Self-hosting kao profesionalna praksa

Poslužitelj nije ništa više od računala. Pitanje nije treba li ga imati, već gdje žive podaci vaših klijenata, tko ih podržava i tko snosi odgovornost kada nešto pođe po zlu.

Da se razumijemo: Vaši podaci uvijek žive u nečijem računalu: u onom diva kojem sve povjeravate, u unajmljenom kojim vi upravljate ili u vašem vlastitom. Što više kontrole želite, to više odgovornosti preuzimate. Delegiranje velikoj trećoj strani smiruje, ali ne oslobađa: informacija je vaša —i vaših klijenata—, a odgovorna osoba ste vi.

Pitanje između oblaka i podruma

Dobro je započeti deaktivacijom riječi koja bezrazložno plaši: poslužitelj. Poslužitelj nije tajanstveni stroj u ohlađenoj prostoriji. To je jednostavno tuđe računalo —ili vaše— koje pohranjuje informacije i predaje ih onome tko ih zatraži. Desetljećima smo podatke naših klijenata čuvali u mapi, u kartoteci, na radnom stolu i nitko nije gubio san zbog toga. Informacije nisu bile zastrašujuće jer su bile na papiru; ne moraju biti ni zato što su na disku.

„Oblak" također nije eteričan. To je računalo tvrtke, gotovo uvijek daleko i gotovo uvijek tuđe. To sam nenamjerno naučio onog dana kada sam, uvjeren da su moje datoteke sigurne na Google Driveu, otkrio da mapa na mom računalu ne sadrži moje dokumente, već prečace do dokumenata koji žive negdje drugdje. Ako bi to drugo mjesto odlučilo zatvoriti, promijeniti cijenu ili otkazati pretplatu, moj mir bi otišao s njim. Nisam posjedovao svoje stvari; imao sam dopuštenje za pristup njima.

Odatle se rađa pitanje ove Bilježnice, lakše za izreći nego za odgovoriti: gdje bi trebali živjeti podaci tvojih klijenata? A tvoji vlastiti? Javna rasprava ga postavlja kao da postoje samo dva suprotstavljena odgovora — oblak velikih platformi ili to napraviti sam —, gotovo kao pitanje tabora. No to nisu dva puta: tri su, i nijedan nije čin vjere. Čitani polako, imaju više nijansi i traže više nego što se čini.

Ovo se tiče vas, bez obzira na to što prodajete

Lako je misliti da je povjerljivost stvar odvjetnika, liječnika ili novinara i da ostali nemaju što skrivati. To je pogreška, i to skupa. Gotovo svaka tvrtka čuva podatke svojih klijenata podložne zakonu, a mnogi čuvaju, ne znajući to, informacije mnogo osjetljivije nego što se čini.

Trgovina kaučima bilježi ime, adresu i telefon onoga tko kupuje; ako ima financiranja, i njegove ekonomske podatke. Tvrtka za preuređenja ili dekoraciju čuva fotografije unutrašnjosti domova svojih klijenata i potpune nacrte njihovih stanova. Tvrtka za čišćenje barata nacrtima ureda koje čisti, često označenima bojama i brojevima koji pokazuju koji zaposlenik ulazi kamo, u koliko sati i kojim ključem. Ništa od toga ne djeluje kao velika stvar dok se čovjek ne zapita za koga bi još imalo vrijednost: ti nacrti čišćenja su, gledani drugim očima, savršena karta za onoga tko se želi provaliti da krade.

To što je tvrtka mala ili što prodaje sofe umjesto obrane u parnicama, ne čini njezine podatke bezvrijednima niti uzrokuje da se zakon prestane primjenjivati na nju. To samo uzrokuje da njezin vlasnik obično manje razmišlja o

tome. A malo razmišljanje o nečemu što je vaša odgovornost upravo je mjesto gdje počinju problemi.

Gdje žive vaši podaci?

Na to pitanje u biti postoje tri odgovora. I dobro je sjetiti se da „podaci" nisu samo dosje klijenta ili skup računa i predračuna: to su i tvoji razgovori s njim — preko WhatsAppa, preko profesionalne usluge čavrljanja, preko Solo2 —. Tri odgovora koja slijede nisu stupnjevi čistoće niti ljestvica od dobrih do loših: to su tri načina raspodjele istog, kontrole i odgovornosti.

