Publicisztika
A szerző összes írása

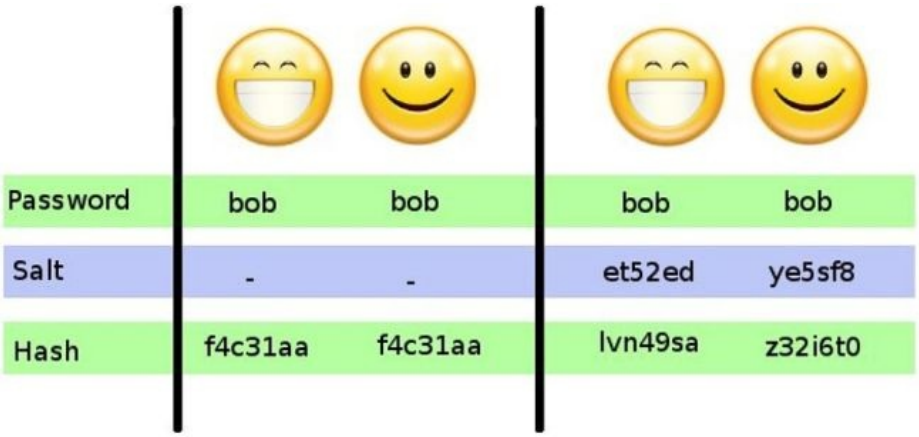
Csizmazia István

Like Send g+1 0 Tweet 0

Meghökkentő mesék
2014. 05. 29. csütörtök 16:00

Divatos téma lett manapság a biztonság, mindenfajta értelemben, de mi persze főként a számítógépes biztonsággal kapcsolatos vonalra fókuszálunk. Eheti kérdésünk, hogy rajtunk mint felhasználókon lévő felelősséget mennyire tudatosan kezeljük? Pedig kéne, és ez az alábbi rövid történetekből is szemléletesen látszik majd.

Volt a minap egy érdekes cikk a TheRegister hasábjain, ahol röviden azt boncolgatták, hogy bár a biztonság otthon kezdődik, nem igazán teszünk meg érte mindent mégsem. Amikor aztán incidens van, például kikerülnek a jelszavaink vagy a hashek a szolgáltatónktól, akkor ujjal mutogatunk rájuk, lám ők tehetnek mindenről. Nem meglepő módon ők pedig mi ránk mutogatnak: A TE jelszavad, változtass jelszót! - mondják nekünk. Védjétek jobban az adatainkat! - mondhatnánk erre mi őnekik. Ami igaz, igaz, sok helyen valóban vigyázhatnának rájuk sokkal jobban is, hogy csak egy példát mondjunk, a LinkedIn is csak a 2012 nyári feltörés után alkalmazta a jelszóhashek sózását.
http://antivirus.blog.hu/2012/06/13/biztonsagi_tanacsok_a_linkedin_incidens_kapcsan



Persze az is tény, hogy a minket érintő temérdek szolgáltatás, account biztonságtudatos használata nem mindig egyszerű feladat, emellett pedig az elektronikus kártevők, csalások, adathalász támadások, átverések egyre gyarapodó számát tekintve a védekezés szinte lehetetlen feladat egy átlagfelhasználó szemszögéből. Pedig muszáj felnőni ehhez a feladathoz, és a felhasználóknak olyan alapvető dolgokon elgondolkozni, hogy biztosan jó ötlet-e mindenhol ugyanazt a jelszót használni. Sokszor ugyanis a minden weboldalon azonosan használt jelszó okozza a problémákat, vagy például a szótáralapon percek alatt törhető primitív "abc123" típusú password-ök választása. És ilyenkor valóban jó kérdés, hogy ki mutogathat kire.

Ugyanígy érdemes lehet manapság a vállalati kémkedések korában a különböző cégeknek azt is végiggondolni, hogy nem biztos, hogy minden esetben jó ötlet kiszervezni az IT részleget, vagy az ügyfélkapcsolatok kezelését a költségek csökkentése miatt. Mert az efféle szolgáltatások végzése, vagy az ügyfél adatokhoz való hozzáférés - akár csak egy biztonsági szoftver kiválasztása - mélyen bizalmi kérdés (is). Ami aztán okkal, vagy ok nélkül is meginoghat időnként, akár politikai csatározások keretében is, mint legutóbb Kínában, ahol először május 16-án azt jelentették be, hogy a kormányzati számítógépeken nem engedélyezik a Windows 8 operációs rendszer használatát. Még a szakértőknek sem teljesen világos a döntés háttere, egyesek nem is a rejtett backdoor lehetőséggel magyarázták, hanem az ottani 70%-os XP részesedés miatti nyomásgyakorlásnak tudták be. Amit aztán május végén követett az újabb hír, megtiltják a helyi bankoknak az IBM-szerverek használatát. A kínai kormány itt már indoklást is adott, miszerint a tiltást biztonsági okokra hivatkozva vezetné be. Igaz elemzők ebben az esetben is látnak politikai szálat, vagyis hogy valójában mindez sokkal inkább a kémkedési ügy miatti reváns lehet.

