Аналіз · 25 травня 2026 р.

← Попередній·Наступний →

Self-hosting як професійна практика

Сервер — це не більше ніж комп'ютер. Питання не в тому, чи варто його мати, а в тому, де живуть дані ваших клієнтів, хто їх підтримує і хто несе відповідальність, коли щось йде не так.

Щоб ми розуміли один одного: Ваші дані завжди живуть у чиємусь комп'ютері: у комп'ютері гіганта, якому ви всьому довіряєте, в орендованому комп'ютері, яким керуєте ви, або у вашому власному. Чим більше контролю ви хочете, тим більше відповідальності ви на себе берете. Делегування великій третій стороні заспокоює, але не звільняє від відповідальності: інформація ваша — і ваших клієнтів, — і відповідальна особа — ви.

Питання між хмарою та підвалом

Варто почати з демістифікації слова, яке лякає без причини: сервер. Сервер — це не таємнича машина в охолоджуваній кімнаті. Це просто комп'ютер іншої людини — або ваш власний, — який зберігає інформацію і видає її тому, хто її запитує. Десятиліттями ми зберігали інформацію наших клієнтів у папках, у картотеках, на робочому столі, і ніхто не втрачав через це сон. Інформація не була лякаючою, тому що вона була на папері; вона не має бути лякаючою і тому, що вона на диску.

«Хмара» теж не є чимось ефірним. Це комп'ютер компанії, який майже завжди знаходиться далеко і майже завжди належить комусь іншому. Я дізнався про це мимоволі того дня, коли, будучи впевненим, що мої файли в безпеці в Google Drive, виявив, що папка на моєму комп'ютері містила не мої документи, а ярлики до документів, які жили в іншому місці. Якби те інше місце вирішило закритися, змінити ціну або скасувати підписку, мій спокій зник би разом із ним. Я не володів своїми речами; у мене був дозвіл на доступ до них.

Звідси народжується питання цього Cuaderno, яке простіше сформулювати, ніж відповісти на нього: де мають жити дані ваших клієнтів? А ваші власні? Публічне обговорення ставить його так, ніби є лише дві протилежні відповіді — хмара великих платформ або зробити все самому, — майже як питання вибору табору. Але шляхів не два: їх три, і жоден із них не є актом віри. Якщо вчитатися в них неквапливо, у них більше нюансів, і вони вимагають більшого, ніж здається.

Це стосується вас, що б ви не продавали

Легко думати, що конфіденційність — це справа адвокатів, лікарів чи журналістів, а іншим нічого приховувати. Це помилка, і дорога. Майже будь-який бізнес зберігає дані своїх клієнтів, що підпадають під дію закону, і багато хто зберігає, самі того не знаючи, інформацію набагато конфіденційнішу, ніж здається.

Магазин диванів записує ім’я, адресу й телефон покупця; якщо є розстрочка — то й його фінансові дані. Фірма з ремонту чи дизайну інтер’єрів зберігає фотографії внутрішніх приміщень будинків своїх клієнтів і повні плани їхніх осель. Клінінгова компанія працює з планами офісів, які вона прибирає, часто розмічених кольорами й цифрами, що вказують, який працівник куди заходить, о котрій годині та з яким ключем. Ніщо з цього не здається чимось серйозним, доки не запитаєш себе, для кого ще це могло б мати

цінність: ці плани прибирання, якщо поглянути на них іншими очима, — ідеальна карта для того, хто захоче проникнути всередину, щоб украсти.

Те, що бізнес малий чи продає дивани замість захисту інтересів у суді, не робить його дані менш цінними і не змушує закон перестати до нього застосовуватися. Це лише призводить до того, що його власник схильний менше про це думати. А менше думати про те, що є вашою відповідальністю, — це якраз те місце, де починаються проблеми.

Де живуть ваші дані?

На це питання є, по суті, три відповіді. І варто пам’ятати, що «дані» — це не лише досьє клієнта чи блок рахунків і кошторисів: це ще й ваші розмови з ним — через WhatsApp, через професійний чат-сервіс, через Solo2. Три відповіді, що йдуть нижче, — це не ступені чистоти й не сходи від добрих до поганих: це три способи розподілити те саме — контроль і відповідальність.

