Self-hosting mint szakmai gyakorlat

A szerver nem más, mint egy számítógép. A kérdés nem az, hogy legyen-e ilyenünk, hanem az, hogy hol élnek az ügyfeleink adatai, ki tartja fenn azokat, és ki vállalja a felelősséget, ha valami elromlik.

Hogy értsük egymást: Az adatai mindig valakinek a számítógépén élnek: egy óriásén, akire mindent rábíz, egy béreltén, amit Ön kezel, vagy a sajátján. Minél több kontrollt akar, annál több felelősséget vállal. Egy nagy harmadik félre való delegálás megnyugtat, de nem mentesít: az információ az Öné —és az ügyfeleié—, és a felelős Ön.

A felhő és a pince közötti kérdés

Érdemes egy olyan szó demisztifikálásával kezdeni, amely ok nélkül ijesztő: szerver. A szerver nem egy titokzatos gép egy hűtött helyiségben. Egyszerűen valaki más —vagy a saját— számítógépe, amely információkat tárol, és átadja azokat annak, aki kéri. Évtizedekig egy mappában, egy irattartóban, az íróasztalon őriztük ügyfeleink adatait, és senki sem veszítette el emiatt az álmát. Az információ nem volt ijesztő, mert papíron volt; nem kell ijesztőnek lennie csak azért sem, mert lemezen van.

A „felhő” sem éteri. Egy cég számítógépe, szinte mindig messze, és szinte mindig valaki másé. Akaratlanul tanultam meg ezt azon a napon, amikor abban a hitben, hogy fájljaim biztonságban vannak a Google Drive-on, felfedeztem, hogy a számítógépemen lévő mappa nem a dokumentumaimat tartalmazta, hanem máshol lévő dokumentumokra mutató parancsikonokat. Ha az a másik hely úgy döntene, hogy bezár, árat változtat vagy megszünteti a szolgáltatást, a nyugalmam vele együtt veszne el. Nem a dolgaim voltak birtokomban; hozzáférési engedélyem volt hozzájuk.

Innen ered e Füzet kérdése, könnyebb kimondani, mint megválaszolni: hol kellene lakniuk az ügyfeleid adatainak? És a sajátjaidnak? A nyilvános vita úgy veti fel, mintha csak két szembenálló válasz létezne — a nagy platformok felhője vagy a magad megoldása —, szinte mint táborkérdést. De ez nem két út: három, és egyik sem hitbéli cselekedet. Lassan olvasva több árnyalatuk van, és többet kérnek, mint amennyinek látszik.

Ez Önről szól, függetlenül attól, mit árul

Könnyű azt hinni, hogy a titoktartás az ügyvédek, orvosok vagy újságírók dolga, és a többieknek nincs mit rejtegetniük. Ez hiba, mégpedig a drága fajtából. Szinte minden vállalkozás őriz a törvény hatálya alá tartozó ügyféladatokat, és sokan tudtukon kívül sokkal érzékenyebb információkat tárolnak, mint amilyennek látszik.

Egy kanapébolt feljegyzi a vásárló nevét, címét és telefonszámát; ha van finanszírozás, a gazdasági adatait is. Egy felújító vagy lakberendező cég megőrzi ügyfelei otthonainak belső fotóit és lakásaik teljes alaprajzait. Egy takarítócég az általa takarított irodák alaprajzaival dolgozik, gyakran színekkel és számokkal jelölve, hogy melyik alkalmazott hová lép be, hány órakor és milyen kulccsal. Mindez nem tűnik nagy dolognak, amíg az ember fel nem teszi a kérdést, ki másnak lenne értéke: azok a takarítási alaprajzok, más szemmel nézve, tökéletes térkép annak, aki be akar törni lopni.

Az, hogy egy vállalkozás kicsi, vagy kanapékat árul a perek védelme helyett, nem teszi adatait értéktelenné, és nem jelenti azt, hogy a törvény nem vonatkozik rá. Csak azt eredményezi, hogy a tulajdonosa hajlamos kevesebbet gondolni erre. És az, hogy keveset gondolunk valamire, ami a mi felelősségünk, pontosan az a pont, ahol a problémák kezdődnek.

