

# Self-hosting jako profesionální praxe

Server není nic víc než počítač. Otázka není, zda ho máte mít, ale kde bydlí údaje vašich klientů, kdo je udržuje a kdo nese odpovědnost, když něco selže.

**Abychom si rozuměli:** Vaše data vždy bydlí v něčem počítači: v počítači giganta, kterému vše svěříte, v pronajatém počítači, který spravujete vy, nebo ve vašem vlastním. Čím více kontroly chcete, tím více odpovědnosti přebíráte. Delegování na velkou třetí stranu uklidňuje, ale nezabavuje viny: informace je vaše — a vašich klientů — a odpovědnou osobou jste vy.

## Otázka mezi cloudem a suterénem

Je dobré začít demytizací slova, které bezdůvodně straší: server. Server není tajemný stroj v chlazené místnosti. Je to prostě počítač jiné osoby — nebo váš vlastní — který uchovává informace a předává je tomu, kdo o ně požádá. Desetiletí jsme uchovávali informace našich klientů ve složce, v kartotéce, na kancelářském stole a nikdo kvůli tomu neztrácel spánek. Informace nebyly strašidelné proto, že byly na papíře; nemusí být strašidelné ani proto, že jsou na disku.

Ani „cloud“ není éterický. Je to počítač nějaké firmy, téměř vždy daleko a téměř vždy někoho jiného. Naučil jsem se to neúmyslně v den, kdy jsem v přesvědčení, že mé soubory jsou v bezpečí na Google Drive, zjistil, že složka na mém počítači neobsahovala mé dokumenty, ale zástupce k dokumentům, které žily někde jinde. Pokud by se to jiné místo rozhodlo zavřít, změnit cenu nebo zrušit službu, můj klid by odešel s ním. Nevlastnil jsem své věci; měl jsem povolení k přístupu k nim.

Odtud pramení otázka tohoto Sešitu, snazší na vyslovení než na zodpovězení: kde by měla žít data vašich klientů? A vaše vlastní? Veřejná debata ji předkládá, jako by existovaly jen dvě protichůdné odpovědi — cloud velkých platforem, nebo si to zařídit sám —, skoro jako otázku tábora. Jenže nejsou to dvě cesty: jsou tři, a žádná není aktem víry. Když je čtete pomalu, mají víc odstínů a žádají si víc, než se zdá.

## Týká se to vás, ať prodáváte cokoli

Je snadné si myslet, že důvěrnost je záležitostí právníků, lékařů nebo novinářů a že ostatní nemají co skrývat. Je to chyba, a to drahá. Téměř každá firma uchovává údaje svých klientů podléhající zákonu a mnozí uchovávají, aniž by o tom věděli, informace mnohem citlivější, než se zdá.

Obchod s pohovkami si zapíše jméno, adresu a telefon toho, kdo nakupuje; pokud je v tom financování, pak i jeho ekonomické údaje. Firma na rekonstrukce nebo dekorace uchovává fotografie interiérů domů svých klientů a kompletní plány jejich bydlení. Úklidová firma pracuje s plány kanceláří, které uklízí, často označenými barvami a čísly udávajícími, který zaměstnanec kam vstupuje, v kolik hodin a jakým klíčem. Nic z toho nevypadá jako velká věc, dokud si člověk nepoloží otázku, pro koho dalšího by to mělo cenu: ty úklidové plány jsou, viděno jinýma očima, dokonalou mapou pro toho, kdo se chce vloupat krást.

To, že je firma malá nebo že prodává pohovky namísto obhajoby v soudních sporech, nečiní její údaje bezcennými ani nezpůsobuje, že se na ni přestává vztahovat zákon. Způsobuje to jen to, že její majitel o tom

obvykle méně přemýšlí. A málo přemýšlet o něčem, co je vaší odpovědností, je přesně to místo, kde začínají problémy.