Sve povjeriti jednom pružatelju. To je najuobičajenije i za većinu jedino što poznaje. Stavim sve u Google Workspace ili u Microsoft 365 i povjerim to u cijelosti pružatelju. Plaćam svoju pretplatu i prestajem misliti na to. Najekstremniji oblik toga su usluge gdje čak ni nemaš svoje podatke: neki programi za izdavanje računa u oblaku, primjerice, čuvaju ti račune i predračune — i rade vrlo dobro —, ali informacije žive u njihovom sustavu, ne u tvojem. Dok plaćaš, pristupaš; na dan kad odeš, otkriješ da je ponijeti vlastitu povijest teško ili nemoguće. Imati tvoje podatke napola kao taoca za poneku tvrtku upravo je ono što te sprječava da odeš konkurenciji. U zamjenu za udobnost predajem kontrolu i — ne govoreći to naglas — osjećaj da odgovornost više nije moja. Tu pristaje nijansa koja se gotovo nikad ne pravi: delegirati nije isto što i američko. Mogu sve jednako udobno povjeriti europskom pružatelju — na primjer Infomaniaku — i jednim potezom riješiti dobar dio dvojbi o međunarodnim prijenosima koje smo vidjeli u „Schrems II", ne hostajući ništa sam. Nisu to Sjedinjene Države protiv ostatka svemira: i unutar čistog delegiranja već postoje odluke koje su važne.

Iznajmljivanje i upravljanje vlastitim poslužiteljem. Imam isto što bi mi dali Microsoft ili Google, ali to sam postavljam. Unajmljujem poslužitelj kod europskog pružatelja —Hetzner, OVH, Scaleway—, instaliram slobodni softver (Nextcloud za datoteke, na primjer) i sam upravljam rezultatom. Dobivam stvarnu kontrolu: znam što radi, gdje i zašto. Ali stroj se i dalje nalazi u podatkovnom centru treće strane i, iznad svega, mijenja se tko snosi posljedice. Delegiranjem, ako nešto ne uspije, imate koga kriviti. Samostalnim upravljanjem, najvjerojatnije će krivnja biti vaša.

Imati to na vlastitom računalu. To je opcija o kojoj gotovo nitko ne govori, a ona je srce ove Bilježnice. Ne treba vam ogroman poslužitelj koji radi dvadeset i četiri sata dnevno unutar makro podatkovnom centra za udomljavanje vaših stvari. Vaše uredsko računalo već je poslužitelj: ono poslužuje vas. Ostavite ga uključenog u uredu i povezujete se s njim s prijenosnog računala kod klijenta ili s mobitela kada ste kod kuće. Zovemo ga «uredsko računalo», ne «poslužitelj», ali ono radi točno isto što i prethodne dvije opcije. Kontrola je maksimalna, kao i blizina: vaši podaci su tamo gdje ste i vi. Druga strana, rečeno bez ukrasa, jest da je i odgovornost maksimalna. Ako nestane struje, u Nürnbergu nema dežurnog tehničara: na vama je da podignete osigurač. A da bi to računalo bilo dostupno izvana, potrebno je nešto što gradi most između vašeg prijenosnog računala i njega. To nije magija i dobro je to znati prije odabira ovog puta.

I nije čak ni potrebno ponovno iskoristiti uredsko računalo: postoji uređaj osmišljen upravo za ovo, NAS (proizvode ih Synology, QNAP i drugi). Kao i gotovo sve što smo vidjeli u ovim Cuadernos, iznutra nema magije: to je specijalizirano računalo, ista vrsta stroja koju biste iznajmili u podatkovnom centru, samo izrađeno za pohranu podataka i njihovo posluživanje preko mreže, bez monitora i tipkovnice između. Priključite na njega zaslon i tipkovnicu i imate obično računalo; instalirajte odgovarajući softver na svoje računalo i imate NAS. Razlika je u tome što NAS dolazi već spreman za upotrebu. Kupite ga, priključite kod kuće ili u uredu, i vaš je. Ne plaćate mjesečnu pretplatu; platite jednom i pripada vam, kao i svaki drugi alat vašeg poslovanja. Uključite ga, isključite ga, odnesete ga drugamo ako želite. A budući da je vaš, ništa vas ne sprječava da imate dva —jedan kod kuće, jedan u uredu— ili tri, dodajući jedan na sigurnom mjestu, međusobno sinkronizirane: vaša vlastita redundancija, bez ovisnosti o tome da je održava treća strana. Samostalno hostiranje, na kraju, nije jedna stvar: to je kombinacija strojeva, vlasništva, lokacija i softvera.

