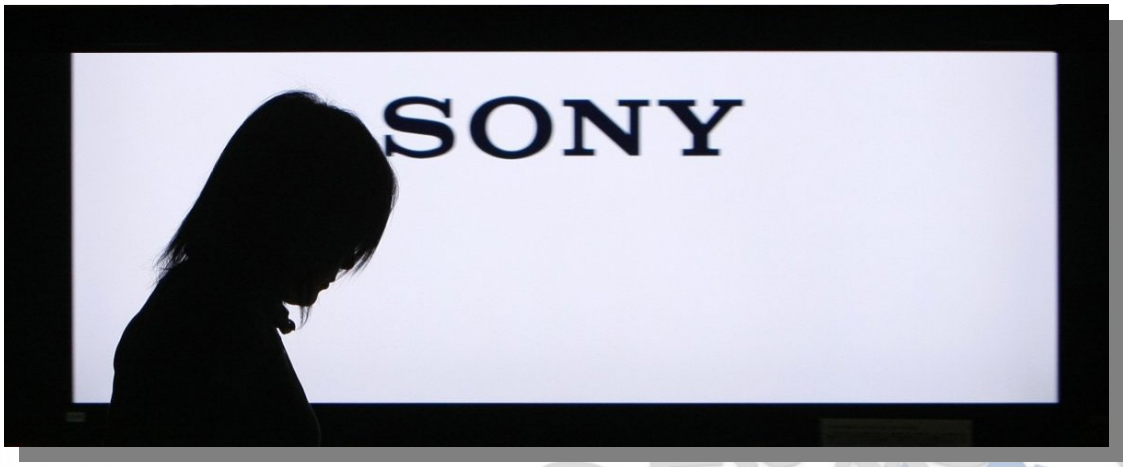



- Avid Life Media fizetős szolgáltatása anonimitást ígért
- 37 millió "ügyfél" adat: nevek, e-mailcimek, bankkártya, szexuális preferenciák
- feltöltött fotók, ügyfelek és a belső munkatársak levelezése
- 9.7 GB adat (Impact Team)
- A 19 dolláros végleges törlés nem működött

*- Üzemeltetői hibák: e-mail regisztráció hitelesítés nélkül, hamis női profilok, hibás törlés, Reputation Management Consultants*
*- Retorziók az USA hadseregben, első öngyilkosságok (Torontó)*
*- Kezdődő perek (pl. magánszemély 5 millió USD)*

\o/ NEM ÉRDEMES SPÓROLNI A BIZTONSÁGON \o/

# ::Döntések, következmények, védekezés::




A SONY 20 egymást követő támadás sorozatának (2014.) mérlege az audit után:

- 24 milliárd USD veszteség
- Rosszul kezelték, rosszul kommunikálták
- 10 ezer USD költséggel megelőzhető lett volna (HP)

- *Incidens után gyors reagálás: tájékoztatás, hitelkártya-monitorozás, Security Incident Response Team*
- *Fontos a megelőzés: befektetni a biztonságba, biztosítani a folytonos üzletmenetet, rendszeres biztonsági oktatás, pentesting, audit*

SICONTACT
biztonság a digitális világban

\o/ NEM ÉRDEMES SPÓROLNI A BIZTONSÁGON \o/

# ::A Sicontact küldetése a biztonság::


*http://www.sicontact.hu*
*csizmazia.istvan@sicontact.hu*

ESET Cyberoam AIDA64