Mikel Olasagasti
Sistema administraria

Kutxak

Aurrekoan kexuka etorri zitzaidan lagun bat; mugikorrean hilero duen konexio azkarreko muga nonbait laster amaitzen zaiola zioen haserre. Mugikorrak berak ematen dituen datuetan oinarrituta Dropbox eta Google+ zerbitzuek datu pila mugitzen zituztela ikus zitekeen. Erabiltzen ote zituen galdetutakoan ezetz esan zidanez, erraza zen nondik jo. Selfie, paisaia eta katuari argazki mordoa ateratzen dizkio eta argazki horiek automatikoki aipatutako bi zerbitzuetara igotzen zaizkio. Normalean WiFi bidez bakarrik egiten da, baina, bai edo ez galderaren aurrean, erabiltzaileen erdiek baiezkoa eta besteek ezezkoa sakatzen dute, askok zer dioen irakurri gabe. Ondorioz, gerta daiteke argazkiak WiFi gabe ere igotzeko aukera aktibatuta edukitzea.

Misterioa argituta, pentsakor jarri zen. Zertarako gordetzen zaizkit argazkiak bi aldiz? Izatez, ez da ideia txarra. Gure argazki zein dokumentuak gure mugikorraren almazenamendua baino zerbait «ziurrago» batean gordetzeak askotan mesede egin dezake, terminala apurtu edo galtzen bada adibidez. Baina kanpoko eraso modura planteatu dezakegu.

Google+ eta Drive, iCloud, Dropbox eta beste hainbat zerbitzuk gure fitxategiak sinkronizatzeko balio dute. Mugikorretan instalatzen direnean hainbat eskubide lortu nahi dituzte, hala nola, sortzen diren fitxategi eta argazki guztiak euren eskuetatik pasatzea. Euren zerbitzua publikoa denez, eraso egingo dietela pentsatzea eta horren beldur izatea ez da arraroa.

Bi modu daude eraso egiteko. Lehenengoa lan teknikoa litzateke, segurtasun arazo bat topatuz edo indarrez sartzen saiatzea, eta bestea gehiago da ikertzaile lana. Norbaiten galdera ezkutua edo pasahitza maskotaren izena edo jaiotze herria badira, edota plataforma guztietan pasahitz bera erabiltzeko ohitura izanez gero, denbora kontua izan daiteke norbait nahi ez den eduki pertsonaletara sartzea. Pertsona "anonimoen" kasuan horrelako erasoak ingurutik datoz, baina pertsonaia publiko baten atzetik edonor ibili daiteke.

Famatu edo ospetsuak beti daude eraso horien jomugan, izan xantaia bitarteko edo nolabait min egiteko asmoz. Horren adibide da abuztu bukaeran gertatutako "Celebgate" izeneko "filtrazioa", ehundik gora pertsonaia ezagunen argazki pribatuak publikatu zirena. Jabeen kontrolpetik at dauden argazki gehiago omen daude publikatzeko zain, baina, kaleratu bitartean, ezin horrelakorik konfirmatu.

Kaltetuen zerrenda luzetik batzuek ezeztatu egin dute eurenak direla, beste batzuek ez dute onartu, eta tartean argazkiak ateratako garaian adin txikikoak zirela esan duenik ere aurkitu daiteke. Kezkagarria irudiak ezabatuta zituenaren aitzakiak irakurtzea izan da. Irudiak ezabatuta badaude, orduan horiek lortzeko hainbat aukera egon daitezkeela dirudi. Alde batetik, zerbitzu horietako pasahitzak aspalditik jakitea. Bestetik, zuzenean argazkietako pertsonaiaren kontuetara sartu beharrean, datu horiek jaso zituztenen kontuetara sartu direla. Eta, azkenik, arazoa benetan zerbitzu horietakoren bateko segurtasun zuloren bat bada, horrek esan nahi du ezabatutakoak ez direla benetan ezabatzen.

Zerbitzu horien aukera libre eta printzipioz ziurrak eskuragarri daude, baina mundu guztia ez da konturatzen zenbateraino kontrolatzen gaituzten eta zenbateraino gauden publikora zabalik. OwnCloud bezalako harribitxiak instalatzea ez da zaila baina denbora behar du. Errazena, tarteka pasahitzak aldatzea da. Galdera ezkutuen erantzunak nonbait gorde eta datu faltsuak ematea. Eta, azkenik, izan beti gogoan sekretu bat salbu mantentzeko onena frogarik ez uztea dela. •

Telefono mugikorren erabateko segurtasuna ziurtatzea ez da erraza. GAUR8