Tu je neizbježno imenovati ono što radimo, i radimo to bez krinke: u Solo2 taj most postavlja sama aplikacija. Računalo u tvojem uredu ostaje dostupno samo tvojim pouzdanim uređajima, i uvijek pod enkripcijom, a tvoji se ostali uređaji sami povezuju s njim. Kad klijent razgovara s tobom, tvoje računalo — ne ono trećega — razgovara s klijentom. Ne rješavamo nestanak struje; rješavamo most. I nismo jedini: za gotovo svaku potrebu

danas postoje programi — slobodni ili vlasnički — koji omogućuju upravo to, imati podatke na svojem uređaju i dolaziti do njih izvana. Naše je primjer; bitna je ideja, ne marka.

Redundantnost nije supermoć

Ovdje se javlja trenutni prigovor, i on je razuman: ako imam sve na svom uredskom računalu, što se događa ako se pokvari? Pitanje je dobro. Odgovor je da je sigurnosna mreža koju zamišljamo kod velikih pružatelja usluga skromnija —i lakša za oponašanje— nego što se čini.

Kada ostavim svoje podatke u podatkovnom centru multinacionalne kompanije, vjerujem da ona ima kopije na nekoliko mjesta. I vjerojatno ih ima: na drugoj lokaciji, možda na trećoj. Ali ta redundantnost nije beskonačna i, iznad svega, nije moja: to ostaje tvrdi disk kojeg nisam vlasnik, kojim upravlja netko u koga polažem vjeru koju gotovo nikada ne provjeravam.

Tu istu mrežu mogu isplesti i ja, i to s odlučujućom prednošću. Moja svakodnevna usluga živi na uredskom računalu. Odatle čuvam kriptiranu kopiju na računalu prijateljske tvrtke —kolege u struci, drugog ureda od povjerenja— i drugu kriptiranu kopiju, ako želim, kod istog onog europskog pružatelja usluga o kojem smo govorili. Razlika je u svemu: ono što ostavljam vani nije moja usluga niti moji podaci u čistom obliku, već kriptirana kopija koju samo ja mogu otvoriti. Vanjski pružatelj usluga čuva zatvorenu škrinju za koju nema ključ. Ne povjeravam mu svoje informacije: povjeravam mu neke bajtove koji bez mene ne znače ništa.

Bilo je sigurno dok više nije bilo

Dopustite mi osobu priču, jer ona ovo ilustrira bolje od bilo kojeg argumenta. Više od deset godina bio sam odani klijent CrashPlana, tehnički izvanredne usluge sigurnosnog kopiranja. Sigurnosno sam kopirao u njihov oblak sva svoja računala i računala svoje obitelji —ona od tvrtke i ona od kuće, sve—, s verzijama koje sam mogao oporaviti učestalošću kojom sam želio, putujući natrag kroz vrijeme do određene datoteke od prije nekoliko mjeseci. Nakon prve kopije prenosi samo razlike, kriptirane i komprimirane, tako da sam bez imalo truda održavao ogroman backup ažurnim. Spasilo me mnogo puta, od glupog dokumenta do cijelog diska. Cijena je godinama rasla i bilo mi je svejedno: plaćao sam sretan.

Ono što nisam znao bilo je da je CrashPlan napravio pogrešku u izračunu: ugovorom su obećali neograničenu pohranu, prostorno i vremenski. A prostor pomnožen s vremenom —godine povijesti, verzije svakih nekoliko minuta— raste dok ne postane neodrživo. Jednog dana su nas sve obavijestili da usluga prestaje. Učinili su to elegantno i s izdašnim rokom, gotovo godinu dana, i dali nam sredstva za preuzimanje naših stvari. Ali kamo ide čovjek s više od deset godina verziranih kopija svih svojih diskova? Tu otkrivate da nemate ni načina kako sve preuzeti ni kamo to staviti, a i da možete, novo skladište koštalo bi bogatstvo.

Spasio sam četiri nužne stvari. Ostalo je otišlo kad su ugasili prekidač. Bio sam miran, moje informacije bile su na sigurnom... dok nisu prestale biti. I ne zbog izdaje: CrashPlan se ponio besprijekorno — za razliku od Evernotea, koji se godinama kasnije ponio sramotno —; jednostavno je moj anđeo čuvar u oblaku odlučio, s punim pravom, prestati to biti. Rezultat je za mene bio jednak: ono što sam mislio da je sigurno, nestalo je.

Ono što ova priča uistinu uči ima više veze s ljudskom naravi nego s tehnologijom. Kada netko osjeća da je nešto njegova odgovornost, djeluje preventivno: radi kopije, osigurava se, sumnja s dobrom prosudbom. Kada vjeruje —pogrešno— da odgovornost snosi velika i solventna treća strana, opušta se i pušta stvari da idu svojim tijekom. Taj delegirani mir nije razboritost: to je, bez šminke, oblik neodgovornosti.