## Kde bydlí vaše data?

Na tu otázku existují v zásadě tři odpovědi. A je dobré připomenout, že „data“ nejsou jen složka klienta nebo blok faktur a rozpočtů: jsou jimi i vaše konverzace s ním — přes WhatsApp, přes profesionální chatovací službu, přes Solo2 —. Tři odpovědi, které následují, nejsou stupně čistoty ani žebřík od dobrých ke špatným: jsou to tři způsoby, jak rozdělit totéž, kontrolu a odpovědnost.

**Svěřit vše jednomu poskytovateli.** To je nejběžnější a pro většinu lidí to jediné, co znají. Dám všechno do Google Workspace nebo do Microsoft 365 a svěřím to celé poskytovateli. Platím svůj poplatek a přestávám na to myslet. Nejkrainější podobou tohoto jsou služby, kde svá data ani nemáte: některé fakturační programy v cloudu vám například uchovávají faktury a rozpočty — a fungují velmi dobře —, ale informace žijí v jejich systému, ne ve vašem. Dokud platíte, máte přístup; v den, kdy odejdete, zjistíte, že odnést si vlastní historii je obtížné nebo nemožné. Mít vaše data napůl jako rukojmí je pro nejednoho poskytovatele právě to, co vám brání odejít ke konkurenci. Výměnou za pohodlí předávám kontrolu a — aniž bych to řekl nahlas — pocit, že odpovědnost už není moje. Sem patří odstín, který se téměř nikdy nedělá: delegovat není totéž co americké. Mohu vše stejně pohodlně svěřit evropskému poskytovateli — třeba Infomaniak — a jedním tahem vyřešit dobrou část pochybností o mezinárodních přenosech, které jsme viděli v „Schrems II“, aniž bych cokoli hostoval sám. Není to Spojené státy proti zbytku vesmíru: i v čisté delegaci jsou rozhodnutí, na kterých záleží.

**Pronajmout si a spravovat vlastní server.** Mám totéž, co by mi dal Microsoft nebo Google, ale postavím si to sám. Pronajmu si server u evropského poskytovatele —Hetzner, OVH, Scaleway— nainstaluji svobodný software (například Nextcloud pro soubory) a sám výsledek spravuji. Získávám skutečnou kontrolu: vím, co běží, kde a proč. Ale stroj se stále nachází v datovém centru třetí strany a především se mění to, kdo nese následky. Delegováním máte v případě selhání koho obviňovat. Při vlastní správě je vysoce pravděpodobné, že chyba bude vaše.

**Mít to na vlastním počítači.** Toto je možnost, o které téměř nikdo nemluví, a je to srdce tohoto Sešitu. Nepotřebujete obrovský server zapnutý čtyřadvacet hodin denně v makro datovém centru, abyste hostovali své věci. Váš kancelářský počítač již je serverem: slouží vám. Necháte ho zapnutý v kanceláři a připojujete se k němu z notebooku u klienta nebo z mobilu, když jste doma. Nazýváme ho „kancelářský počítač“, nikoli „server“, ale dělá přesně totéž, co předchází dvě možnosti. Kontrola je maximální a blízkost také: vaše data jsou tam, kde jste vy. Odvrácenou stranou, řečeno bez příkras, je, že i odpovědnost je maximální. Pokud vypadne elektřina, v Norimberku není žádná služba konající technik: je na vás, abyste nahodili jistič. A aby byl ten počítač přístupný zvenčí, je zapotřebí něco, co vytvoří most mezi vašim notebookem a jím. Není to magie a je dobré to vědět předtím, než si zvolíte tuto cestu.

