Analiżi · 16 ta' Mejju 2026

← Preċedenti·Li jmiss →

Meta ma hemm ħadd fin-nofs

Il-kriptaġġ ta' dak li jgħaddi minn server jipproteġi l-kontenut. Li ma jkunx hemm server fin-nofs jelimina l-mistoqsija. Mhumiex l-istess ħaġa.

Żewġ persuni, konverżazzjoni waħda

Meta żewġ persuni jitkellmu wiċċ imb wiċċ f'kamra, ħadd m'għandu jwiegħed li ma sema' xejn. Ma semgħux għax ma kienux hemm. Meta żewġ persuni jgħaddu karta minn id għal oħra, ħadd fin-nofs ma jrid jaħlef li ma qarax din il-karta. Ma hemm ħadd fin-nofs.

Il-biċċa l-kbira tal-affarijiet fil-ħajja ta' kuljum jiffunzjonaw b'dan il-mod. Aħna ma niffirmawx ftehimiet ta' kunfidenzjalità mal-arja li tittrażmetti leħinna, u lanqas mal-karta li nżommu f'idejna. Il-privatezza tal-konverżazzjoni ma tistrieħx fuq il-wegħda ta' intermedjarju, peress li ma jeżistix intermedjarju. Dik hija waħda mill-aktar forom b'saħħithom ta' privatezza: mhux għax xi ħaġa jew xi ħadd iġib ruħu tajjeb, iżda minħabba n-nuqqas ta' din ix-xi ħaġa jew xi ħadd.

Meta l-konverżazzjoni tgħaddi f'kanal diġitali, dan jinbidel b'mod awtomatiku. Il-mudell komuni huwa s-segwenti: żewġ persuni jaqbdu ma' server, is-server jirċievi l-messaġġ, jikkriptah jew jissejvjah kriptat, u jgħaddih lir-riċevitur. Is-server jinsab fin-nofs. Is-server jista' jkun onest. Jista' jkun ġie awditjat. Jista' jopera f'ġurisdizzjoni favorevoli u taħt politika ta' privatezza stretta. Dan kollu jista' jkun minnu. Iżda s-server jinsab fin-nofs.

Id-differenza bejn il-kriptaġġ u l-fatt li ma jinġabrux data (it-tieni parti)

F'artiklu preċedenti minn din l-istess serje nargumentaw li l-kriptaġġ tal-kontenut u n-nuqqas tal-ġbir ta' metadejta mhumiex l-istess. Hemm pass ieħor li għandu jiġi fformulat b'mod ċar: il-kriptaġġ ta' dak li jgħaddi minn server u li m'għandekx server lanqas mhumiex l-istess.

L-ewwel mudell — is-server fin-nofs, kontenut kriptat — jipproteġi l-kontenut mill-operatur tas-server, mill-persunal tal-manutenzjoni tiegħu, u minn attakkant estern li jikkompromett i s-sistema. U dan huwa importanti. Iżda ma jeliminax lis-server. Is-server għadu hemm. Għadu qed jipproċessa l-metadejta. Jibqa' l-punt li jista' jirċievi mandat mill-qorti, intervent legali, pressjoni politika, jew jesperjenza ksur tas-sigurtà. Jibqa' l-punt fejn ikollok bżonn tpoġġi l-fiduċja tiegħek f'xi ħadd.

It-tieni mudell — fejn ma jkun hemm l-ebda server bejn iż-żewġ estremitajiet — ma jipproteġix aħjar il-kontenut kriptat: jekk il-kriptografija hija soda, il-kontenut ikun protett fiż-żewġ każijiet. Dak li jinbidel mhuwiex il-kontenut. Li jinbidel hu li l-mistoqsija *«x'jiġri bis-server?»* titlef l-iskop tagħha, minħabba li m'hemm l-ebda server x'tistaqsi dwaru.