Mi viszont most ne bonyolódjunk bele a kusza politikai szálak boncolgatásába, de azért maradjunk még egy kis időre Kínánál és a hardvereknél. Egy nemrég lezajlott hacker konferencián ugyanis az egyik érdekes előadás arról szólt, hogy a gyanútlan felhasználó számára egy nevetségesen (vagy gyanúsan) olcsó kínai Androidos telefon is váratlan, sőt egyenesen kellemetlen meglepetéseket tartogathat. A biztonsági kutató szépen tételesen lenaplózta, milyen csapdákat talált a külsőre Samsung Galaxynak látszó (!) eszközben. Volt itt aztán temérdek indokolatlan engedélykérés, hamisított appok sokasága, észrevétlenül különféle kínai címekre küldött személyes adatok tömkelege, és hasonlók. Nagyon szemléletes volt mindez például az előretelepített "Opera böngésző" hasonmás esetében, ahol a gyári, ártalmatlan eredeti változattal ellentétben a fake program simán hozzáférhetett a címjegyzékünkhöz, az SMS üzeneteinkhez, és minden egyéb bizalmas személyes telefon adatainkhoz, emellett felhatalmazása volt külön értesítés nélküli letöltésre, sőt a háttérben hangrögzítésre is.

A rovat ajánlója
Hosszú búcsú Ingerküszöbök
Fel kéne már ébredni - helyzet van
Te is lehetsz célszemély
Legolvasottabb cikkek
Pénzutalás mobilszámra
Felhők felett a Kék Óriás
Jócskán spórolhatnak a háztartások új számítógépekkel
Fel kéne már ébredni - helyzet van
Döbbenetes nyomtatók

Eseménynaptár

Kiemelt esemény:
2014.
Május

H	K	Sz	Cs	P	Sz	V
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

És most újra menjünk vissza kicsit a jelszavakhoz, amikből nem véletlenül állítják össze minden évben az elrettentő Worst Password gyűjteményt. Sajnos ez a valóság, szembesít minket a katasztrofális jelszóválasztási szokásainkkal. Sokan nem látják bele azt a pluszt, hogy nem azért választok jelszót, hogy kipipáljam, ezt is elvégeztem, hanem minden áron meg akarom védeni az értékes adataim, ezért most Edgar Allen Poe-t vagy Lovecraft-ot megszégyenítő trükkös és furmányos módon fogok kibabrálni minden próbálkozó szemétládával. Mostani történetünk az Apple háza tájáról származik, amelyben ausztrál lapok arról számoltak be, hogy egyes iPhone és iPad felhasználókat kizártak a készülékükből. A közösségi oldalak beszámolói szerint a pórul járt áldozatok egy kéretlen üzenetet kaptak a készülékükre a Find My iPhone funkció nevében, amely azt állította, hogy az adott eszközt meghackelték. A feloldáshoz - a hamis antivírusokhoz és a háttértárat titkosító CryptoLockerhez hasonlóan - itt is pénzt kért az állítólagos Oleg Pliss nevű támadó, jellemzően 5 és 100 amerikai dollár közötti összeget. A felhasználók egy nagy része most az Apple-nél reklamált, aki viszont azt válaszolta nekik: mivel rendszerük elvileg nem törhető fel, ezért nem illetékesek segíteni. És akkor most hogy is jön ide a jelszó témakör? Hát úgy, hogy szakértők szerint valószínűleg arról lehet szó, hogy a kiberbűnözők a más helyszínről és más forrásból megszerzett jelszavakat elkezdték kipróbálgatni az Apple Find My iPhone szolgáltatáson, hátha valaki itt is ugyanazt használta.

Biztonság és bizalom fontosak így együtt. Benne a milyen jelszót választunk, használjuk-e több helyen is ugyanazt, milyen hardvert veszünk, kinek a termékében bízhatunk és hogyan használjuk biztonságtudatosan az eszközeinket igen lényeges kérdések maradnak továbbra is. Amihez ugye folyamatos gondolkodásra, odafigyelésre, a világban történő biztonsági incidensek naprakész követésére, és okos döntésekre van-lenne szükség.

Csizmazia-Darab István, IT biztonsági szakértő
a NOD32 antivírus termékek magyarországi képviselete
antivirus.blog.hu

Címkék: Csizmazia_István, it-biztonság, fenyegetés, védelem

SHARE Továbbküldés Nyomtatás

Korábbi írások