Self-hosting kot profesionalna praksa

Strežnik ni nič drugega kot računalnik. Vprašanje ni, ali bi ga imeli, temveč kje živijo podatki vaših strank, kdo jih vzdržuje in kdo prevzame odgovornost, ko gre kaj narobe.

Da se razumemo: Vaši podatki vedno živijo v nekem računalniku: v tistem od giganta, ki mu vse zaupate, v najetem, ki ga upravljate vi, ali v vašem lastnem. Več nadzora ko želite, več odgovornosti prevzamete. Delegiranje veliki tretji osebi pomirja, vendar ne odvezuje: informacije so vaše —in vaših strank—, odgovorna oseba pa ste vi.

Vprašanje med oblakom in kletjo

Prav je začeti z demistifikacijo besede, ki brez razloga straši: strežnik. Strežnik ni skrivnosten stroj v hlajenem prostoru. Je preprosto računalnik druge osebe —ali vaš lasten—, ki hrani informacije in jih preda tistemu, ki jih zahteva. Desetletja smo podatke naših strank hranili v mapi, v kartotečni omari, na pisarniški mizi in nihče zaradi tega ni izgubljal spanca. Informacije niso bile strašljive, ker so bile na papirju; ni treba, da so strašljive niti zato, ker so na disku.

Tudi «oblak» ni eteričen. Je računalnik nekega podjetja, skoraj vedno daleč in skoraj vedno od nekoga drugega. To sem se nehote naučil tistega dne, ko sem v prepričanju, da so moje datoteke varne na Google Drive, ugotovil, da mapa na mojem računalniku ne vsebuje mojih dokumentov, temveč bližnjice do dokumentov, ki so živeli drugje. Če bi se tisto drugo mesto odločilo zapreti, spremeniti ceno ali preklicati storitev, bi moj mir odšel z njim. Svojih stvari nisem imel v lasti; imel sem dovoljenje za dostop do njih.

Od tod izvira vprašanje tega Zvezka, lažje za izreči kot za odgovoriti: kje naj prebivajo podatki vaših strank? In vaši lastni? Javna razprava ga postavlja, kot da obstajata le dva nasprotujoča si odgovora — oblak velikih platform ali si to urediti sam —, skoraj kot vprašanje tabora. A to nista dve poti: so tri, in nobena ni dejanje vere. Če jih beremo počasi, imajo več odtenkov in zahtevajo več, kot se zdi.

To se tiče vas, ne glede na to, kaj prodajate

Zlahka si mislimo, da je zaupnost stvar odvetnikov, zdravnikov ali novinarjev in da ostali nimajo česa skrivati. To je napaka, in to draga. Skoraj vsako podjetje hrani podatke svojih strank, ki so predmet zakona, in mnogi hranijo, ne da bi vedeli, informacije, ki so veliko bolj občutljive, kot se zdi.

Trgovina s kavči si zapiše ime, naslov in telefon tistega, ki kupuje; če gre za financiranje, tudi njegove ekonomske podatke. Podjetje za prenove ali dekoracijo hrani fotografije notranjosti domov svojih strank in popolne načrte njihovih stanovanj. Čistilno podjetje upravlja z načrti pisarn, ki jih čisti, pogosto označenih z barvami in številkami, ki kažejo, kateri zaposleni vstopa kam, ob kateri uri in s katerim ključem. Nič od tega se ne zdi velika stvar, dokler se človek ne vpraša, za koga drugega bi imelo vrednost: ti čistilni načrti so, gledano z drugimi očmi, popoln zemljevid za tistega, ki bi se rad vlomil krasti.

To, da je podjetje majhno ali da prodaja sedežne garniture namesto obrambe v pravdah, ne pomeni, da so njegovi podatki brez vrednosti ali da zakon zanj neha veljati. Pomeni le to, da lastnik o tem ponavadi manj razmišlja. In

to, da malo razmišljate o nečem, kar je vaša odgovornost, je ravno tista točka, kjer se začnejo težave.

