Rosa Arruabarrena Santos
EHUko Donostiako Informatika Fakultateko irakaslea eta ikertzailea

Neurriak hartu eta zure kontu digitalak babestu

Internetek eta teknologiek Covid-19aren ondorioz izan dugun konfinamendua jasateko laguntza eskaini digute, eta, bat baino gehiago, enpresa edo gizabanako gisa, telelana egitera ere behartu gaituzte, orain arte imajinaezinak ziren aplikazio ugari ikastera eta erabiltzera, «online» izapideak egitera, adin-tarte guztietan aisialdi telematikoa eragitera, eta abar luze batera. Aplikazio horiek erabiliz era guztietako gailuetatik eta, hedaduraz, sare-zerbitzu ugaritatik, egun, gure datuek ihes egiten digute, harea-pikor gisa. Eta, ondorioz, gure kontu digitalak besteen gauzak maite dituztenen jomuga bihurtu dira.

Egungo egoerak segurtasun-gertaeren areagotzea islatzen duenean, aitortu behar da erabat segurua den sistemarik ez dagoela. Horregatik, enpresek ez ezik, erakundeek eta gizabanakoek ere neurriak hartu behar ditugu gure kontu digitalak babesteko. Eman beharreko lehen erantzuna, erraza izan arren, zaila da ezartzen; izan ere, erabiltzaileen alfabetatze digitala eskatzen du, pasahitz-sendoen erabileran eta zenbait urrats egiaztatzen dituzten kautotze-sistemetan heztea. Artikulu honetan jorratuko ditugu gaiok.

Pasahitz gogorrak erabiltzea da gure web profiletara edo kontuetara sartzean hartu behar den lehen neurria, sistemak hala eskatu ala ez. Horrela, pasahitz bat gogorra (edo segurua) dela esaten da luzera handia duenean eta sinboloak, hizki larriak, xeheak eta zenbakiak barnebiltzen dituenean. Pasahitz seguruak sortzeko eta gogoratzeko metodo erraz bat norberarentzat garrantzitsua den esaldi baten bidez lortzea da, esaldiko hitzen hasierak erabiliz; adibidez, “LIzar GAixo DAgo, 09:00etan MEdikuarengana JOan, RAmon” esaldiak “Ligada.09mejora” pasahitza osatuko luke. Esan beharrik ez dago erabiltzen diren zerbitzuetan pasahitz desberdinak erabili behar direla, eta, behar izanez gero, KeePass bezalako aplikazioak erabili behar direla modu seguruan horiek gordetzeko.

Hala ere, urrats hori ez da nahikoa, eta jada kautotze-sistema askok euren zerbitzuetara atzitu aurretiko identifikazio-urratsak bikoiztu edo hirukoiztu dituzte, haratago joanez hirugarrenei sarbidea oztopatuz.

Oro har, faktore anitzeko autentifikazioa sarbide informatikoko kautotze edo kontrol metodo bat da, eta erabiltzaileak bi ebidentzia edo gehiago behar bezala aurkeztu ondoren soilik du sarbidea baimenduta. Ebidentziok hainbat printzipio edo faktoretan oinarritzen dira: *ezagutza* (erabiltzaileak bakarrik ezagutzen duen zerbait, pasahitza bezala), *jabetza* (erabiltzaileak duen zerbait, telefonoa kasu) eta *berezkoa* (erabiltzailearen datu biometrikoren bat, hatz-marka adibidez). Eta, zehazki, alegatutako identitatea bi faktore desberdinen konbinazioaren bidez baieztatzen denean, bi faktoreren kautotzea (2FA) edo bi urratseko egiaztapen-sistema erabiltzen dela esaten da. Adibidez, kutxazain automatikoetan erabiltzen den sistema da, txartela (*jabetza*) eta PINa (*ezagutza*) baitira beharrezkoak.

Kontu digitalak mehatxatzen dituzten arriskuak direla eta, «online» mundurako 2FA sistema batzuk garatu dira. Lehen faktorea ohiko pasahitza da, edozein kontutarako estandarra dena. Eta beste faktore desberdin batekin osatzen dute sarbidea; faktore hori *smartphone*, konputagailu edo beste gailu bateko aplikazio batetik berreskuratutako egiaztapen-kodea da. Ugaritzen doaz bigarren faktore gisa datu biometrikoak erabiltzen dituzten aplikazioak/gailuak (hatz-marka, begiaren irisa, aurpegiaren azterketa eta iritsiko diren beste asko). Adibidez, *online* bankuek bezeroak euren kontuetara sartzeko 2FA sistemak erabiltzen dituzte batez ere. Halaber, 2FA sistemetarako beste izen batzuk OTP (erabilera bakarreko pasahitza) eta TOTP (denboramuga duen erabilera bakarreko pasahitz-algoritmoa) dira.

Orain gure gailu eta aplikazioekin hobeto moldatzen dakigunez, eta Interneten sortzen diren arriskuez jabetuta, jarri abian defentsa teknikok, eta ez eman behar baino datu gehiago! •

Zenbait defentsa teknika erabili beharra dago Interneten sortzen diren arriskuak saihesteko.