A není ani potřeba znovu využít kancelářský počítač: existuje zařízení navržené přesně k tomuto účelu, NAS (vyrábějí je Synology, QNAP a další). Jako téměř všechno, co jsme v těchto Cuadernos viděli, uvnitř není žádné kouzlo: je to specializovaný počítač, stejný druh stroje, jaký byste si pronajali v datovém centru, jen určený k ukládání dat a jejich poskytování po síti, bez monitoru a klávesnice mezi tím. Připojte k němu obrazovku a klávesnici a máte běžný počítač; nainstalujte vhodný software do svého PC a máte NAS. Rozdíl je v tom, že NAS přichází připravený k použití. Koupíte jej, zapojíte doma nebo v kanceláři, a je váš. Neplatíte měsíční poplatek; zaplatíte jednou a patří vám, jako kterýkoli jiný nástroj vašeho podnikání. Zapnete jej, vypnete jej, vezmete jej jinam, pokud chcete. A protože je váš, nic vám nebrání mít dva —jeden doma, jeden v kanceláři— nebo tři, přidáním jednoho na bezpečném místě, vzájemně synchronizovaných: vaše vlastní redundance, bez závislosti na tom, že ji udržuje třetí strana. Vlastní hostování nakonec není jediná věc: je to kombinace strojů, vlastnictví, umístění a softwaru.

Tady je nevyhnutelné pojmenovat to, co děláme, a děláme to bez přetvářky: v Solo2 ten most staví sama aplikace. Počítač ve vaší kanceláři zůstává přístupný jen vašim důvěryhodným zařízením, a vždy pod šifrováním, a vaše ostatní přístroje se k němu připojují samy. Když s vámi mluví klient, je to váš počítač — ne počítač třetí

strany —, kdo s klientem mluví. Neřešíme výpadek proudu; řešíme ten most. A nejsme jediní: pro téměř každou potřebu dnes existují programy — svobodné i proprietární —, které umožňují právě tohle, mít data ve svém zařízení a dostat se k nim zvenčí. To naše je příklad; důležitá je myšlenka, ne značka.

## Redundance není superschopnost

Zde vyvstává okamžitá námitka, a je rozumná: pokud mám vše na kancelářském počítači, co se stane, když se porouchá? Otázka je dobrá. Odpověď je, že záchranná síť, kterou si představujeme u velkých poskytovatelů, je skromnější — a snáze napodobitelná —, než se zdá.

Když nechám svá data v datovém centru nadnárodní firmy, důvěřuji, že má kopie na více místech. A pravděpodobně je má: na druhém místě, možná na třetím. Ale tato redundance není nekonečná a především není moje: stále je to pevný disk, jehož nejsem vlastníkem, spravovaný někým, do koho vkládám víru, kterou téměř nikdy neověřuji.

Tuto stejnou síť si mohu utkat sám, a to s rozhodující výhodou. Moje každodenní služba žije na kancelářském počítači. Odtud uchovávám šifrovanou kopii na počítači přátelské firmy — kolegy z profese, jiné důvěryhodné kanceláře — a další šifrovanou kopii, pokud chci, u téhož evropského poskytovatele, o kterém jsme mluvili. Rozdíl je ve všem: to, co nechávám venku, není moje služba ani mé údaje v čitelné formě, ale šifrovaná kopie, kterou mohu otevřít jen já. Externí poskytovatel uchovává zamčenou truhlu, od které nemá klíč. Nesvěřuji mu své informace: svěřuji mu pár bajtů, které beze mě nic neznamenaají.

## Bylo to v bezpečí, dokud nebylo

Dovolte mi osobní příběh, protože ten to ilustruje lépe než jakýkoli argument. Více než deset let jsem byl oddaným klientem CrashPlan, technicky výjimečné služby pro zálohování. Zálohoval jsem do jejich cloudu všechny své počítače i počítače své rodiny — firemní i domácí, všechno — s verzemi, které jsem mohl obnovit s libovolnou frekvencí, přičemž jsem cestoval zpět v čase až ke konkrétnímu souboru z doby před měsíci. Po první kopii přenášel již jen rozdíl, šifrovaně a komprimovaně, takže jsem bez většího úsilí udržoval obrovskou zálohu aktuální. Zachránilo mě to mnohokrát, od banálního dokumentu až po celý disk. Cena v průběhu let stoupala a bylo mi to jedno: platil jsem rád.