Hol élnek az adatai?

Erre a kérdésre lényegében három válasz van. És jó észben tartani, hogy az „adatok” nem csupán egy ügyfél dossziéja vagy a számlák és árajánlatok halmaza: a vele folytatott beszélgetéseid is azok — WhatsAppon, professzionális csevegőszolgáltatáson, Solo2-n keresztül —. A következő három válasz nem a tisztaság fokozatai, sem a jótól a rosszig vezető létra: három módja annak, hogy ugyanazt osszuk el, az ellenőrzést és a felelősséget.

Mindent egyetlen szolgáltatóra bízni. Ez a legelterjedtebb, és a többség számára az egyetlen, amit ismer. Mindent beleteszek a Google Workspace-be vagy a Microsoft 365-be, és teljesen a szolgáltatóra bízom. Fizetem a díjamat, és többé nem gondolok rá. Ennek legszélsőségesebb formája azok a szolgáltatások, ahol még csak nem is birtoklod az adataidat: bizonyos felhős számlázóprogramok például megőrzik a számláidat és árajánlataidat — és nagyon jól működnek —, de az információ az ő rendszerükben él, nem a tiédben. Amíg fizetsz, hozzáférsz; azon a napon, amikor távozol, rájössz, hogy elvinni a saját előzményeidet nehéz vagy lehetetlen. Az adataidat félig túszul ejteni nem egy szolgáltató számára épp az, ami visszatart attól, hogy a versenytárshoz menj. A kényelemért cserébe átadom az ellenőrzést és — hangosan ki nem mondva — azt az érzést, hogy a felelősség már nem az enyém. Ide kívánkozik egy árnyalat, amit szinte soha nem tesznek meg: delegálni nem egyenlő az amerikaival. Ugyanolyan kényelmesen rábízhatok mindent egy európai szolgáltatóra — például az Infomaniakra — és egy tollvonással megoldhatom a nemzetközi adattovábbításokkal kapcsolatos kételyek jó részét, amelyeket a „Schrems II”-ben láttunk, anélkül hogy bármit is magam tárolnék. Ez nem az Egyesült Államok a világegyetem többi része ellen: már a tiszta delegáláson belül is vannak döntések, amelyek számítanak.

Saját szervert bérelni és kezelni. Megvan ugyanaz, amit a Microsoft vagy a Google adna, de magam építem fel. Bérelek egy szervert egy európai szolgáltatónál —Hetzner, OVH, Scaleway—, szabad szoftvert telepítek (például Nextcloudot a fájlokhoz), és magam adminisztrálom az eredményt. Valódi kontrollt nyerek: tudom, mi fut, hol és miért. De a gép továbbra is egy harmadik fél adatközpontjában van, és mindenekelőtt változik az, hogy ki viszi el a balhét. Delegálással, ha valami elromlik, van kit hibáztatni. Saját kezeléssel valószínűleg az enyém lesz a hiba.

A saját számítógépén tartani. Ez az a lehetőség, amiről szinte senki sem beszél, és ez e füzet szíve. Nincs szükség egy hatalmas, a nap huszonnégy órájában egy óriási adatközpontban működő szerverre a dolgai hosztolásához. Az irodai számítógépe már most is egy szerver: Önt szolgálja ki. Bekapcsolva hagyja az irodában, és csatlakozik hozzá a laptopjáról egy ügyfélnél, vagy a mobiljáról, amikor otthon van. „Irodai számítógépnek” hívjuk, nem „szervernek”, de pontosan ugyanazt teszi, mint az előző két opció. A kontroll maximális, és a közelség is: az adatai ott vannak, ahol Ön. A hátulütője, díszítés nélkül kimondva, az, hogy a felelősség is maximális. Ha elmegy az áram, nincs ügyeletes technikus Nürnbergben: Önnek kell visszakapcsolnia a biztosítékot. És ahhoz, hogy ez a számítógép kívülről elérhető legyen, szükség van valamire, ami hidat ver a laptopja és aközött. Ez nem mágia, és jó ezt tudni, mielőtt ezt az utat választja.