Kje živijo vaši podatki?

Na to vprašanje obstajajo v bistvu trije odgovori. In dobro se je spomniti, da „podatki“ niso le dosje stranke ali sklop računov in predračunov: so tudi vaši pogovori z njo — prek WhatsApp, prek profesionalne klepetalne storitve, prek Solo2 —. Trije odgovori, ki sledijo, niso stopnje čistosti niti lestev od dobrih k slabim: so trije načini, kako razdeliti isto, nadzor in odgovornost.

Vse prepustiti enemu ponudniku. To je najbolj običajno in za večino edino, kar pozna. Dam vse v Google Workspace ali v Microsoft 365 in to v celoti zaupam ponudniku. Plačam svojo naročnino in neham razmišljati o tem. Najbolj skrajna oblika tega so storitve, kjer svojih podatkov sploh nimate: nekateri programi za izstavljanje računov v oblaku vam na primer hranijo račune in predračune — in delujejo zelo dobro —, vendar informacije prebivajo v njihovem sistemu, ne v vašem. Dokler plačujete, dostopate; na dan, ko odidete, odkrijete, da je odnesti lastno zgodovino težko ali nemogoče. Imeti vaše podatke napol kot talca je za marsikaterega ponudnika prav tisto, kar vam preprečuje, da bi odšli h konkurenci. V zameno za udobje izročim nadzor in — ne da bi to rekel naglas — občutek, da odgovornost ni več moja. Sem sodi odtenek, ki se skoraj nikoli ne naredi: prepustiti ni isto kot ameriško. Vse lahko enako udobno prepustim evropskemu ponudniku — na primer Infomaniak — in z enim zamahom rešim dober del dvomov o mednarodnih prenosih, ki smo jih videli pri „Schrems II“, ne da bi karkoli gostil sam. To niso Združene države proti preostalemu vesolju: tudi znotraj čiste prepustitve so že odločitve, ki štejejo.

Najem in upravljanje lastnega strežnika. Imam isto, kar bi mi dal Microsoft ali Google, vendar si to postavim sam. Najamem strežnik pri evropskem ponudniku —Hetzner, OVH, Scaleway—, namestim prosto programsko opremo (na primer Nextcloud za datoteke) in sam upravljam rezultat. Pridobim dejanski nadzor: vem, kaj teče, kje in zakaj. Toda stroj se še vedno nahaja v podatkovnem centru tretje osebe in predvsem se spremeni to, kdo nosi posledice. Z delegiranjem imate ob morebitni napaki koga kriviti. Z lastnim upravljanjem je zelo verjetno, da bo krivda vaša.

Imeti to na lastnem računalniku. To je možnost, o kateri skoraj nihče ne govori, in je srce tega Zvezka. Za gostovanje svojih stvari ne potrebujete ogromnega strežnika, ki bi deloval štiriindvajset ur na dan v makro podatkovnem centru. Vaš pisarniški računalnik je že strežnik: služi vam. Pustite ga vklopljenega v pisarni in se nanj povežete s prenosnika pri stranki ali z mobitela, ko ste doma. Pravimo mu «pisarniški računalnik», ne «strežnik», vendar počne natanko isto kot prejšnji dve možnosti. Nadzor je maksimalen, prav tako bližina: vaši podatki so tam, kjer ste vi. Druga stran, povedana brez olepšav, je, da je tudi odgovornost maksimalna. Če zmanjka elektrike, v Nürnbergu ni dežurnega tehnika: vi ste tisti, ki morate dvigniti varovalko. In da bi bil ta računalnik dostopen od zunaj, je potrebno nekaj, kar zgradi most med vašim prenosnikom in njim. To ni magija in prav je, da to veste, preden izberete to pot.