Co jsem však nevěděl, bylo, že CrashPlan udělal chybu ve výpočtech: smluvně slíbili neomezené úložiště, v prostoru i čase. A prostor vynásobený časem — roky historie, verze každých pár minut — roste, dokud se nestane neudržitelným. Jednoho dne nám všem oznámili, že služba končí. Udělali to elegantně a s velkorysým termínem, téměř rok, a dali nám prostředky ke stažení našich věcí. Ale kam jde člověk s více než deseti lety verzovaných kopií všech svých disků? Tam zjistíte, že nemáte ani způsob, jak vše stáhnout, ani kam to dát, a že i kdybyste mohli, nový sklad by stál jmění.

Zachránil jsem čtyři nezbytné věci. Zbytek zmizel, když vypnuli vypínač. Byl jsem klidný, mé informace byly v bezpečí... dokud nepřestaly být. A ne kvůli zradě: CrashPlan se zachoval bezvadně — na rozdíl od Evernote, který se o roky později zachoval ostudně —; prostě se můj strážný anděl v cloudu rozhodl, plným právem, jím přestat být. Výsledek byl pro mě totožný: co jsem považoval za jisté, zmizelo.

To, co tento příběh ve skutečnosti učí, má více společného s lidskou povahou než s technologií. Když někdo cítí, že je něco jeho odpovědností, jedná preventivně: dělá kopie, jistí se, je podezřívavý se zdravým úsudkem. Když věří — mylně —, že odpovědnost nese velká a solventní třetí strana, uvolní se a nechá věci plynout. Ten delegovaný klid není obezřetnost: je to, bez příkras, forma nezodpovědnosti.

## Platit neznamená splňovat pravidla

Ta tichá nezodpovědnost se velmi podobá rodičům, kteří zapíší syna do nejdražší školy, zaplatí mu poté magisterské studium a tím věří, že si splnili svou povinnost. Nesplnili. Být rodičem znamená starat se o to, co se dnes naučil, o to, čemu nerozumí, o jeho hodnoty, o jeho sebevědomí. Pokud v pětadvaceti letech ten syn neumí pracovat ani se chovat, chyba není ve škole, která inkasovala peníze: je v tom, kdo delegoval a zaplatil v přesvědčení, že to stačilo. Placení třetí straně nezbavuje odpovědnosti. Nikdy tomu tak nebylo.

S daty je to stejné a nedávná historie to potvrzuje. Před padesáti či sto lety si profesionál ukládal věci svých klientů do složek, ve své kanceláři nebo doma, a cítil se za ně odpovědný. Málokdy se něco ztratilo. Přešli jsme do digitálního světa a s ohromující lehkostí nahráváme všechno do „cloudu“ — což není nic jiného než počítač jedné nadnárodní firmy — a přestáváme se starat. A často dochází k nehodám, jsou firmy, které ztratí všechno, a pak se říká: vina byla na Googlu, vina byla na Microsoftu. Ne. Informace jsou vaše, nebo vašich klientů, ale odpovědný jste vy.

Hostování vlastních věcí není technický rozmar: je to znovuzískání onoho klidu před desítkami let, toho, že víte, kde se každá věc nachází a proč. Ochrana údajů mezitím zažila prudký výkyv kyvadla — od neexistence jakékoli normy, kdy kdokoli bez přemýšlení vystavoval údaje klienta, až po požadavek, který s neúměrnou tvrdostí dopadá na toho nejmenšího, na živnostníka, který dá telefon klienta kurýrovi. Nezpochybňuji cíl; pozoruji nepoměr. Ale nepoměr nás nezbavuje viny: v den, kdy administrativa bude mít prostředky ke sledování a sankcionování ve velkém měřítku, velikost přestane kohokoli chránit a je rozumné nečekat na ten den s neuklizeným domem. Mít údaje pod vlastní kontrolou pomáhá splňovat pravidla a pomáhá to dokázat. A především to vrací věci na své místo: když jsou informace vaše, odpovědnost je plně vaše — neexistuje žádná třetí strana, kterou byste mohli vinit, ani třetí strana, jejíž selhání by vás ohrozilo—.