És még csak az irodai számítógépet sem kell újrahasznosítani: létezik egy kifejezetten erre tervezett eszköz, a NAS (a Synology, a QNAP és mások gyártják). Mint szinte minden, amit ezekben a Cuadernos-ban láttunk, belül nincs semmi varázslat: ez egy specializált számítógép, ugyanaz a fajta gép, amelyet egy adatközpontban bérelnél, csak arra építve, hogy adatokat tároljon és azokat a hálózaton keresztül kiszolgálja, monitor és billentyűzet nélkül. Csatlakoztass hozzá egy képernyőt és egy billentyűzetet, és egy közönséges számítógéped van; telepítsd a megfelelő szoftvert a gépedre, és egy NAS-od van. A különbség az, hogy a NAS már használatra kész állapotban érkezik. Megveszed, otthon vagy az irodában csatlakoztatod, és a tiéd. Nem fizetsz havi díjat; egyszer fizeted ki, és a tiéd, mint vállalkozásod bármely más eszköze. Bekapcsolod, kikapcsolod, elviszed máshová, ha akarod. És mivel a tiéd, semmi sem akadályoz meg abban, hogy kettő legyen —egy otthon, egy az

irodában— vagy három, egyet egy biztonságos helyre is hozzáadva, egymással szinkronizálva: a saját redundanciád, anélkül, hogy egy harmadik fél karbantartásától függnél. Az önálló üzemeltetés végső soron nem egyetlen dolog: gépek, tulajdon, helyszínek és szoftver kombinációja.

Itt elkerülhetetlen megnevezni, amit csinálunk, és álca nélkül csináljuk: a Solo2-ben ezt a hidat maga az alkalmazás veri. Az irodád számítógépe csak a megbízható eszközeid számára marad elérhető, és mindig titkosítás alatt, a többi készüléked pedig magától újrakapcsolódik hozzá. Amikor egy ügyfél beszél veled, a te számítógéped — nem egy harmadik félé — beszél az ügyféllel. Nem oldjuk meg az áramszünetet; a hidat oldjuk meg. És nem vagyunk egyedül: szinte minden igényre léteznek ma programok — szabadok vagy zártak —, amelyek épp ezt teszik lehetővé, hogy az adatok a saját gépeden legyenek, és kívülről elérd őket. A miénk egy példa; a lényeg az ötlet, nem a márka.

A redundancia nem szupererő

Itt merül fel az azonnali ellenvetés, és ez ésszerű: ha mindenem az irodai számítógépemen van, mi történik, ha elromlik? A kérdés jó. A válasz az, hogy a nagy szolgáltatóknál elképzelt biztonsági háló szerényebb —és könnyebben utánozható—, mint amilyennek látszik.

Amikor egy multinacionális cég adatközpontjában hagyom az adataimat, bízom benne, hogy több helyen is van róla másolata. És valószínűleg van is: egy második helyszínen, talán egy harmadikon. De ez a redundancia nem végtelen, és mindenekelőtt nem az enyém: ez továbbra is egy merevlemez marad, amelynek nem én vagyok a tulajdonosa, és amelyet valaki olyan kezel, akibe olyan bizalmat fektetek, amelyet szinte soha nem ellenőrzök.

Ezt a hálót én magam is meg tudom szőni, mégpedig döntő előnnyel. A napi szolgáltatásom az irodai számítógépen él. Onnan egy titkosított másolatot őrzök egy baráti cég számítógépén —egy kollégánál, egy másik megbízható irodában— és egy másik titkosított másolatot, ha akarom, ugyanannál az európai szolgáltatónál, akiről beszéltünk. A különbség minden: amit kívül hagyok, az nem a szolgáltatásom és nem is az adataim olvasható formában, hanem egy titkosított másolat, amit csak én tudok kinyitni. A külső szolgáltató egy lezárt ládát őriz, amelyhez nincs kulcsa. Nem az információimat bízom rá: néhány bájtot bízok rá, amelyek nélkülem semmit sem jelentenek.

