Ali baba és a negyvenezer adatrabló

2013.03.14. csütörtök

A biztonság vagy annak illúziója nem létezhet a védekezésre kifejlesztett programok nélkül – ennyit már szinte minden számítógép-felhasználó tud, a többség telepít is valamilyen vírusirtót, internetbiztonsági csomagot és egyéb védelmi alkalmazást. Ám az, hogy elkerülhessük a fertőzéseket, az adatszivárgást, a banki adataink elleni adathalász akciókat, szükség van emellett a megfelelő hozzáállásra is, úgynevezett biztonságtudatos szokások kialakítására.

Ilyen például a titkosított https kapcsolat preferálása, a telepítendő alkalmazások előzetes alapos kiválasztása, a kéretlenül kapott üzenetek és linkek higgadt hárítása, ígérjenek azok csaliként bármilyen szenzációs, erotikus vagy jól jövedelmezőnek látszó tartalmat.

Nem szerepelt a fenti felsorolásban az egyik legfontosabb összetevő, ami nem más, mint a "megfelelő" jelszó. Hogy pontosan mit is értünk megfelelő alatt, azt már sokszor és sokan összefoglalták, frappánsan most azt mondhatjuk: kellően hosszú, azaz legalább 8-10 karakter, vegyesen tartalmaz kis- és nagybetűket, számokat, valamint egyéb írásjeleket is. Tipikus hiba, ha valaki olyan gyenge jelszót vagy jelszó emlékeztető kérdést választ, ami nem véd megfelelően – ilyen például az „abc”, vagy „1234”. Nem javasolt saját vagy családtag, házikedvenc neve, születési évszáma, magyarán minden olyan adat, amely az illetőt ismerve, rákeresve a neten, a közösségi oldalakon bárki számára könnyen azonosítható vagy egyszerűen kitalálható. Hogy aztán a szintaktikailag már szépen megkonstruált "megfelelő" jelszavunk be is töltse a neki szánt szerepet, azaz sikeresen védelmezze belépésünket az illetéktelenek elől, ahhoz tartoznak még további hasznos szabályok, amiket sajnos sokan elhanyagolnak, megkerülnek, figyelmen kívül hagynak, és ezzel aztán a kezdeti, egyébként jó és biztató kiindulást elrontják.

Az egyik ilyen "best practice", hogy a jelszó minden egyes helyszínen egyedi és különböző legyen. A rövid emlékezet, vagy a kényelem sem adhat felmentést arra, hogy valaki az e-mail-fiókjától kezdve a Facebook elérésén át a weboldala admin jelszaváig mindenhol egy és ugyanazt a jelszót használja. Bevett gyakorlat ugyanis, hogy ha bármely helyszínen adathalász támadás áldozata leszünk – vagy az adott szolgáltatás szervereit feltörve jelszavakat lopnak, lásd LinkedIn – a támadók az összes lehetséges helyszínen végigpróbálgatják a megszerzett accountot, hátha szerencséjük lesz, és sajnos sokszor ez így is történik.

A másik fontos szabály pedig az, hogy a saját személyes jelszavunkat soha ne osszuk meg másokkal. Ahogy a "Szezám, tárulj fel!" szavakra bárkinek feltárul a mesebeli kincses barlang, ugyanúgy tárva-nyitva állnak ilyenkor állományaink, leveleink, beállításaink mások előtt. A jelszavunk a mi belépésünket szolgálja, azt ne használjuk közösen senkivel, ne adjuk oda szívességből másnak – ez utóbbi sajnos gyakran előforduló hiba munkahelyi környezetben, ahol sokan megengedik, hogy a másik az ő bejelentkezésünket használva intézze ajajaj de sürgős tennivalóját. De ne legyünk hanyagok se, és ne ragasszuk a jelszavunkat postitre a monitor szélén, sőt még arra is figyeljünk, nehogy begépeléskor valaki a hátunk mögül orvul kifigyelhesse. Emellett arra is kell vigyázni, hogy nyitott wifin, publikus hotspoton, netkávézóban ne lépjünk be azonosítást kérő oldalainkra, és természetesen banki ügyeinket sem szabad innen intézni, hiszen akár a közösen használt gépekre kémprogramot telepítő ügyeskedőnek, akár a közönség között észrevétlenül megbúvó FireSheep böngészőkiegészítőt futtatónak tálcán kínáljuk ezzel bizalmas adatainkat.

Végül érdemes megemlíteni a jelszó cserét is, amelyre sokan csak úgy gondolnak, hogy az vagy a munkahelyi rendszergazda bosszúja emlékezőtehetségünk megtornáztatására, vagy pedig csak akkor kell ehhez folyamodni, ha már feltörték valamilyen elérésünket. Ám igazság szerint már a puszta gyanú esetén is érdemes elvégezni ezt a műveletet, emellett ahol lehet, ott érdemes igénybe venni a kétfaktoros azonosítási lehetőséget is. Ez utóbbi különben akkor ér valamit, ha fizikailag két különböző készüléket használunk hozzá. Azaz ha valaki az okostelefonjáról bankol és ugyanarra kapja a mobilaláírás sms-t is, az kevésbé számít biztonságosnak, mintha egy külön pc-ről történik a banki belépés, és külön a telefonra érkezik a tranzakciót megerősítő egyedi kód. Ha nincs szabályozva, a jelszó cserének egyébként érdemes valamilyen rendszeres időperiódust kiválasztani, ami lehet két hónap, negyedév, félév, stb. és ennek leteltével mindenfajta biztonsági incidens nélkül is javasolt egy olyan újat választani, ami a régebbi ismeretében nem található ki. A gondosan kiválasztott, óvatosan használt és rendszeresen változtatott jelszó egy olyan pillér, amelyet egyetlen biztonságtudatos felhasználó sem nélkülözhet, ha távol akarja tartani kincseitől az adatrablókat.

IT Business Online