In niti ni treba znova uporabiti pisarniškega računalnika: obstaja naprava, zasnovana prav za to, NAS (izdelujejo jih Synology, QNAP in drugi). Kot skoraj vse, kar smo videli v teh Cuadernos, znotraj ni nobene čarovnije: gre za specializiran računalnik, isto vrsto stroja, kot bi ga najeli v podatkovnem središču, le da je zasnovan za shranjevanje podatkov in njihovo posredovanje prek omrežja, brez monitorja ali tipkovnice vmes. Priklopite nanj zaslon in tipkovnico in imate običajen računalnik; namestite ustrezno programsko opremo na svoj računalnik in imate NAS. Razlika je v tem, da je NAS že pripravljen za uporabo. Kupite ga, priklopite doma ali v pisarni, in je vaš. Ne plačujete mesečne naročnine; plačate enkrat in je vaš, kot vsako drugo orodje vašega podjetja. Vklopite ga, izklopite ga, odnesete ga drugam, če želite. In ker je vaš, vam nič ne preprečuje, da bi imeli dva —enega doma, enega v pisarni— ali tri, tako da enega dodate na varnem mestu, med seboj sinhronizirane: vaša lastna redundanca, brez odvisnosti od tega, da jo vzdržuje tretja oseba. Samostojno gostovanje navsezadnje ni ena sama stvar: je kombinacija strojev, lastništva, lokacij in programske opreme.

Tu je neizogibno poimenovati, kar počnemo, in to počnemo brez preobleke: v Solo2 ta most postavi sama aplikacija. Računalnik v vaši pisarni ostane dostopen le vašim zaupanja vrednim napravam, in vedno pod šifriranjem, vaše druge naprave pa se nanj povežejo same. Ko se stranka pogovarja z vami, je vaš računalnik —

ne računalnik tretje osebe —, ki se pogovarja s stranko. Ne rešujemo izpada elektrike; rešujemo most. In nismo edini: za skoraj vsako potrebo danes obstajajo programi — prosti ali lastniški —, ki omogočajo prav to, imeti podatke na svoji napravi in priti do njih od zunaj. Naš je primer; pomembna je zamisel, ne znamka.

Redundanca ni supermoč

Tu se pojavi takojšen ugovor, ki je razumen: če imam vse na pisarniškem računalniku, kaj se zgodi, če se pokvari? Vprašanje je dobro. Odgovor je, da je varnostna mreža, ki si jo predstavljamo pri velikih ponudnikih, skromnejša —in lažje posnemljiva—, kot se zdi.

Ko pustim svoje podatke v podatkovnem centru multinacionalke, zaupam, da ima kopije na več mestih. In verjetno jih ima: na drugi lokaciji, morda na tretji. Toda ta redundanca ni neskončna in predvsem ni moja: še vedno ostaja trdi disk, katerega lastnik nisem jaz, upravlja pa ga nekdo, ki mu zaupam na slepo, česar skoraj nikoli ne preverim.

To isto mrežo si lahko spletem sam, in to z odločilno prednostjo. Moja vsakodnevna storitev živi na pisarniškem računalniku. Od tam hranim šifrirano kopijo na računalniku prijateljskega podjetja —kolega v stroki, druge zaupanja vredne pisarne— in še eno šifrirano kopijo, če želim, pri istem evropskem ponudniku, o katerem smo govorili. Razlika je v vsem: tisto, kar pustim zunaj, ni moja storitev niti moji podatki v čisti obliki, temveč šifrirana kopija, ki jo lahko odprem le jaz. Zunanji ponudnik hrani zaprto skrinjo, za katero nima ključa. Ne zaupam mu svojih informacij: zaupam mu nekaj bajtov, ki brez mene ne pomenijo nič.