Biztonságban volt, amíg már nem

Engedjen meg egy személyes történetet, mert ez bármilyen érvnél jobban szemlélteti ezt. Több mint tíz évig voltam a CrashPlan hűséges ügyfele, amely technikailag egy rendkívüli biztonsági mentési szolgáltatás volt. A felhőjükbe mentettem minden számítógépemet és a családomét is —a cégeseket és az otthoniakat, mindent—, olyan verziókkal, amelyeket az általam kívánt gyakorisággal tudtam visszaállítani, visszautazva az időben akár hónapokkal ezelőtti konkrét fájlokig. Az első másolat után csak a különbségeket továbbította, titkosítva és tömörítve, így szinte erőfeszítés nélkül tartottam naprakészen egy hatalmas biztonsági mentést. Sokszor megmentett, egy ostoba dokumentumtól kezdve egészen egy egész lemezig. Az ár az évek során emelkedett, de nem érdekelt: boldogan fizettem.

Amit nem tudtam, az az volt, hogy a CrashPlan számítási hibát követett el: szerződésben korlátlan tárhelyet ígért, térben és időben egyaránt. A tér megszorozva az idővel —évek történelme, verziók pár percenként— pedig addig nő, amíg fenntarthatatlanná válik. Egy nap mindannyiunkkal közölték, hogy a szolgáltatás megszűnik. Elegánsan tették, és bőséges határidővel, majdnem egy évvel, és eszközöket adtak a dolgaink letöltéséhez. De hová megy az ember az összes lemezének több mint tíz évnyi verziózott másolatával? Ott jön rá az ember, hogy sem módja nincs mindent letölteni, sem helye, ahová tehetné, és ha mégis tudná, az új raktár egy vagyonba kerülne.

Megmentettem négy nélkülözhetetlen dolgot. A többi elment, amikor lekapcsolták a kapcsolót. Nyugodt voltam, az információim biztonságban voltak... amíg meg nem szűntek azok lenni. És nem árulás miatt: a CrashPlan kifogástalanul viselkedett — ellentétben az Evernote-tal, amely évekkel később szégyenletesen viselkedett —;

egyszerűen a felhőbeli őrangyalom úgy döntött, teljes joggal, hogy nem lesz többé az. Az eredmény számomra azonos volt: amit biztonságosnak hittem, eltűnt.

Amit ez a történet valóban tanít, annak több köze van az emberi természethez, mint a technológiához. Amikor valaki úgy érzi, hogy valami az ő felelőssége, megelőző módon cselekszik: másolatokat készít, bebiztosítja magát, józan ítélőképességgel bizalmatlan. Amikor azt hiszi —tévesen—, hogy a felelősséget egy nagy és fizetőképes harmadik fél viseli, ellazul és hagyja menni a dolgokat. Ez a delegált nyugalom nem körültekintés: ez, smink nélkül, a felelőtlenség egy formája.

Fizetni nem ugyanaz, mint megfelelni

Ez a csendes felelőtlenség nagyon hasonlít azokhoz a szülőkhöz, akik beíratják gyermeküket a legdrágább iskolába, kifizetnek neki utána egy mesterképzést, és ezzel azt hiszik, teljesítették a kötelességüket. Nem teljesítették. Szülőnek lenni azt jelenti, hogy aggódunk azért, mit tanult ma, amit nem ért, az értékeiért, az önmagába vetett hitéért. Ha huszonöt évesen az a gyerek nem tud dolgozni vagy viselkedni, a hiba nem az iskolaé, amely felvette a pénzt: azé, aki delegált és fizetett, abban a hitben, hogy ez elég. Egy harmadik félnek való fizetés nem mentesít a felelősség alól. Soha nem tette.

Az adatokkal ugyanígy van, és a közelmúlt története ezt megerősíti. Ötven vagy száz évvel ezelőtt egy szakember mappákban őrizte ügyfelei dolgait, az irodájában vagy otthon, és felelősnek érezte magát értük. Ritkán veszett el bármi. Átléptünk a digitális világba, és bámulatos könnyedséggel mindent feltöltünk a „felhőbe” — ami nem más, mint egy multinacionális cég számítógépe — és nem aggódunk többé. És gyakran történnek balesetek, vannak cégek, amelyek mindent elveszítenek, és olyankor azt mondják: a Google volt a hibás, a Microsoft volt a hibás. Nem. Az információ a tiéd vagy az ügyfeleidé, de a felelős te vagy.