Передати все провайдерові. Це найпоширеніший варіант, і для більшості — єдиний, який вони знають. Поміщаю все в Google Workspace або в Microsoft 365 і цілком довіряю це провайдерові. Плачу свій внесок і перестаю про це думати. Найкрайніша форма цього — сервіси, де ви навіть не отримуєте доступу до своїх даних: деякі хмарні програми для виставлення рахунків, наприклад, зберігають ваші рахунки й кошториси — і працюють дуже добре, — але інформація живе в їхній системі, а не у вашій. Поки платите — у вас є доступ; того дня, коли ви йдете, ви виявляєте, що забрати власну історію важко або неможливо. Тримати ваші дані напівзаручниками для іншого провайдера — це якраз те, що заважає вам піти до конкурента. В обмін на зручність я віддаю контроль і — не кажучи про це вголос — відчуття, що відповідальність уже не моя. Тут доречний нюанс, який майже ніколи не роблять: делегувати не означає американське. Я можу так само зручно передати все європейському провайдерові — наприклад, Infomaniak — і одним махом зняти більшу частину сумнівів щодо міжнародних передач даних, які ми бачили в «Schrems II», нічого не розміщуючи в себе. Це не Сполучені Штати проти всього іншого всесвіту: усередині чистого делегування вже є рішення, які важливі.

Орендувати та керувати власним сервером. У мене є те саме, що дали б мені Microsoft або Google, але я налаштовую це сам. Я орендую сервер у європейського провайдера — Hetzner, OVH, Scaleway, — встановлюю вільне ПЗ (наприклад, Nextcloud для файлів) і сам адмініструю результат. Я отримую реальний контроль: я знаю, що запущено, де і чому. Але машина все одно перебуває в дата-центрі третьої сторони і, перш за все, змінюється той, хто несе наслідки. При делегуванні, якщо щось піде не так, вам є кого звинуватити. При самостійному керуванні, швидше за все, вина буде вашою.

Зберігати на власному комп'ютері. Це варіант, про який майже ніхто не розповідає, і це серце цього зошита. Вам не потрібен величезний сервер, що працює цілодобово всередині макро-дата-центру, щоб хостити свої дані. Ваш офісний комп'ютер — це вже сервер: він обслуговує вас. Ви залишаєте його увімкненим в офісі та підключаєтеся до нього з ноутбука у клієнта або з мобільного телефону, коли ви вдома. Ми називаємо його «офісним комп'ютером», а не «сервером», але він робить рівно те саме, що і два попередні варіанти. Контроль максимальний, як і близькість: ваші дані знаходяться там само, де і ви. Зворотний бік, якщо говорити без прикрас, полягає в тому, що відповідальність також максимальна. Якщо зникне електрика, у Нюрнберзі немає чергового техніка: ви самі повинні увімкнути рубильник. І для того, щоб цей комп'ютер був доступний ззовні, потрібно щось, що налагодить міст між вашим ноутбуком і ним. Це не магія, і про це варто знати, перш ніж вибирати цей шлях.

І навіть не потрібно пристосовувати офісний комп’ютер: існує пристрій, придуманий саме для цього, — NAS (його випускають Synology, QNAP та інші). Як і майже все, що ми бачили в цих Cuadernos, усередині нього немає жодного чаклунства: це спеціалізований комп’ютер, та сама машина, яку ви орендували б у центрі обробки даних, тільки розрахована на те, щоб зберігати дані й віддавати їх мережею, без монітора та клавіатури. Під’єднайте до нього екран і клавіатуру — і ви маєте звичайний комп’ютер; установіть відповідне програмне забезпечення на свій ПК — і ви маєте NAS. Різниця в тому, що NAS уже надходить готовим до роботи. Ви купуєте його, вмикаєте вдома чи в офісі, і він ваш. Ви не

платите щомісячну плату; ви платите один раз, і він належить вам, як будь-який інший інструмент вашої справи. Ви його вмикаєте, вимикаєте, за бажання везете в інше місце. А оскільки він ваш, ніщо не заважає мати два —один удома, інший в офісі— або три, додавши ще один у надійному місці, синхронізовані між собою: ваше власне резервування, не залежачи від того, що його підтримує хтось третій. Самостійний хостинг, зрештою, — це не одна річ: це поєднання обладнання, власності, місць розташування та програмного забезпечення.