## Odpovědnost také chrání

Bylo by nepoctivé líčit to bez stínů. Zaujmout místo prostředníka znamená nést jeho břemeno: udržovat aktuální zálohy, instalovat aktualizace a právní odpovědnost — tu podle RGPD —, která ve skutečnosti nikdy nepřestala být tak úplně vaše (odkazy v patičce upřesňují konkrétní články). Je tu práce a je tu den, kdy něco selže v nevhodnou chvíli. Neskrýváme to.

Ale strach, který obklopuje to slovo, odpovědnost, je špatně nastavený. Je mnohem snazší ztratit své soubory ve cloudové službě, která skončí, nebo své fotky v Fotkách Google, než ztratit tu složku důležitých dokumentů, kterou máte ve vlastním počítači: tu, o níž víte, kde je, a u níž byste si všimli, že chybí, jakmile by zmizela. To, co cítíte jako své, opatrujete; to, co považujete za bezpečné v ruce někoho jiného, zanedbáváte.

Vzpomeňte si na dřívější fotoalba, ta z vyvolaného papíru schovaná v zásuvce. Slyšeli jste někdy někoho říct, že „ztratil“ své rodinné album? Slyší se o domě, který shořel i s albem uvnitř; ale ztratit ho jen tak, ne. A naproti tomu lidé, kteří měli všechny své fotky ve Fotkách Google nebo ve Fotkách Apple a zůstali bez ničeho: tahle historka se vrací každých pár měsíců, protože věřili, že je to v bezpečí. Fotky Google se o vaše fotky starají, to ano; ale nestarají se o ně tak, jako se rodiče starají o album, kde jsou jejich děti a vnoučata. Tento rozdíl nespraví žádné datové centrum: odpovědnost, když je vaše, není jen břemeno; je také tou nejlepší zárukou.

## Čtyři otázky před rozhodnutím

Pokud uvažujete o tom, že uděláte tento krok v jakékoli jeho formě, je dobré nejprve bez emocí a upřímně odpovědět na čtyři otázky:

1. Která část vašich dat by vás bolela ztratit, nebo si je nemoci odnést? A pozor na to odbýt jako „rutinní“: historie faktur vypadá jako ta nejprozaičtější věc na světě, dokud nezměníte program a nezjistíte, že ty faktury patřily poskytovateli, ne vám — že si je nanejvýš můžete vytisknout do PDF, aniž byste v nich už mohli vyhledávat —. Není to jen otázka citlivosti: je to otázka toho, komu doopravdy patří to, co potřebujete uchovat.

2. Která možnost je úměrná vaší skutečné technické schopnosti? Vlastní dobře udržovaný počítač je v dosahu každého; spravovat celý server, to už méně. Buďte k sobě upřímní v tom, co umíte a co ne. A pamatujte, že mezi postavit si celý server a svěřit všechno je velmi rozumné mezipole: programy — svobodné i proprietární —, které ukládají vaše data ve vašem vlastním zařízení a nechají vás dostat se k nim zvenčí. Pro mnoho lidí je to nejlepší rovnováha.
3. Jaký máte plán pro nejhorší den? Únik údajů, odcházející disk, končící poskytovatel, technik na neschopence. Pokud plán začíná slovy „to by se nemělo stát“, není to plán.
4. Věděli byste prokázat, že splňujete pravidla, pokud by vás zítra přišli zkontrolovat? Dělat to dobře a vědět dokázat, že to děláte dobře, není totéž. Zákon vyžaduje to druhé.