Bilo je varno, dokler ni več bilo

Dovolite mi osebno zgodbo, saj ta to ponazarja bolje od katerega koli argumenta. Več kot deset let sem bil zvesta stranka CrashPlana, tehnično izjemne storitve za varnostno kopiranje. V njihov oblak sem kopiral vse svoje računalnike in računalnike svoje družine —tiste od podjetja in tiste od doma, vse—, z različicami, ki sem jih lahko obnovil s poljubno pogostostjo, s potovanjem nazaj v času do določene datoteke izpred mesecev. Po prvi kopiji je prenašal le razlike, šifrirane in stisnjene, tako da sem brez večjega truda vzdrževal ogromno varnostno kopijo posodobljeno. Rešilo me je velikokrat, od nepomembnega dokumenta do celotnega diska. Cena se je z leti zviševala in mi je bilo vseeno: plačeval sem z veseljem.

Česar nisem vedel, je bilo to, da je CrashPlan naredil napako v izračunu: s pogodbo so obljubili neomejeno shranjevanje, tako v prostoru kot v času. In prostor, pomnožen s časom —leta zgodovine, različice vsakih nekaj minut— raste, dokler ne postane nevzdržno. Nekega dne so nas vse obvestili, da se storitev končuje. To so storili elegantno in z velikodušnim rokom, skoraj leto dni, ter nam dali sredstva za prenos naših podatkov. Toda kam gre človek z več kot desetletnimi različicami kopij vseh svojih diskov? Tam ugotoviš, da nimaš niti načina, kako bi vse prenesel, niti mesta, kam bi to dal, in da bi tudi če bi lahko, novo skladišče stalo celo premoženje.

Rešil sem štiri nujne stvari. Ostalo je izginilo, ko so izklopili stikalo. Bil sem miren, moje informacije so bile na varnem... dokler niso več bile. In ne zaradi izdaje: CrashPlan se je obnašal brezhibno — za razliko od Evernote, ki se je leta pozneje obnašal sramotno —; preprosto se je moj angel varuh v oblaku odločil, s polno pravico, da to ne bo več. Rezultat je bil zame enak: kar sem mislil, da je varno, je izginilo.

Tisto, kar ta zgodba dejansko uči, ima več opraviti s človeško naravo kot s tehnologijo. Ko nekdo čuti, da je nekaj njegova odgovornost, deluje preventivno: dela kopije, se zavaruje, je sodeč po zdravi pameti sumničav. Ko verjame —napačno—, da odgovornost nosi tretja oseba, velika in plačilno sposobna, se sprosti in pusti stvarem prosto pot. Ta delegirani mir ni previdnost: je, brez ličil, oblika neodgovornosti.

Plačevanje ni isto kot izpolnjevanje obveznosti

Tista tiha neodgovornost je zelo podobna staršem, ki sina vpišejo v najdražjo šolo, mu pozneje plačajo še magisterij in s tem verjamejo, da so izpolnili svojo dolžnost. Niso je. Biti starš pomeni skrbeti za to, kaj se je danes naučil, za tisto, česar ne razume, za njegove vrednote, za njegovo samozavest. Če pri petindvajsetih letih ta sin ne zna delati ali se obnašati, krivda ni na šoli, ki je pobrala denar: je na tistem, ki je delegiral in plačal v prepričanju, da je to dovolj. Plačilo tretji osebi ne odvezuje odgovornosti. Nikoli ni.

S podatki je enako in nedavna zgodovina to potrjuje. Pred petdesetimi ali sto leti je profesionalec hranil reči svojih strank v mapah, v svoji pisarni ali doma, in se zanje čutil odgovornega. Le redko se je kaj izgubilo. Prešli smo v digitalni svet in z osupljivo lahkoto vse naložimo v „oblak“ — ki ni nič drugega kot računalnik neke multinacionalke — in se nehamo skrbeti. In pogosto se zgodijo nesreče, so podjetja, ki izgubijo vse, in potem se reče: kriv je bil Google, kriv je bil Microsoft. Ne. Informacije so vaše ali vaših strank, vendar odgovorni ste vi.