Тут неминуче назвати те, що робимо ми, і робимо це без прикрас: у Solo2 цей міст наводить сам застосунок. Комп’ютер у вашому офісі залишається доступним лише для ваших довірених пристроїв і завжди під шифруванням, а решта ваших пристроїв перепідключаються до нього самі. Коли клієнт спілкується з вами, саме ваш комп’ютер — а не чужий — розмовляє з клієнтом. Ми не розв’язуємо проблему вимкнення електрики; ми розв’язуємо проблему моста. І ми не єдині: майже під кожну потребу сьогодні існують програми — вільні або пропрієтарні, — які дозволяють саме це: зберігати дані на вашому обладнанні й діставатися до них іззовні. Наше — це приклад; важлива ідея, а не марка.

Надмірність — це не суперсила

Тут виникає негайне заперечення, і воно цілком обґрунтоване: якщо у мене все на офісному комп'ютері, що буде, якщо він зламається? Питання хороше. Відповідь полягає в тому, що мережа безпеки, яку ми уявляємо у великих провайдерів, скромніша — і її легше наслідувати, — ніж здається.

Коли я залишаю свої дані в дата-центрі транснаціональної компанії, я вірю, що у неї є копії в декількох місцях. І, ймовірно, вони є: у другому місці, можливо, у третьому. Але ця надмірність не нескінченна і, перш за все, вона не моя: це як і раніше жорсткий диск, власником якого я не є, керований кимось, кому я довіряю на віру, яку майже ніколи не перевіряю.

Цю саму мережу я можу сплести сам, причому з вирішальною перевагою. Мій щоденний сервіс живе на офісному комп'ютері. Звідти я зберігаю зашифровану копію на комп'ютері дружньої компанії — колеги по професії, іншого довіреного офісу — і ще одну зашифровану копію, якщо захочу, у того самого європейського провайдера, про якого ми говорили. Різниця у всьому: те, що я залишаю зовні, — це не мій сервіс і не мої відкриті дані, а зашифрована копія, яку можу відкрити тільки я. Зовнішній провайдер зберігає закриту скриню, від якої у нього немає ключа. Я не вверяю йому свою інформацію: я вверяю йому кілька байтів, які без мене нічого не значать.

Це було безпечно, поки не перестало бути таким

Дозвольте мені розповісти особисту історію, тому що вона ілюструє це краще за будь-який аргумент. Понад десять років я був відданим клієнтом CrashPlan — технічно видатного сервісу резервного копіювання. Я робив резервні копії в їхній хмарі для всіх своїх комп'ютерів і комп'ютерів моєї родини — робочих і домашніх, усіх без винятку — з версіями, які я міг відновити з будь-якою бажаною частотою, повертаючись у часі до конкретного файлу багатомісячної давнини. Після першої копії сервіс передавав лише зміни, зашифровані та стиснуті, так що я без особливих зусиль підтримував величезний бекап в актуальному стані. Це рятувало мене багато разів, від дріб'язкового документа до цілого диска. Ціна зростала з роками, і мені було все одно: я платив із задоволенням.

Чого я не знав, так це того, що CrashPlan припустився помилки в розрахунках: за контрактом вони обіцяли необмежене сховище як у просторі, так і в часі. А простір, помножений на час — багаторічна історія, версії кожні кілька хвилин — зростає доти, доки не стає нестійким. Одного разу вони повідомили нам усім, що сервіс припиняє роботу. Вони зробили це елегантно, надавши щедрий термін майже в один рік і давши нам засоби для завантаження наших даних. Але куди йти людині з понад десятирічною історією версійних копій усіх її дисків? Саме тоді виявляється, що у вас немає ні способу завантажити все відразу, ні місця, куди це покласти, і що, навіть якби ви могли, нове сховище коштувало б ціле багатство.

Я врятував чотири необхідні речі. Решта зникла, коли вимкнули рубильник. Я був спокійний, моя інформація була в безпеці... доки не перестала нею бути. І не через зраду: CrashPlan повівся бездоганно — на відміну від Evernote, який роки потому повівся ганебно, — просто мій ангел-охоронець у хмарі вирішив, маючи на те повне право, перестати ним бути. Результат для мене був однаковий: те, що я вважав надійним, зникло.