A saját hosztolás nem technikai hóbort: a évtizedekkel ezelőtti nyugalom visszaszerzése, annak tudata, hogy mi hol van és miért. Az adatvédelem eközben egy éles ingamozgást élt át —a szabályok teljes hiányától kezdve, amikor bárki gondolkodás nélkül mutogatta egy ügyfél adatait, egy olyan követelményig, amely aránytalan keménységgel sújtja a legkisebbet, az egyéni vállalkozót, aki odaadja egy ügyfél telefonszámát a futárnak. Nem a célt vitatom; az aránytalanságot észlelem. De az aránytalanság nem mentesít minket: azon a napon, amikor a közigazgatásnak meglesznek az eszközei a nagyarányú nyomon követéshez és szankcionáláshoz, a méret már nem fog megvédeni senkit, és bölcs dolog nem rendezetlen házzal várni azt a napot. Az adatok saját kontroll alatt tartása segít a megfelelésben és segít annak bizonyításában is. És mindenekelőtt a helyükre teszi a dolgokat: amikor az információ az Öné, a felelősség teljes egészében az Öné —nincs harmadik fél, akit hibáztathatna, sem harmadik fél, akinek a hibája Önt veszélybe sodorná—.

A felelősség véd is

Tisztességtelen lenne árnyak nélkül lefesteni ezt. A közvetítő helyét elfoglalni azt jelenti, hogy vinni kell a vele járót: naprakész másolatokat tartani, frissítéseket alkalmazni és egy jogi felelősséget — a RGPD szerintit —, amely valójában sosem szűnt meg teljesen a tiéd lenni (a lábjegyzetbeli hivatkozások részletezik a konkrét cikkeket). Van munka, és van egy nap, amikor valami rosszkor mond csődöt. Nem rejtjük el.

De a félelem, amely ezt a szót, a felelősséget körülveszi, rosszul van kalibrálva. Sokkal könnyebb elveszíteni a fájljaidat egy felhőszolgáltatásban, amely bezár, vagy a fotóidat a Google Fotókban, mint elveszíteni azt a fontos dokumentumokat tartalmazó mappát, amely a saját számítógépeden van: azt, amelyikről tudod, hol van, és amelynek hiányát észrevennéd, amint eltűnne. Amit a magadénak érzel, gondozod; amit másnál biztonságban hiszel, elhanyagolod.

Gondolj a régi fényképalbumokra, az előhívott papírból készültekre, amelyeket egy fiókban őriztek. Hallottad valaha is, hogy valaki azt mondja, „elveszítette” a családi albumát? Hallani a házról, amely leégett az albummal együtt; de csak úgy elveszíteni, nem. Ezzel szemben az emberek, akiknek minden fotójuk a Google Fotókban vagy az Apple Fotókban volt, és semmi nélkül maradtak: ez a történet néhány havonta visszatér, mert azt hitték,

biztonságban van. A Google Fotók gondozza a fotóidat, persze; de nem gondozza úgy, ahogy a szülők gondozzák az albumot, amelyben a gyerekeik és unokáik vannak. Ezt a különbséget egyetlen adatközpont sem javítja ki: a felelősség, amikor a tiéd, nem csupán teher; egyben a legjobb garancia is.

Négy kérdés a döntés előtt

Ha bármilyen formában fontolgatja a lépés megtételét, érdemes először négy kérdésre elfogulatlan őszinteséggel válaszolni:

1. Adataid mely részét fájna elveszítened, vagy nem tudnod elvinni? És óvatosan a „rutinszerű” elvetésével: a számlák előzménye a világ legprózaibb dolgának tűnik, amíg programot nem váltasz, és rá nem jössz, hogy azok a számlák a szolgáltatóé voltak, nem a tieid — hogy legfeljebb PDF-be nyomtathatod őket, anélkül hogy bennük kereshetnél —. Nem csak az érzékenység kérdése: az a kérdés, kihez tartozik valójában az, amit meg kell őrizned.
2. Melyik lehetőség arányos a valós technikai képességeddel? Egy jól karbantartott saját számítógép bárki számára elérhető; egy egész szervert üzemeltetni már kevésbé. Légy őszinte magaddal azzal kapcsolatban, mit tudsz és mit nem. És ne feledd, hogy egy egész szerver felépítése és a minden delegálása között van egy nagyon ésszerű köztes terep: programok — szabadok vagy zártak —, amelyek a saját gépeden tárolják az adataidat, és hagyják, hogy kívülről elérd őket. Sok ember számára ez a legjobb egyensúly.
3. Mi a terve a legrosszabb napra? Adatszivárgás, tönkremenő lemez, megszűnő szolgáltató, betegszabadságon lévő technikus. Ha a terv úgy kezdődik, hogy „ennek nem szabadna megtörténnie”, az nem terv.
4. Tudná-e bizonyítani, hogy megfelel a szabályoknak, ha holnap ellenőriznék? Jól csinálni és bizonyítani tudni, hogy jól csinálja, nem ugyanaz. A törvény az utóbbit követeli meg.

Nincs univerzális válasz. Van egy arányos válasz, amelyet őszintén fogadunk el arról, hogy mit nyerünk és mit öröklünk. És a technikán túl egy egyszerű bizonyosság: az adatai valakinek a számítógépén élnek. Az egyetlen kérdés, ami igazán számít, az az, hogy kinek a számítógépe legyen az.

A saját hosztolás nem erény és nem is bűn: ez egy olyan eszköz, amelynek konkrét képességei és felelősségei vannak. A kérdés sosem az volt, hogy a sajátodat hosztold-e, hanem az, hogy mit, hogyan és milyen támogató hálózattal. Az adatok feletti kontroll visszaszerzése nem a pincébe való visszatérést jelenti, és nem is a mindenben való bizalmatlanságot: ez a visszatérés ahhoz a felelősségérzethez, ami a miénk, mint amikor az az adat még egy asztalon lévő mappában élt. Ez a felelősség, helyesen értelmezve, a valódi szolgáltatás, amelyet egy szakember nyújt az ügyfeleinek.

Források és további olvasnivalók

- 2016/679/EU rendelet — 28. cikk (adatfeldolgozó), 32. cikk (az adatkezelés biztonsága), 33. cikk (adatvédelmi incidens bejelentése), 37. cikk (adatvédelmi tisztviselő kijelölése).
- Spanyol Adatvédelmi Ügynökség — *Gyakorlati útmutató a személyes adatok kezelésének kockázatelemzéséhez* (érvényes változat). Keretrendszer azon adatkezelők számára, akik saját technikai feladatokat vállalnak.
- Európai Adatvédelmi Testület — *Guidelines 1/2024 on processing of personal data based on legitimate interests*. Alkalmazható a saját infrastruktúrával kapcsolatos döntések arányossági vizsgálatára is.
- Európai Bizottság — az európai joghatóság alatt álló információs szolgáltatók nyilvános jegyzéke. Adminisztratív kiindulópont az európai felügyelt hosztolási lehetőségek azonosításához.
- Nextcloud GmbH (Németország) — *Nextcloud Enterprise architecture and compliance documentation*. Dokumentált eset szabad szoftverrel, saját hosztolású és európai szolgáltató által felügyelt módozatokkal; hasznos technikai referenciaként egy 2016 óta európai joghatóság alatt fenntartott projekthez.

← ElőzőA 24 szó: mi az a kriptográfiai identitásKövetkező →Valódi vs. látszólagos adatvédelem: a kérdések, amelyeket érdemes feltenni

Legutóbbi olvasmányok

- Reflexió · 2026. június 29. Nem vagy névtelen
- Reflexió · 2026. május 27. Amit egy aláírás nem tud megoldani
- Elemzés · 2026. május 26. Valódi vs. látszólagos adatvédelem: a kérdések, amelyeket érdemes feltenni

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 a4eb243eec03047a76365afe45e0ccaebe8e822764d93bbf253903a63f86078d

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