

Mis on tegelikult VPN

See muudab seda, kes sind näeb, mitte seda, kas keegi näeb.

Lihtsalt seletades: VPN ei lase sinu internetipakkujal ega lennujaama Wi-Fi-l näha, kuhu sa ühendud. See teave ei kao kuskile: see läheb VPN-i ettevõttele, kes seda nüüd näeb. See, mis liikus juba krüpteeritult, nagu e-post või pank, oli krüpteeritud ka varem. See täidab mõnda kindlat eesmärki ja seda müüakse sageli nii, nagu lahendaks see palju enamat.

Aastaid kuulsin VPN-idest ega teinud neist välja, täpselt nagu viirusetõrjest: ma ei kasuta viirusetõrjet või peaaegu mitte kunagi. Mul on kõigest reaalajas koopiad kolmes kohas ja olen väga ettevaatlik sellega, mida alla laadin, millistel linkidel klõpsan ja milliseid veebisaite külastan. See pole sajabrotsendiline turvalisus, aga see toimib minu jaoks. Ühel päeval nägin VPN-i pakkumist veidi enam kui kahe euro eest kuus ja tellisin selle uudishimust. See töötab hästi, kuid sellest on olnud mulle vähe kasu: näiteks selleks, et proovida teenust, mis avanes tol ajal ainult Ameerika Ühendriikides. Kas ma tunnen end turvalisemalt? Ei. Kui nad pakuvad mulle seda uuesti selle hinnaga, siis võib-olla pikendan; kui ei, siis mitte. See on vaid minu kogemus, see ei tõesta midagi. Nii küsisin endalt, mida VPN täpselt teeb. Nii olen mina sellest aru saanud.

Kujuta ette, et postitad kirja postkasti nii, et saaja aadress on selgelt nähtav. Kirjakandja näeb, kellele sa selle saadad, kuigi ta ei saa seda lugeda, kui see on suletud. See kirjakandja on sinu internetipakkuja. VPN paneb sinu kirja teise ümbriku sisse, mis on adresseeritud vahendajale, kes selle avab ja edasi saadab. Sinu tavaline kirjakandja ei näe enam tegelikku aadressi. Ta näeb vaid, et kirjutad sellele vahendajale.

See, kes kontrollib võrku, kust sa ühenduse lood – näiteks lennujaama Wi-Fi –, ei näe enam, kuhu sa lähed. Kuid vahendaja näeb nüüd seda, mida varem nägi sinu operaator, ja mõnikord rohkemgi, sest kogu sinu liiklus käib tema kaudu. Järelevalve ei kao: see vahetab omanikku. Sellest ka nimi.

Lisaks liigub peaaegu kõik, mida sa täna teed – näiteks meili avamine või panka sisenemine –, brauseri tabaluku tõttu juba sihtserverini krüpteeritult. See toimub nii VPN-iga kui ka ilma selleta. VPN lisab kaitse ainult esimesel lõigul, kuni oma serverini. Seal edasi on tee endine.

Seepärast on asju, mida see ei saa sulle lubada, kuigi seda mõnikord nii reklaamitakse. Kui oled oma meili või panka sisse loginud, teab see teenus, et see oled sina, koos VPN-iga või ilma. Samuti ei taga see, et keegi sinu liiklust ei vaataks: see muudab ainult seda, kes vaatab. Kui ettevõtte ütleb, et ta «ei pea logisid», on see lubadus, täpselt nagu siis, kui suur platvorm ütleb «teie sõnumid on krüpteeritud, me ei loe neid». Audit võib seda konkreetsel hetkel toetada, kuid see jääb millekski, mille täitmist sa usaldad, mitte millekski, mida ei saaks ülesehituse tõttu rikkuda.

Ja vestluse sisu jääb samaks. Kui sinu sõnumirakendus juba krüpteerib otsast lõpuni, ei lisa VPN midagi. Kui ta seda ei tee, ei paranda seda ka VPN: see kaitseb sõnumi teekonda, mitte seda, mida rakendus või selle server sellega kohale jõudes teeb.