Il-fiduċja, in-nuqqas, u d-differenza bejniethom

Il-fiduċja tista' titqiegħed f'post tajjeb. Jeżistu kumpaniji onesti. Jeżistu awdituri rigorużi. Jeżistu leġiżlazzjonijiet favorevoli għall-utent. Jeżistu servizzi serji li jikkonformaw skrupolożament ma' dak kollu msemmi hawn fuq. Il-fiduċja, meta tingħata lil operatur li jixirqilha, m'hijiex qbil ħażin.

Iżda l-fiduċja, minkejja kemm tista' tkun soda, xorta waħda tibqa' fiduċja. Hija soluzzjoni soċjali, u mhux soluzzjoni teknika. Kumpanija tista' tinbidel minn id għal oħra. Ġurisdizzjoni tista' tibdel il-gvern tagħha. Mandat minn qorti jista' jasal għada. Vulnerabbiltà ġdida tista' tiġi skoperta x-xahar id-dieħel. Xejn minn dan ma jiġri minħabba mala fede. Jiġri għax l-operatur jeżisti, u dak kollu li jeżisti huwa suġġett għall-kontinġenzi tad-dinja.

L-assenza ta' operatur mhijiex soġġetta għall-istess kontinġenzi. Ordni mill-qorti ma tistax titlob data minn server li ma jeżistix. Attakkant ma jistax jikkomprometti server li ma jeżistix. Bidla fil-politika ta' kumpanija ma tistax taffettwa data li l-kumpanija qatt ma kellha. Il-fraži ewlenija hija sempliċi: id-data li ma teżistix ma tistax tintilef.

Dwar l-argument leġittimu min-naħa tas-server

Dawk li joffru servizz ta' messaġġi professjonali b'server fin-nofs spiss jipprovdu tliet argumenti perfettament validi. L-ewwel nett, li s-server huwa meħtieġ biex jiggarantixxi l-kunsinna meta d-destinatarju ma jkunx online. It-tieni nett, li l-kriptaġġ tal-kontenut huwa b'saħħtu u għalhekk l-operatur ma jistax jaqrah. It-tielet nett, li s-servizz jikkonforma mal-leġiżlazzjoni Ewropea u d-data hija protetta mil-liġi.

It-tliet argumenti huma kollha minnhom. Xejn minnhom ma jbiddel in-natura tal-kwistjoni. Veru li server jippermetti li l-messaġġi jiġu ssejvjati għal kunsinna posposta; minnu wkoll li t-twassil pospost jista' jiġi riżolt b'mod ieħor, permezz ta' protokolli ta' komunikazzjoni diretta bejn tagħmir li ġew raffinati għal għexieren ta' snin u llum il-ġurnata għadhom effettivi. Veru li l-kriptaġġ tal-kontenut waqt it-trażmissjoni huwa b'saħħtu f'servizzi serji. U huwa minnu li l-leġiżlazzjoni Ewropea tipproteġi lill-utenti tagħha aktar minn ħafna postijiet oħra.

Il-kwistjoni m'hijiex jekk is-servizzi b'server fin-nofs humiex legali, u lanqas jekk humiex siguri, u lanqas jekk jipproteġux il-kontenut. Dawn jistgħu jkunu hekk, huma legali u ġeneralment sikuri. L-isħabi hawn huwa li jkollok server fin-nofs hija għażla arkitettonika u mhux impożizzjoni teknika. U kull għażla għandha konsegwenzi. Arkitettura b'server fin-nofs bilfors toħloq attur li trid tafda fih. Arkitettura mingħajr server fin-nofs m'għandhiex għalfejn.

Dak li tgħid il-liġi, u dak li tagħmel l-arkitettura

Il-GDPR ma jirrikjedix mudell arkitettoniku speċifiku. Jeħtieġ riżultati: minimizzazzjoni tad-data, limitazzjoni tal-għanijiet, protezzjoni bid-disinn u b'mod awtomatiku, u l-abbiltà li jintwera l-konformità. Servizz li jinkludi server fin-nofs jista' jissodisfa r-rekwiżiti kollha. Servizz mingħajr server fin-nofs jilħaq bosta minnhom mid-disinn, mhux permezz ta' dikjarazzjoni. Il-minimizzazzjoni assoluta — fejn l-ebda data ma tinġabar ħlief dik li hija verament bżonnjuża sabiex jintbagħat messaġġ — hija sempliċi meta ma jkun hemm l-ebda server biex jiġbor xi ħaġa.

