Erdian inor ez dagoenean

Zerbitzari batetik pasatzen dena enkriptatzeak edukia babesten du. Erdian zerbitzaririk ez izateak galdera ezabatzen du. Ez dira gauza bera.

Bi pertsona, elkarrizketa bat

Bi pertsona gela batean aurrez aurre hitz egiten ari direnean, inork ez du agindu beharrik ez duela ezer entzun. Ez zuen entzun egon ez zelako. Bi pertsona paper bat eskutik eskura pasatzen ari direnean, erdian dagoen inork ez du zin egin beharrik ez duela irakurri. Ez dago inor erdian.

Eguneroko bizitzako gauza gehienak horrela funtzionatzen dute. Ez dugu konfidentzialtasun-akordiorik sinatzen gure ahotsa transmititzen duen airearekin, ezta eskuan dugun paperarekin ere. Elkarrizketaren pribatutasuna ez dago bitartekari baten promesan oinarrituta, ez dagoelako bitartekaririk. Hori da pribatua izateko modurik indartsuenetako bat: ez zerbait edo norbait ondo portatzen delako, baizik eta zerbait edo norbait ez dagoelako.

Elkarrizketa kanal digital batera pasatzen denean, hori aldatu egiten da defektuz. Eredu arrunta honako hau da: bi pertsona zerbitzari batera konektatzen dira, zerbitzariak mezua jaso, enkriptatu edo enkriptatuta gorde, eta hartzaileari ematen dio. Zerbitzaria erdian dago. Zerbitzaria zintzoa izan daiteke. Auditatua egon daiteke. Jurisdikzio aldeko batean eta pribatutasun-politika zorrotz baten pean lan egin dezake. Hori guztia egia izan daiteke. Baina zerbitzaria erdian dago.

Enkriptatzearen eta ez jasotzearen arteko aldea (bigarren zatia)

Serie honetako aurreko artikulu batean defendatu genuen edukia enkriptatzea eta metadatuak ez jasotzea ez direla gauza bera. Badago urrats bat harago, argi eta garbi formulatzea komeni dena: zerbitzari batetik igarotzen dena enkriptatzea eta zerbitzaririk ez izatea ere ez dira gauza bera.

Lehenengo ereduak —zerbitzaria erdian, edukia enkriptatua— zerbitzariaren operadorearengandik, mantentze-lanetako langileengandik edo sistema arriskuan jartzen duen kanpoko erasotzaile batengandik babesten du edukia. Eta hori garrantzitsua da. Baina ez du zerbitzaria ezabatzen. Zerbitzariak hor jarraitzen du. Metadatuak prozesatzen jarraitzen du. Eskari judizial bat, esku-hartze legal bat, presio politiko bat edo segurtasun-haustura bat jaso dezakeen puntua izaten jarraitzen du. Norbaitengan konfiantza izatea eskatzen duen puntua izaten jarraitzen du.

Bigarren ereduak —no haber servidor entre los dos extremos— ez du edukia hobeto babesten: kriptografia sendoa bada, edukia babestuta doa bi kasuetan. Aldatzen dena ez da edukia. Aldatzen dena da *«zer gertatzen da zerbitzariarekin?»* galderak zentzua galtzen duela, galdetzeko zerbitzaririk ez dagoelako.

Konfiantza, gabezia, eta bien arteko aldea

Konfiantza ondo kokatuta egon daiteke. Enpresa zintzoak badaude. Auditore zorrotzak badaude. Erabiltzailearen aldeko legediak badaude. Aurreko guztia zorrotz betetzen duten zerbitzu serioak badaude. Konfiantza, merezi

duen operadore bati ematen zaionean, ez da konponbide txarra.

Baina konfiantza, sendoa izan arren, konfiantza izaten jarraitzen du. Konponbide soziala da, ez konponbide teknikoa. Enpresa bat jabe bidez alda daiteke. Jurisdikzio batek gobernuz alda dezake. Agindu judizial bat bihar iritsi daiteke. Ahultasun berri bat datorren hilean aurki daiteke. Horietako bat ere ez da fede txarragatik gertatzen. Operadorea existitzen delako gertatzen da, eta existitzen den guztia munduko kontingentzien mende dago.

Operadore baten gabeziak ez ditu kontingentzia horiek. Agindu judizial batek ezin dio daturik eskatu existitzen ez den zerbitzari bati. Erasotzaile batek ezin du existitzen ez den zerbitzari bat arriskuan jarri. Enpresa baten politikaren aldaketa batek ezin die eragin enpresa horrek inoiz izan ez zituen datuei. Esaldi nagusia erraza da: existitzen ez diren datuak ezin dira galdu.

Zerbitzariaren aldeko argumentu zilegiari buruz

Erdian zerbitzaria duen mezularitza-zerbitzu profesional bat eskaintzen duenak hiru argumentu guztiz baliozko erabili ohi ditu. Lehenengoa, zerbitzaria hartzailea deskonektatuta dagoenean entrega bermatzeko beharrezkoa dela. Bigarrena, edukiaren enkriptatzea sendoa dela eta, beraz, operadoreak ezin duela irakurri. Hirugarrena, zerbitzuak Europako legedia betetzen duela eta datuak legeak babestuta daudela.