Gostovanje lastnih stvari ni tehnična kaprica: je vrnitev tiste umirjenosti izpred desetletij, tiste, ko veš, kje je vsaka stvar in zakaj. Varstvo podatkov je medtem doživelo sunkovito nihanje —od odsotnosti kakršnega koli pravila, ko je kdor koli brez razmišljanja razkazoval podatke stranke, do zahteve, ki z nesorazmerno strogostjo pade na najmanjšega, na samostojnega podjetnika, ki dostavljavcu da telefonsko številko stranke. Ne oporekam cilju; opažam neskladje. Toda neskladje nas ne odvezuje: tisti dan, ko bo imela uprava sredstva za sledenje in sankcioniranje v velikem obsegu, velikost ne bo več nikogar ščitila, in modro je ne čakati tistega dne z neurejeno hišo. Imeti podatke pod lastnim nadzorom pomaga pri izpolnjevanju obveznosti in pomaga to dokazati. Predvsem pa vrača stvari na svoje mesto: ko so informacije vaše, je odgovornost v celoti vaša —ni tretje osebe, ki bi jo lahko krivili, niti tretje osebe, katere neuspeh bi vas izpostavil—.

Odgovornost tudi ščiti

Bilo bi nepošteno slikati to brez senc. Zasesti mesto posrednika pomeni nositi njegovo breme: vzdrževati ažurne varnostne kopije, nameščati posodobitve in pravno odgovornost — tisto po RGPD —, ki v resnici nikoli ni nehala biti povsem vaša (sklici v nogi natančneje navajajo člene). Je delo in je dan, ko kaj odpove ob neprimernem času. Tega ne skrivamo.

A strah, ki obkroža tisto besedo, odgovornost, je slabo umerjen. Veliko lažje je izgubiti svoje datoteke v oblačni storitvi, ki se zapre, ali svoje fotografije v Googlovih fotografijah, kot izgubiti tisto mapo pomembnih dokumentov, ki jo imate na svojem računalniku: tisto, za katero veste, kje je, in bi opazili, da manjka, takoj ko bi izginila. Kar čutite kot svoje, negujete; kar mislite, da je na varnem v rokah nekoga drugega, zanemarjate.

Pomislite na nekdanje foto albume, tiste iz razvitega papirja, shranjene v predalu. Ste kdaj slišali koga reči, da je „izgubil“ svoj družinski album? Sliši se o hiši, ki je zgorela z albumom v njej; izgubiti ga kar tako, ne. In nasprotno, ljudje, ki so imeli vse svoje fotografije v Googlovih fotografijah ali v Applovih fotografijah in so ostali brez vsega: ta zgodba se vrača vsakih nekaj mesecev, ker so verjeli, da je na varnem. Googlove fotografije skrbijo za vaše fotografije, to že; vendar ne skrbijo zanje, kot starši skrbijo za album, kjer so njihovi otroci in vnuki. Te razlike ne popravi noben podatkovni center: odgovornost, kadar je vaša, ni le breme; je tudi najboljše jamstvo.

Štiri vprašanja pred odločitvijo

Če razmišljate o tem koraku, v kateri koli njegovi obliki, je prav, da najprej brez strasti in pošteno odgovorite na štiri vprašanja:

1. Kateri del vaših podatkov bi vas bolelo izgubiti ali ne moči odnesti? In pazite, da ne zavržete „rutinskega“: zgodovina računov se zdi najbolj prozaična stvar na svetu, dokler ne zamenjate programa in ne odkrijete, da so bili tisti računi ponudnikovi, ne vaši — da jih lahko kvečjemu natisnete v PDF, ne da bi v njih lahko še iskali —. Ni le vprašanje občutljivosti: je vprašanje, komu zares pripada tisto, kar morate ohraniti.
2. Katera možnost je sorazmerna z vašo resnično tehnično sposobnostjo? Lastni dobro vzdrževani računalnik je na dosegu vsakogar; upravljati cel strežnik pa že manj. Bodite iskreni do sebe glede tega, kaj znate in