Plaćanje nije isto što i pridržavanje pravila

Ta tiha neodgovornost jako nalikuje roditeljima koji upišu sina u najskuplju školu, plate mu nakon toga magisterij i time vjeruju da su ispunili svoju dužnost. Nisu ispunili. Biti roditelj znači brinuti o tome što je danas

naučio, o onome što ne razumije, o njegovim vrijednostima, o njegovom samopouzdanju. Ako u dvadeset i petoj godini taj sin ne zna raditi ili se ponašati, krivnja nije na školi koja je naplatila: ona je na onome tko je delegirao i platio vjerujući da je to dovoljno. Plaćanje trećoj strani ne oslobađa od odgovornosti. Nikada nije.

S podacima je isto, a nedavna povijest to potvrđuje. Prije pedeset ili sto godina profesionalac je čuvao stvari svojih klijenata u fasciklima, u svom uredu ili kod kuće, i osjećao se odgovornim za njih. Rijetko se što gubilo. Prešli smo u digitalni svijet i sa zapanjujućom lakoćom sve postavljamo u „oblak" — koji nije ništa drugo nego računalo jedne multinacionalke — i prestajemo se brinuti. I često se događaju nesreće, postoje tvrtke koje izgube sve, i tada se kaže: kriv je bio Google, kriv je bio Microsoft. Ne. Informacije su tvoje ili tvojih klijenata, ali odgovoran si ti.

Udomljavanje vlastitih stvari nije tehnički hir: to je povratak onog mira od prije nekoliko desetljeća, onoga da znate gdje je svaka stvar i zašto. Zaštita podataka, u međuvremenu, doživjela je nagli zamah klatna —od nepostojanja ikakvog pravila, kada je svatko bez razmišljanja izlagao podatke klijenta, do zahtjeva koji s neproporcionalnom strogošću pada na najmanjeg, slobodnog profesionalca koji dostavljaču daje telefon klijenta. Ne raspravljam o cilju; primjećujem nesrazmjer. Ali nesrazmjer nas ne oslobađa: onoga dana kada administracija bude imala sredstva za praćenje i sankcioniranje u velikim razmjerima, veličina će prestati štititi bilo koga, i mudro je ne čekati taj dan s nesređenom kućom. Imati podatke pod vlastitom kontrolom pomaže u pridržavanju pravila i pomaže u dokazivanju toga. I, nadasve, vraća stvari na svoje mjesto: kada je informacija vaša, odgovornost je u potpunosti vaša —nema treće strane koju biste krivili, niti treće strane čiji bi vas neuspjeh izložio—.

Odgovornost također štiti

Bilo bi nepošteno slikati ovo bez sjena. Zauzeti mjesto posrednika znači nositi njegov teret: održavati ažurne sigurnosne kopije, primjenjivati ažuriranja i pravnu odgovornost — onu prema RGPD-u —, koja u stvarnosti nikad nije sasvim prestala biti tvoja (reference u podnožju navode konkretne članke). Ima posla i ima dan kad nešto zataji u nezgodno vrijeme. Ne skrivamo to.

No strah koji okružuje tu riječ, odgovornost, loše je kalibriran. Mnogo je lakše izgubiti svoje datoteke u usluzi u oblaku koja se zatvori, ili svoje fotografije na Google fotografijama, nego izgubiti onaj fascikl važnih dokumenata koji imaš na vlastitom računalu: onaj za koji znaš gdje je i čiji bi nedostatak primijetio čim bi nestao. Ono što osjećaš svojim, čuvaš; ono što misliš da je na sigurnom u tuđim rukama, zanemaruješ.

Sjeti se nekadašnjih foto albuma, onih od razvijenog papira spremljenih u ladicu. Jesi li ikad čuo nekoga da je „izgubio" svoj obiteljski album? Čuje se za kuću koja je izgorjela s albumom unutra; izgubiti ga tek tako, ne. A nasuprot tome, ljudi koji su imali sve svoje fotografije na Google fotografijama ili na Apple fotografijama i ostali bez ičega: ta se priča vraća svakih nekoliko mjeseci, jer su vjerovali da su na sigurnom. Google fotografije čuvaju tvoje fotografije, dakako; ali ne čuvaju ih kao što roditelji čuvaju album u kojem su njihova djeca i unuci. Tu razliku ne popravlja nijedan podatkovni centar: odgovornost, kad je tvoja, nije samo teret; ona je i najbolje jamstvo.