Hiru argumentuak egiazkoak dira. Batek ere ez du gaiaren natura aldatzen. Egia da zerbitzari batek mezuak entrega geroraturako gordetzea ahalbidetzen duela; egia da, halaber, entrega geroratua beste modu batera konpon daitekeela, gailuen arteko komunikazio zuzeneko protokoloen bidez, hamarkadetan finduak eta gaur egun operatibo daudenak. Egia da igarotzean edukia enkriptatzea sendoa dela zerbitzu serioetan. Eta egia da Europako legediak erabiltzaileak beste toki askotakoak baino gehiago babesten dituela.

Kontua ez da erdian zerbitzaria duten zerbitzuak legalak diren, ezta seguruak diren edo edukia babesten duten ere. Izan daitezke, legalak dira, eta seguruak izaten dira. Kontua da erdian zerbitzari bat izatea hautu arkitektonikoa dela, ez inposizio teknikoa. Eta hautu bakoitzak ondorioak ditu. Erdian zerbitzari bat duen arkitektura batek nahitaez sortzen du konfiantza izan behar den aktore bat. Erdian zerbitzaririk ez duen arkitektura batek, aldiz, ez.

Legeak dioena eta arkitekturak egiten duena

RGPDak ez du eredu arkitektoniko zehatzik eskatzen. Emaitzak eskatzen ditu: datuen minimizazioa, xede mugatua, diseinu bidezko eta defektuzko babesa, betetzea frogatzeko gaitasuna. Erdian zerbitzaria duen zerbitzu batek baldintza horiek guztiak bete ditzake. Erdian zerbitzaririk ez duen zerbitzu batek eraikuntza bidez betetzen ditu horietako batzuk, ez adierazpen bidez. Minimizazio absolutua —mezua entregatzeko ezinbestekoa ez den ezer ez jasotzea— hutsala da zerbait jaso dezakeen zerbitzaririk ez dagoenean.

Eguneroko erabilera ez-sentikorretarako, zerbitzaria duen arkitektura bat guztiz arrazoizkoa da, eta operadore serio batenganako konfiantza konponbide baliozkoa da. Beste erabileretarako —sekretu profesional arautua dutenak, ardura deontologikoa dutenak, informazio bereziki sentikorra ukitzen dutenak—, konfiantza-punturik ez izatea ez da luxua, abantaila estrukturala da.

Irakurle profesionalarentzat

Komunikazio-zerbitzu profesional baten aurrean egin beharreko galderak, serie honetako aurreko artikuluetatik ezagunak direnak, arkitektura-galdera bat gehiagorekin osatzen dira:

1. ¿Edukia enkriptatzen du igarotzean? (Seguruenik bai.)
2. ¿Norekin eta noiz hitz egiten dudan metadatuak sortu eta gordetzen ditu? (Seguruenik bai.)
3. ¿Badago zerbitzaririk nire gailuaren eta hartzailearenaren arteko bidean?

4. Balego: ¿nork operatzen du, zein jurisdikziotan, eta zer gertatu beharko litzateke nire inguruko datuak eman ditzan?
5. Ez balego: aurreko galderek ez dute zentzurik.

Bi kategorien arteko aldea ez da mailakoa, motakoa baizik. Bezero bati, paziente bati edo kolega bati azaldu behar zaionean, formulaziorik zintzoena errazena ere bada: batean norbait dago erdian; bestean, ez.

Artikulu honek Cuadernos Lacre-ren hasierako zikloa ixten du. Enkriptatzeari, metadatuei eta sekretu profesionalari buruz hitz egin ondoren, koadro arkitektonikoa osatzen dugu: edukia enkriptatzea eta erdian zerbitzaririk ez izatea gauza ezberdinak dira. Biak izan daitezke legalak; bakarrak ezabatzen du konfiantza-puntua.

Iturriak eta irakurgai gehiago

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Sistema baten bermeak muturretan inplementatu behar direlako printzipioaren testu fundazionala, ez tarteko kanalean.
- 2016/679 (EB) Erregelamendua, 25. art. — datuen babesa diseinu bidez eta defektuz.
- 2016/679 (EB) Erregelamendua, 5.1.c art. — datuen minimizazio-printzipioa.
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. Eraikuntza bidez bilketa minimizatzen duten arkitekturei buruzko kapituluak.

← AurrekoaRGPD eta mezularitza profesionala: zergatik hausten dituzten gehienek arauak jakin gabeHurrengoa →CUADERNOS_LIST_SCHREMS_TITLE

Azken irakurketak

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Eraman artikulu hau zurekin behar duzun lekura.

↓ Markdown ↓ Testu arrunta ↓ PDF

Fitxategia zure gailura deskargatuko da. Bertatik gorde, Solo2ra inportatu edo nahi duzun lekuan parteka dezakezu. Cuadernosek ez du helburua zure ordez erabakitzen.

Lakre-zigilua · SHA-256 8cf87075c67d63b29f1c82ea28c64b0e91b5619e88dadd548076621b517c7251

Cuadernos Lacre · Menzuri Gestión S.L.ren argitalpena ·
R.Eugeniok idatzia · Solo2 taldeak editatua.