Elemzés · 2026. május 16.

← Előző·Következő →

Amikor nincs senki középen

A szerveren áthaladó adatok titkosítása védi a tartalmat. Ha nincs szerver középen, a kérdés fel sem merül. Nem ugyanaz.

Két ember, egy beszélgetés

Amikor két ember szemtől szemben beszélget egy szobában, senkinek sem kell megígérnie, hogy nem hallott semmit. Nem hallotta, mert nem volt ott. Amikor két ember egy papírt ad át egymásnak egyik kézből a másikba, senkinek sem kell megesküdnie a kettő között, hogy nem olvasta el. Nincs senki középen.

A mindennapi élet dolgainak nagy része így működik. Nem írunk alá titoktartási szerződést a hangunkat közvetítő levegővel, sem a kezünkben tartott papírral. A beszélgetés magánélete nem egy közvetítő ígéretén nyugszik, mert nincs közvetítő. Ez az egyik legerősebb létező módja a magánszféra megőrzésének: nem azért, mert valami vagy valaki jól viselkedik, hanem azért, mert nincs ott valami vagy valaki.

Amikor a beszélgetés digitális csatornára terelődik, ez alapértelmezés szerint megváltozik. A megszokott modell a következő: két ember csatlakozik egy szerverhez, a szerver megkapja az üzenetet, titkosítja, vagy titkosítva elmenti, és kézbesíti a címzettnek. A szerver középen van. A szerver lehet becsületes. Lehet auditált. Működhet kedvező joghatóság alatt és szigorú adatvédelmi szabályzat szerint. Mindez lehet igaz. De a szerver középen van.

A különbség a titkosítás és a nem gyűjtés között (második rész)

Ugyanezen sorozat egy korábbi cikkében azzal érveltünk, hogy a tartalom titkosítása és a metaadatok nem gyűjtése nem ugyanaz. Van még egy lépés, amelyet világosan meg kell fogalmazni: a szerveren áthaladó adatok titkosítása és a szerver hiánya szintén nem ugyanaz.

Az első modell — szerver középen, titkosított tartalom — megvédi a tartalmat a szerver üzemeltetőjétől, a karbantartó személyzettől, és a rendszert kompromittáló külső támadótól. És ez fontos. De nem küszöböli ki a szervert. A szerver továbbra is ott van. Továbbra is feldolgozza a metaadatokat. Továbbra is egy olyan pont marad, amely bírósági megkeresést, jogi beavatkozást, politikai nyomást vagy biztonsági rést szenvedhet el. Továbbra is egy olyan pont, amely megköveteli, hogy bízzunk valakiben.

A második modell — nincs szerver a két végpont között — nem védi jobban a titkosított tartalmat: ha a kriptográfia szilárd, a tartalom mindkét esetben védett. Ami változik, az nem a tartalom. Ami változik, az az, hogy a *„mi a helyzet a szerverrel?”* kérdés értelmét veszti, mert nincs szerver, amiről kérdezni lehetne.

Bizalom, hiány, és a kettő közötti különbség

A bizalom lehet megalapozott. Léteznek becsületes cégek. Léteznek szigorú auditorok. Léteznek felhasználóbarát jogszabályok. Léteznek komoly szolgáltatások, amelyek szigorúan betartják a fentieket. A bizalom, ha egy azt megérdemlő operátornak adjuk, nem egy rossz egyezség.

De a bizalom, bármennyire is szilárd, csak bizalom marad. Ez egy társadalmi megoldás, nem technikai megoldás. Egy cég gazdát cserélhet. Egy joghatóság megváltoztathatja a kormányát. Egy bírósági végzés érkezhet holnap. Egy új sebezhetőség kiderülhet a jövő hónapban. Mindez nem rosszhiszeműségből történik. Azért történik, mert az operátor létezik, és minden, ami létezik, ki van téve a világ eshetőségeinek.

Az operátor hiánya nincs kitéve ugyanezen eshetőségeknek. Egy bírósági végzés nem kérhet adatokat egy nem létező szervertől. Egy támadó nem kompromittálhat egy nem létező szervert. Egy cég politikájának megváltozása nem befolyásolhat olyan adatokat, amelyekkel a cég soha nem is rendelkezett. A kulcsmondat egyszerű: a nem létező adatokat nem lehet elveszíteni.

A szerveroldali legitim érvről

Aki professzionális üzenetküldő szolgáltatást kínál szerverrel a középpontban, általában három tökéletesen érvényes érvet fogalmaz meg. Először, hogy a szerver szükséges a kézbesítés garantálásához, amikor a címzett offline állapotban van. Másodszor, hogy a tartalom titkosítása erős, és ezért az operátor nem tudja elolvasni. Harmadszor, hogy a szolgáltatás megfelel az európai jogszabályoknak, és az adatokat a törvény védi.