Četiri pitanja prije odlučivanja

Ako razmišljate o poduzimanju ovog koraka, u bilo kojem njegovom obliku, dobro je prvo odgovoriti na četiri pitanja s nepristranom iskrenošću:

1. Koji bi te dio tvojih podataka boljelo izgubiti ili ne moći ponijeti? I oprez s odbacivanjem onoga „rutinskog": povijest računa djeluje kao najprozaičnija stvar na svijetu dok ne promijeniš program i ne otkriješ da su ti računi bili pružateljevi, ne tvoji — da ih, u najboljem slučaju, možeš ispisati u PDF, ne mogavši više pretraživati po njima —. Nije samo pitanje osjetljivosti: pitanje je kome uistinu pripada ono što trebaš sačuvati.

2. Koja je opcija razmjerna tvojoj stvarnoj tehničkoj sposobnosti? Vlastito dobro održavano računalo na dohvatu je svakomu; administrirati cijeli poslužitelj, ne toliko. Budi iskren prema sebi o tome što znaš, a što ne. I zapamti da između toga da postaviš cijeli poslužitelj i da sve povjeriš postoji vrlo razuman međuprostor: programi — slobodni ili vlasnički — koji čuvaju tvoje podatke na tvojem vlastitom uređaju i daju ti da dolaziš do njih izvana. Za mnogo je ljudi to najbolja ravnoteža.
3. Koji plan imate za najgori dan? Proboj podataka, disk koji umire, pružatelj usluga koji se zatvara, tehničar na bolovanju. Ako plan počinje s „to se ne bi smjelo dogoditi”, to nije plan.
4. Biste li znali dokazati da se pridržavate pravila ako bi vas sutra nadzirali? Činiti to dobro i moći dokazati da to činite dobro nisu isto. Zakon traži ovo drugo.

Ne postoji univerzalni odgovor. Postoji razmjeran odgovor, usvojen s iskrenošću o tome što se dobiva i što se nasljeđuje. I iznad tehnike jedna jednostavna istina: vaši podaci žive u nečijem računalu. Jedino pitanje koje je uistinu važno jest čije računalo želite da to bude.

Samostalno udomljavanje nije ni vrlina ni mana: to je alat s konkretnim učinkom na sposobnosti i odgovornosti. Pitanje nikada nije bilo trebate li udomiti svoje podatke, već koje podatke, kako i uz koju mrežu podrške. Povratak kontrole nad podacima nije povratak u podrum niti nepovjerenje prema svemu: to je povratak osjećaju odgovornosti za ono što je naše, baš kao kad su ti podaci živjeli u mapi na stolu. Ta odgovornost, ispravno shvaćena, prava je usluga koju profesionalac pruža svojim klijentima.

Izvori i dodatno štivo

- Uredba (EU) 2016/679 — članak 28. (izvršitelj obrade), članak 32. (sigurnost obrade), članak 33. (izvješćivanje o povredi sigurnosti), članak 37. (imenovanje službenika za zaštitu podataka).
- Španjolska agencija za zaštitu podataka — *Praktični vodič za analizu rizika u obradi osobnih podataka* (važeća revizija). Okvir za voditelje obrade koji preuzimaju vlastite tehničke funkcije.
- Europski odbor za zaštitu podataka — *Guidelines 1/2024 on processing of personal data based on legitimate interests*. Primjenjivo i za test proporcionalnosti u odlukama o vlastitoj infrastrukturi.
- Europska komisija — javni imenik pružatelja informacijskih usluga s poslovnim nastanom u europskoj nadležnosti. Administrativno polazište za prepoznavanje opcija europskog upravljanog udomljavanja.
- Nextcloud GmbH (Njemačka) — *Nextcloud Enterprise architecture and compliance documentation*. Dokumentirani slučaj slobodnog softvera s modelima samostalnog udomljavanja i upravljanja od strane europskog pružatelja usluga; korisno kao tehnička referenca projekta podržanog u europskoj nadležnosti od 2016.

← Prethodno24 riječi: što je kriptografski identitetSljedeće →Stvarna naspram prividne privatnosti: pitanja koja si trebate postaviti

Nedavna čitanja

- Razmišljanje · 29. lipnja 2026. Nisi anoniman
- Razmišljanje · 27. svibnja 2026. Ono što potpis ne može popraviti
- Analiza · 26. svibnja 2026. Stvarna naspram prividne privatnosti: pitanja koja si trebate postaviti

Ponesite ovaj članak sa sobom gdje god vam zatreba.

↓ Markdown ↓ Obični tekst ↓ PDF

Datoteka će se preuzeti na vaš uređaj. Od tamo je možete spremiti, uvesti u Solo2 ili dijeliti gdje god želite. Cuadernos ne odlučuje o odredištu umjesto vas.

Cuadernos Lacre · Publikacija Menzuri Gestión S.L. ·
napisao R.Eugenio · uredio tim Solo2.