Mitte miski sellest ei tee seda kasutuks. Varjata seda, kuhu sa ühendud, avaliku Wi-Fi eest, operaatori eest, kes tahaks seda ajalugu müüa, või riigi eest, mis teenuse blokeerib, on tõeline töö ja see teeb seda hästi. Turundus lubab aga reeglina rohkem, kui see kiht anda suudab.

Küsimus, mida tuleks endale esitada VPN-i või mis tahes kaitset lubava teenuse puhul, ei ole «kas see on krüpteeritud?». Tõenäoliselt jah, vähemalt ühel lõigul. See on hoopis see teine: kellele ma usaldan selle usalduse, mille olen teiselt ära võtnud? Ja mis mulle jääb, kui see osutub põhjendamatuks?

VPN, kui see teeb oma tööd hästi, muudab ainult seda, kes on sinu ühenduse vahendaja. Selline rakendus nagu Solo2, mille sõnumid ei läbi ühtegi serverit, eemaldab vahendaja vestlusest täielikult. Nad ei võistle omavahel: nad lahendavad eri probleeme.

Nende omavahel segiajamine on väga tavaline viis pidada end kaitstumaks, kui tegelikult ollakse.

Toimetaja märkus: Kui need Cuadernos nimetavad ettevõtteid või tooteid, ei ole see süüdistamiseks. Nende loojad teevad tööd, mida miljonid inimesed kasutavad ja hindavad. See, millele me osutame, on struktuurne — mudel, mitte bränd. Brände kasutatakse näidetena, sest lugeja tunneb need ära.

Allikad ja täiendav lugemine

- HTTPS-protokoll ja transpordi krüpteerimine on avatud standardid, mida IETF on avalikult dokumenteerinud.
- Samas kogumikus: «Kui kedagi ei ole vahel» ja «Sa ei ole anonüümne» avavad teistest vaatenurkadest sama eristust struktuuri ja lubaduse vahel.

[← Eelmine](#)[Sa ei ole anonüümne](#)

Viimased lugemised

- [Mõtisklus · 29. juuni 2026 Sa ei ole anonüümne](#)
- [Refleksioon · 27. mai 2026 Mida allkiri ei saa parandada](#)
- [Analüüs · 26. mai 2026 Tõeline vs näiline privaatsus: küsimused, mida tasub endalt küsida](#)

Võtke see artikkel endaga kaasa kuhu iganes vaja.

[↓ Markdown](#) [↓ Lihttekst](#) [↓ PDF](#)

Fail laaditakse alla sinu seadmesse. Sealt saad selle salvestada, importida Solo2-sse või jagada kus iganes soovid. Cuadernos ei otsusta sihtkohta sinu eest.

Lakipitsat · SHA-256 a925c8316391cb772374fa34165177ffc994fa5cdb825b667971b1d93917e57f

[Funktsioonid](#) [Hinnad](#) [Paigalda](#) [Uudised](#) [Blogi](#) [Pro](#) [Abi](#) [Meist](#) [Kontakt](#)
[Läbipaistvus](#) [Kontroll](#) [Privaatsus](#) [Tingimused](#) [Küpsised](#)

Cuadernos Lacre · Ettevõtte [Menzuri Gestión S.L.](#) väljaanne ·
kirjutanud R.Eugenio · toimetanud [Solo2](#) meeskond.

See veebileht ei kasuta küpsiseid. Kõik, mida sinu brauser laadib, on meie kirjutatud või meie järelevalve all ja paikneb meie Euroopa serverites: anonüümne külastuste loendur (Umami, ise majutatud) ja minimaalne vajalik JavaScript keelevaliku ning hele või tume teema eelistuse jaoks, mis salvestatakse sinu enda seadmesse. Ei mingeid väliste ettevõtete ressursse, ei mingeid jälitajaid, ei mingit profiilianalüüsi, ei mingit andmete jagamist. Kui soovid meid jälgida: [RSS](#).