Neexistuje univerzální odpověď. Existuje přiměřená odpověď, přijatá s upřímností o tom, co se získává a co se dědí. A nad technikou jedna jednoduchá jistota: vaše data žijí v něčím počítači. Jedinou otázkou, na které skutečně záleží, je, koho počítač to má podle vás být.

---

*Samo-hostování není ani ctnost, ani neřest: je to nástroj s konkrétním dopadem na schopnosti a odpovědnost. Otázka nikdy nezněla, zda máte hostovat svá data, ale jaká data, jak a s jakou podpůrnou sítí. Získání kontroly nad údaji neznamena návrat do suterénu ani nedůvěru vůči všemu: je to návrat k pocitu odpovědnosti za to, co je naše, tak jako v době, kdy tato data žila ve složce na stole. Tato odpovědnost, správně pochopená, je skutečnou službou, kterou profesionál poskytuje svým klientům.*

## Zdroje a další čtení

- Nařízení (EU) 2016/679 — článek 28 (zpracovatel), článek 32 (zabezpečení zpracování), článek 33 (ohlašování porušení), článek 37 (jmenování pověřence).
- Španělský úřad pro ochranu osobních údajů (AEPD) — *Praktická příručka pro analýzu rizik při zpracování osobních údajů* (aktuální revize). Rámec pro správce, kteří přebírají vlastní technické funkce.
- Evropský sbor pro ochranu osobních údajů (EDPB) — *Guidelines 1/2024 on processing of personal data based on legitimate interests*. Použitelné i pro test proporcionality při rozhodování o vlastní infrastruktuře.
- Evropská komise — veřejný adresář poskytovatelů informačních služeb se sídlem v evropské jurisdikci. Administrativní výchozí bod pro identifikaci evropských možností spravovaného hostingu.
- Nextcloud GmbH (Německo) — *Nextcloud Enterprise architecture and compliance documentation*. Zdokumentovaný případ svobodného softwaru se samo-hostovanými i spravovanými modely přes evropského poskytovatele; užitečné jako technická reference projektu udržovaného v evropské jurisdikci od roku 2016.

[← Předchozí24 slov: co je to kryptografická identita](#)[Další → Skutečné vs. zdánlivé soukromí: otázky, které je vhodné si položit](#)

## Nedávné čtení

- [Zamyšlení · 29. června 2026 Nejste anonymní](#)
- [Zamyšlení · 27. května 2026 Co podpis nemůže napravit](#)
- [Analýza · 26. května 2026 Skutečné vs. zdánlivé soukromí: otázky, které je vhodné si položit](#)

Vezměte si tento článek tam, kam potřebujete.

[↓ Markdown](#) [↓ Prostý text](#) [↓ PDF](#)

Soubor se stáhne do vašeho zařízení. Odtud si jej můžete uložit, importovat do Solo2 nebo sdílet, kdekoli chcete. Cuadernos za vás o cíli nerozhoduje.

Pečeť · SHA-256 c2e402fde36badf67173565c73c8eff1e931cccdcfbb3ed7c96aaf0ceabc16db

[Funkce](#) [Novinky](#) [Blog](#) [Nápověda](#) [O nás](#) [Kontakt](#)

Cuadernos Lacre · Publikace [Menzuri Gestión S.L.](#) ·  
napsal R.Eugenio · rediguje tým [Solo2](#).

Tento web nepoužívá cookies. Vše, co váš prohlížeč načítá, je napsané nebo námi dohlížené a umístěné na našich evropských serverech: anonymní počítadlo návštěv (Umami, vlastní hosting) a minimální nezbytný JavaScript pro výběr jazyka a vaši předvolbu světlého nebo tmavého motivu, která se ukládá ve vašem vlastním zařízení. Žádné zdroje od externích společností, žádné trackery, žádné profilování, žádné sdílení dat. Pokud nás chcete sledovat: [RSS](#).