Mindhárom érv igaz. Egyik sem változtatja meg a dolog természetét. Igaz, hogy egy szerver lehetővé teszi az üzenetek tárolását a késleltetett kézbesítéshez; az is igaz, hogy a késleltetett kézbesítés más módon is megoldható, az eszközök közötti közvetlen kommunikációs protokollokkal, amelyeket évtizedek óta finomítanak és ma is működnek. Igaz, hogy a tranzit tartalom titkosítása erős a komoly szolgáltatásokban. És az is igaz, hogy az európai jogszabályok jobban védik a felhasználókat, mint sok más helyen.

A kérdés nem az, hogy a középső szerverrel rendelkező szolgáltatások legálisak-e, nem is az, hogy biztonságosak-e, sem az, hogy védik-e a tartalmat. Lehetnek ilyenek, legálisak és általában biztonságosak. A kérdés az, hogy a középső szerver megléte architekturális választás, nem technikai kényszer. És minden választásnak következményei vannak. A középső szerverrel rendelkező architektúra szükségszerűen létrehoz egy szereplőt, akiben meg kell bízni. Egy szerver nélküli architektúra nem.

Amit a törvény mond, és amit az architektúra tesz

A GDPR nem követel meg egy konkrét architekturális modellt. Eredményeket követel meg: adatminimalizálást, célhoz kötöttséget, beépített és alapértelmezett adatvédelmet, a megfelelés bizonyításának képességét. Egy középső szerverrel rendelkező szolgáltatás minden követelményt teljesíthet. Egy szerver nélküli szolgáltatás közülük többet már a konstrukciójából adódóan, nem csak nyilatkozat alapján teljesít. Az abszolút minimalizálás — annak a mellőzése, hogy bármi olyat gyűjtsenek, ami nem feltétlenül szükséges az üzenet kézbesítéséhez — triviális, ha nincs egy szerver, amely bármit is gyűjthetne.

A mindennapi, nem érzékeny használat esetén egy szerveres architektúra tökéletesen észszerű, és a komoly operátorba vetett bizalom érvényes egyezség. Az egyéb felhasználások esetén — amelyek szabályozott szakmai titoktartást foglalnak magukban, amelyek etikai felelősséggel járnak, amelyek különösen érzékeny információkat érintenek — a bizalmi pont hiánya nem luxus, hanem strukturális előny.

A szakmai olvasónak

A professzionális kommunikációs szolgáltatással kapcsolatos felteendő kérdések, amelyek már ismerősek lehetnek a sorozat korábbi cikkeiből, csak egyetlen további architekturális kérdéssel egészülnek ki:

1. Titkosítja-e a tartalmat továbbítás közben? (Valószínűleg igen.)
2. Létrehoz és tárol-e metaadatokat arról, hogy kivel és mikor beszélek? (Valószínűleg igen.)
3. Van-e egy szerver a saját és a címzett eszköze között az úton?

4. Ha van: ki üzemelteti, melyik joghatóság alatt, és minek kellene történnie ahhoz, hogy adatokat adjon ki rólam?
5. Ha nincs: az előző kérquestions tárgytalannak minősülnek.

A különbség a két kategória között nem fokozati, hanem típusbeli. Amikor eljön az ideje, hogy elmagyarázzuk egy ügyfélnek, egy páciensnek vagy egy kollégának, a legőszintébb megfogalmazás egyben a legegyszerűbb is: az egyikben van valaki középen; a másikban nincs.

Ez a cikk lezárja a Cuadernos Lacre kezdeti ciklusát. Miután beszéltünk a titkosításról, a metaadatokról és a szakmai titoktartásról, kiegészítjük az architekturális képet: a tartalom titkosítása és a szerver hiánya két különböző dolog. Mindkettő lehet legális; de csak az egyik szünteti meg a bizalmi pontot.

Források és további olvasnivalók

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Annak az elvnek az alapvető szövege, amely szerint a rendszer garanciáit a végpontokon kell megvalósítani, nem pedig a köztes csatornában.
- (EU) 2016/679 rendelet, 25. cikk — beépített és alapértelmezett adatvédelem.
- (EU) 2016/679 rendelet, 5. cikk (1) bek. c) pont — adattakarékosság elve.
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. Fejezetek azokról az architektúrákról, amelyek konstrukciójuk révén minimalizálják az adatgyűjtést.

← ElőzőA GDPR és a professzionális üzenetküldés: miért sértik meg a legtöbben tudtukon kívül a szabályokatKövetkező →CUADERNOS_LIST_SCHREMS_TITLE

Legutóbbi olvasmányok

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Vigye magával ezt a cikket, ahová csak szüksége van rá.

↓ Markdown ↓ Egyszerű szöveg ↓ PDF

A fájl letöltődik az Ön eszközére. Onnan elmentheti, importálhatja a Solo2-be, vagy megoszthatja bárhol. A Cuadernos nem dönt Ön helyett a fájl sorsáról.

Viaszpecsét · SHA-256 4f0221bb07010e996884004fca30712f7ed2e7c078880faec7baff16af7d2c6b

Cuadernos Lacre · A Menzuri Gestión S.L. kiadványa ·
írta R.Eugenio · szerkesztette a Solo2 csapata.