Għal użu ta' kuljum li ma jkunx sensittiv, arkitettura b'server hija perfettament raġonevoli, u l-fiduċja f'operatur serju hija arranġament validu. Għal użi oħrajn — dawk li jinvolvu s-sigriet professjonali regolat, dawk li jġorru responsabbiltajiet deontoloġiċi, u dawk li jinvolvu informazzjoni li hija partikolarment sensittiva — l-assenza ta' punt ta' fiduċja mhijiex lussu, hija vantaġġ strutturali.

Għall-qarrej professjonali

Il-mistoqsijiet li wieħed għandu jsaqsi dwar servizz ta' komunikazzjoni professjonali, u li diġà rajnihom f'artikli preċedenti f'din l-istess serje, huma kkomplementati b'mistoqsija arkitettonika oħra biss:

1. Tikkripta l-kontenut fi tranżitu? (Probabbilment iva.)
2. Tiġġenera u taħżen metadejta dwar ma' min inkun qed nitkellem u meta? (Probabbilment iva.)
3. Hemm server fit-triq bejn it-tagħmir tiegħi u dak tad-destinatarju?
4. Jekk jeżisti: min joperah, f'liema ġurisdizzjoni, u x'kellu jiġri biex dan jagħti data dwari?
5. Jekk ma jeżistix: il-mistoqsijiet preċedenti mhumiex applikabbli.

Id-differenza bejn iż-żewġ kategoriji m'hijiex ta' grad, iżda ta' tip. Meta jasal iż-żmien li wieħed jispjegaha lil klijent, pazjent jew kollega, l-aktar mod onest biex ifassalha jkun l-aktar wieħed sempliċi: waħda tkun tinvolvi lil xi ħadd fin-nofs; u l-oħra le.

Dan l-artiklu jagħlaq iċ-ċiklu inizjali ta' Cuadernos Lacre. Wara li tkellimna dwar il-kriptaġġ, il-metadejta, u s-sigriet professjonali, ikkompletaw l-istampa arkitettonika: li jkun hemm kriptaġġ u li ma jkun hemm l-ebda server huma affarijiet differenti. It-tnejn jistgħu jkunu legali; waħda biss telimina l-punt ta' fiduċja.

Sorsi u aktar qari

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Test fundamentali dwar il-prinċipju li bih il-garanziji ta' sistema għandhom jiġu implimentati fit-truf, mhux fil-kanal intermedju.
- Regolament (UE) 2016/679, art. 25 — il-protezzjoni tad-data mid-disinn u b'mod awtomatiku.
- Regolament (UE) 2016/679, art. 5.1.c — il-prinċipju tal-minimizzazzjoni tad-data.
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. Kapitoli dwar l-arkitetturi li jimminimizzaw il-ġbir fid-disinn stess.

← PreċedentiIl-GDPR u l-messaġġi professjonali: għaliex il-biċċa l-kbira jiksru r-regoli mingħajr ma jafuLi jmiss →CUADERNOS_LIST_SCHREMS_TITLE

Letturi riċenti

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Ħu dan l-artiklu miegħek kull fejn għandek bżonnu.

↓ Markdown ↓ Test sempliċi ↓ PDF

Il-fajl se jitniżżel fuq it-tagħmir tiegħek. Minn hemm tista' ssalvah, timportah f'Solo2 jew taqsmu kull fejn tixtieq. Cuadernos ma jiddeċidix id-destinazzjoni għalik.

Siġill tax-xama' · SHA-256 321d7ee4f8dfd9380a85063593a8b89da2829fdbb9e7465935c5a1e9a02d25c4

Cuadernos Lacre · Pubblikazzjoni ta' Menzuri Gestión S.L. ·
miktuba minn R.Eugenio · editjata mit-tim ta' Solo2.