česa ne. In ne pozabite, da je med postaviti si cel strežnik in vse prepustiti zelo razumno vmesno polje: programi — prosti ali lastniški —, ki hranijo vaše podatke na vaši lastni napravi in vam pustijo, da pridete do njih od zunaj. Za marsikoga je to najboljše ravnovesje.
3. Kakšen načrt imate za najslabši dan? Vdor, disk, ki umre, ponudnik, ki se zapre, tehnik na bolniški. Če se načrt začne s «to se ne bi smelo zgoditi», to ni načrt.
4. Bi znali dokazati, da izpolnjujete pravila, če bi vas jutri pregledali? Delati dobro in znati dokazati, da delaš dobro, nista ista stvar. Zakon zahteva drugo.

Univerzalnega odgovora ni. Obstaja sorazmeren odgovor, sprejet s poštenostjo do tega, kaj se pridobi in kaj se podeduje. In nad tehniko ena preprosta gotovost: vaši podatki živijo v nekem računalniku. Edino vprašanje, ki je resnično pomembno, je, čigav računalnik želite, da to je.

Samostojno gostovanje ni niti vrlina niti hiba: je orodje s konkretnim odtisom zmožnosti in odgovornosti. Vprašanje nikoli ni bilo, ali bi morali gostiti svoje podatke, temveč katere podatke, kako in s kakšno podporno mrežo. Ponovna pridobitev nadzora nad podatki ne pomeni vrnitve v klet ali nezaupanja v vse: je vrnitev k občutku odgovornosti za tisto, kar je naše, tako kot takrat, ko so ti podatki živeli v mapi na mizi. Ta odgovornost, če je pravilno razumljena, je dejanska storitev, ki jo strokovnjak nudi svojim strankam.

Viri in nadaljnje branje

- Uredba (EU) 2016/679 — 28. člen (obdelovalec), 32. člen (varnost obdelave), 33. člen (obveščanje o kršitvi), 37. člen (imenovanje pooblaščene osebe za varstvo podatkov).
- Španska agencija za varstvo podatkov — *Praktični vodnik za analizo tveganj pri obdelavi osebnih podatkov* (veljavna revizija). Okvir za upravljavce, ki prevzamejo lastne tehnične funkcije.
- Evropski odbor za varstvo podatkov — *Guidelines 1/2024 on processing of personal data based on legitimate interests*. Uporabno tudi za preizkus sorazmernosti pri odločitvah o lastni infrastrukturi.
- Evropska komisija — javni imenik ponudnikov informacijskih storitev s sedežem v evropski jurisdikciji. Administrativno izhodišče za prepoznavanje možnosti evropsko upravljanega gostovanja.
- Nextcloud GmbH (Nemčija) — *Nextcloud Enterprise architecture and compliance documentation*. Dokumentiran primer proste programske opreme s samostojno gostovanimi in s strani evropskega ponudnika upravljanimi modalitetami; uporabno kot tehnična referenca projekta, vzdrževanega v evropski jurisdikciji od leta 2016.

← Prejšnji24 besed: kaj je kriptografska identitetaNaslednji →Dejanska vs. navidezna zasebnost: vprašanja, ki si jih je smiselno zastaviti

Zadnja branja

- Razmislek · 29. junij 2026 Nisi anonimen
- Razmislek · 27. maj 2026 Česa podpis ne more popraviti
- Analiza · 26. maj 2026 Dejanska vs. navidezna zasebnost: vprašanja, ki si jih je smiselno zastaviti

Vzemite ta članek s seboj, kamor koli ga potrebujete.

↓ Markdown ↓ Navadno besedilo ↓ PDF

Datoteka bo prenesena v vašo napravo. Od tam jo lahko shranite, uvozite v Solo2 ali delite, kjer koli želite. Cuadernos ne odloča o cilju namesto vas.

Cuadernos Lacre · Publikacija podjetja Menzuri Gestión S.L. ·
napisal R.Eugenio · uredila ekipa Solo2.