Ha odavész az okostelefon

2013.09.05. csütörtök

Az okosmobilok széleskörű elterjedése a lopások számának drasztikus növekedésével is együtt járt. Áttekintjük, mik lehetnek ilyenkor a károk, mivel készülhetünk fel, hogyan vigyázzunk.

A National Policy Agency adatai alapján a bejelentett okostelefon lopások a korábbi 2009-es 5575-ről 2012-re már 31 ezerre nőtt Dél-Koreában. Teljes körű adataink nincsenek, de a dél-koreai adatokban bekövetkezett változás gyaníthatóan világszerte mindenhol hasonló mértékű lehet.

Ha kategorizálni szeretnénk, az okostelefon lopások három nagy területen okoznak kárt. Az első ugye a készülék, vagyis a hardver eltűnése. Ha profik viszik el, akkor viszonylag kevés az esély. Ugyanis döntő többségben nem egy konkrét kiszemelt célpont személy telefonja, vagy adata kell nekik, hanem csak maga a készülék, amiből kikapcsolás után azonnal kiveszik a SIM kártyát, és egy rendszer-visszaállító hardver reset után mehet is a használt cikkes piacok polcaira.

Ha kevésbé profik, vagy alkalom szülte tolvajokról van szó, akkor jobbak az esélyeink. Átlagos eltulajdonításnál egy lopásgátló, távtörlő program különösen Androidon hasznos lehet. A különféle mobil biztonsági csomagok különféle szolgáltatásokat kínálnak, illetve az ingyenes verziók és a fizetős változatok tudásában is vannak különbségek, ezért érdemes ezeket a kiválasztás és telepítés előtt alaposan áttanulmányozni. És még mindig a vasnál, azaz hardvernél maradva a lopásnál járulékos kárt jelent még a memória bővítő kártya, különösen ha méretesebb, sok gigásról van szó.

A profi tolvajok mellett a másik véglet, amikor nevetséges hibákat is elkövetnek, például a belépett Facebook fiókba online posztolnak magukról fotókat. Ezekről időnként szép csokrot lehet olvasni a bulvár hírekben, például egy Ibizán meglovasított okostelefon, melyet a Dubaiban élő Hafid nevű tolvaj lopott el, ám azt nem tudta, hogy az azóta a mobiltelefonnal készített összes fotót és videót a készülék automatikusan feltölti az internetre. A károsult bosszúból vicces módon blogot vezet a tolvaj azóta eltelt hétköznapjairól valóságshowként illusztrálva, hogy az éppen merre jár, mit csinál, mit fényképez.

Az első kategóriát kivéve van valamennyi esély rá, hogy egy lopásgátló működhessen, és esetleg megtaláljuk. Az emberrablási esetekhez hasonlóan azonban itt is van egy kezdeti időtartam, amíg az esélyek magasak, ám 24/48 óra elteltével, illetve ennél is később már gyakorlatilag lemondhatunk a készülékről. A témához tartozik még, hogy sajnálatos módon az elhagyott és megtalált készülékeket sem adják vissza többnyire a tulajdonosoknak, hanem felkutatás vagy talált tárgyként való leadás helyett megtartják, eladják. Ha a szolgáltatónál letiltatjuk a kártyát, akkor a tolvaj csak másikkal tudja használni. Sajnos a hardver visszaállítás a SIM kártya cserét sem fogja onnantól észrevenni. Ha pedig letiltatjuk az IMEI számot is, akkor elvileg egyik magyar szolgáltató – Telenor, T-Mobile, Vodafon – kártyájával sem fog működni, igaz ennek átállítása technikailag nem megoldhatatlan feladat. Illetve emellett külföldre még simán kivihetik a készüléket, mert ott már nem él a tiltás.

Jöjjön akkor a hardver után a második terület, hogy személyes adatokat tároltunk rajta, és ezek nincsenek most meg nálunk, mert a készülékkel együtt elvesztek. Erre megoldást csak a rendszeres backup, azaz mentés adhat, 1-2 havonta érdemes ilyet csinálni, és azt egy külön adathordozón őrizni. Ebben az esetben csak az utolsó mentéshez képesti új bejegyzések veszhetnek el, nem pedig minden. Az újabb, KitKat névre hallgató 4.4-es Android verzió már az adatmentés területén is igyekszik állítólag újítást bevezetni, ez pedig a TheCloud nevű feature lesz majd. Itt megint csak színesíti a képet, ha külső adathordozó – jellemzően mikro SD bővítőkártya – is volt a telefonban. Ilyenkor az ezen szereplő adatokat is bukjuk, illetve tartalma szabad préda lesz.

És végül a harmadik szempont, amikor ezeket a bizalmas adatokat, esetleg BYOD-tól sújtott céges

információkat nem akarjuk, hogy illetéktelen kezekbe kerüljenek. Itt újra képbe jön a korábban emlegetett biztonsági program, és a távlezárás, illetve távtörlés. Természetesen van ennek az egésznek egy táncrendje, hogy a lépéseket milyen sorrendben érdemes csinálni, például amíg vadászunk a lopott készülék GPS helyzetére, addig nem célszerű letiltani a telefonkártyát, ám persze túl sokáig sem szabad ezzel várni, különösen amennyiben az adat nagyságrendekkel fontosabb és értékesebb a készüléknél. Érdemes ilyenkor kicsit belegondolni abba is, hogy egy noteszgép esetében milyen egyszerűen és sokféle eszközzel – TrueCrypt, CryptKeeper, EncFS, Bitlocker, stb. – megtehetjük adataink titkosított kezelését, tárolását, és mennyire korlátozottak, nehézkesek ugyanezek megvalósítása az okostelefonokon. És ennek ellenére a nyilvánosságra került elvesztett és ellopott noteszgépek esetében – legyen az egészségügyi adatokat tartalmazó kórházi, vagy éppen az MI6 tulajdonában lévő gép – sajnos még mindig nem élnek elegen a titkosítással.

Így azzal zárunk, hogy a biztonságot sokféleképpen el lehet ugyan képzelni, de ezek között érdemes úgy is, mint egy mérleget: kell tennünk az egyik serpenyőjébe valamit ahhoz, hogy aztán kaphassunk a másikba.

IT Business Online