

Zibersegurtasuna: Beste ikuspuntu bat (1/3)

Zibersegurtasunari dagokionez, bizitzaren beste alderdi batzuetan bezala, zuzenean eragiten diguten gauzetan pentsatzen dugu beti, informatikan eta telekomunikazioetan; zehazki, gure hardwarearen barne-segurtasunari dagokionez, bai PCetan, bai mugikorretan, baina guk ezertxo ere kontrolatzen ez dugun guztia alde batera uzten da. Horretarako, oso argi izan behar dugu non gauden eta zergatik egin daitekeen azken bezero gisa egiten dugun guztia.

Gu komunikatzen gara “Sare Handi” bat dagoelako, INTERNET ospetsua ez dena, “batzuk besteekin” eta, batzuetan, “batzuk besteen kontra” konektatzen gaituena.

“Elementu” hori ez dugu ezertxo ere kontrolatzen, hau da, INTERNETEN barruan INTERNETEN dabilen guztia kontrola daiteke, baina sare horrek, INTERNETek, “Sare Handiko” baliabideak erabiltzen ditu, eta pentsa liteke “Sare Handia” gabe INTERNET ezer ez dela, baina INTERNET gabe “Sare Handia” dena dela.

“Elementu” horrek gutxitan pentsatu ditugun eta hor dauden ezaugarri batzuk ditu, eta horien bidez lortzen dugu “batzuk besteekin” eta “batzuk besteen kontra” konektatzea, eta horiek dira gure komunikazioetan eragin handia dutenak, haiek gabe ez bailuke ezer funtzionatuko.

“Sare Handiaren” barruko egiturak bilakaera handia izan du; hardware izatetik hardware eta software konbinazio izatera pasatu da, eta horrek dakar guztiaren kontrola lehen hardwareari lotuta zegoela eta orain guztia “Sare Handiaren” softwarean zentralizatuta dagoela, hardwarerik gabe ez duela ezertxo ere funtzionatzen ahaztu gabe.



“Globalizazioa” lortu duena software horren aurrerapen teknologikoa da. Izan ere, dagoeneko ez dago eraikin/lokal/eskualde/nazio/estatu bakoitzaren sare berean egon beharrik mugikor bat edo PC bat eskuratu ahal izateko planetako beste puntuan; hori guztia, telekomunikazioen “Globalizazio” horri esker, dagoeneko ez dago eraikin/lokal/eskualde/herrialde/nazio/estatu/estaturik.

Hardwarea edo “sarearen zati fisikoa” gure inguruko “sarbide-puntu” ugarik osatzen dute. Horren ondorioz, “sarbide-puntu” bakoitzean ahultasuna dago, eta, aspaldi, “sarbide-puntu” horiek fisikoki definituta egon behar zuten sarearen “zati fisikoaren” barruan. Hori esan ohi zen sarean “entzutea”, eta fisikoki “entzundakotik” hurbil egin behar zen; baina, orain, zati “fisiko” hori hainbestearaino garatu da, ezen, planetaren beste aldean egonda ere, “entzundakorako” sarbidea ematen duen sareko “zati fisikorako” “sarbide-puntu” bat aurkitzea lortzen duzun arren, hori guztia gero eta handiagoa den “sareen arteko konexioarekin” lortzen da, hori guztia ezinbestekoa baita guztiaren funtzionamendu onerako.

“Sareen arteko konexioa” oinarrizko 2 elementuren bidez egiten da, hala nola sateliteen bidez eta sare finkorako sarbidearen bidez, bai zuntz optikoaren bidez, bai hari gabeko sistemen bidez, bai WiFi, Radio, WIMAX, 5G, 4G, 3G, 2G eta abarren bidez.



Horregatik, operadore baten azken bezeroa izateak eta zure hardwarean segurtasun-software aurreratua erabiltzeak ez du esan nahi segurtasun-maila optimoa aurkitu duzunik; izan ere, zuk, azken bezero gisa, zure operadoreak zure softwareak funtziona dezan eskatzen dizkizun baldintza guztiak bete behar dituzu, eta operadoreak gainerako operadoreek haiekin “interkonektatuta” egoteko eta, hala, “Sare Handia” osatzeko eskatzen dizkioten baldintzak bete behar ditu.

Ohar hori hurrengo “pilulan” kontatuko dut; asko hitz egiten da “TOR” sareaz (The Onion Router); baina hori guztia ondo dago, baina korrika doa, “Sare Handian” dabil INTERNET protokoloekin... Gero, atzeman, bortxatu, barneratu eta manipulatu egin daiteke, bai maila fisikoan, bai berariazko hardware baten bidez.

Zibersegurtasuna: Beste ikuspuntu bat (1/3)

Zibersegurtasuna: Tokiko ikuspegia (2/3)

Zibersegurtasuna: Munduko geopolitika (3/3)

Pablo Martín Galiana