Те, чому насправді вчить ця історія, більше пов'язане з людською природою, ніж з технологіями. Коли людина відчуває, що щось є її відповідальністю, вона діє превентивно: робить копії, страхується, виявляє здоровий недовір. Коли вона вірить — помилково — що відповідальність несе третя сторона, велика і платоспроможна, вона розслабляється і пускає все на самоплив. Цей делегований спокій не є обачністю: це, без прикрас, форма безвідповідальності.

Платити — не означає дотримуватися правил

Ця тиха безвідповідальність дуже схожа на батьків, які записують сина до найдорожчої школи, оплачують йому потім магістратуру і вірять, що тим самим вони виконали свій обов'язок. Вони не виконали обов'язок. Бути батьком — означає турбуватися про те, що він дізнався сьогодні, про те, чого він не розуміє, про його цінності, про його впевненість у собі. Якщо у двадцять п'ять років цей син не вміє ні працювати, ні поводитися, вина лежить не на школі, яка взяла гроші: вона лежить на тому, хто делегував обов'язки та заплатив, вірячи, що цього достатньо. Оплата послуг третьої сторони не звільняє від відповідальності. Ніколи не звільняла.

З даними відбувається те саме, і нещодавня історія це підтверджує. П’ятдесят чи сто років тому фахівець зберігав дані своїх клієнтів у теках, у себе в кабінеті чи вдома, і почувався відповідальним за них. Рідко що-небудь губилося. Ми перейшли в цифровий світ і з разючою легкістю завантажуємо все в «хмару» — яка є не що інше, як комп’ютер транснаціональної корпорації, — і перестаємо турбуватися. І часто трапляються пригоди, і є фірми, які втрачають усе, і тоді кажуть: винен Google, винен Microsoft. Ні. Інформація ваша, або ваших клієнтів, але відповідальний — ви.

Хостинг власних даних — це не технічний каприз: це повернення того спокою десятирічної давності, знання того, де що знаходиться і чому. Захист даних тим часом відчув різке коливання маятника — від відсутності будь-яких норм, коли будь-хто бездумно виставляв дані клієнта напоказ, до вимоги, яка з непропорційною суворістю лягає на найменших, на самозайнятого, який дає телефон клієнта кур'єру. Я не оспорюю мету; я спостерігаю невідповідність. Але невідповідність не звільняє нас від відповідальності: того дня, коли у адміністрації з'являться засоби для масштабного відстеження та покарання, розмір перестане будь-кого захищати, і розумно не чекати того дня з неприбраним будинком. Наявність даних під власним контролем допомагає дотримуватися правил і допомагає довести це. І перш за все, це повертає речі на свої місця: коли інформація належить вам, відповідальність повністю лежить на вас — немає третьої сторони, яку можна звинуватити, і немає третьої сторони, чий збій підставив би вас під удар.

Відповідальність також захищає

Було б нечесно малювати це без тіней. Зайняти місце посередника означає взяти на себе його клопіт: підтримувати копії в актуальному стані, встановлювати оновлення й нести юридичну відповідальність — відповідальність за RGPD, — яка, насправді, ніколи не переставала бути цілком вашою (посилання у виносках деталізують статті). Є робота, і є день, коли щось ламається невчасно. Ми цього не приховуємо.

Але страх, що оточує це слово, відповідальність, відкалібрований неправильно. Набагато легше втратити свої файли в хмарному сервісі, який закривається, або свої фотографії в Google Фото, ніж втратити ту теку з важливими документами, що лежить на вашому власному комп’ютері: ту, про яку ви знаєте, де вона, і чиє зникнення ви б помітили, щойно вона пропаде. Те, що ви відчуваєте своїм, ви бережете; те, що вважаєте в безпеці в чужих руках, ви занедбуєте.

Подумайте про фотоальбоми колишніх часів, ті, з проявленими паперовими знімками, що зберігалися в шухляді. Ви хоч раз чули, щоб хтось сказав, що «втратив» свій сімейний альбом? Чути про дім, який згорів разом з альбомом усередині; але просто так втратити — ні. А ось люди, у яких усі фотографії були в Google Фото чи в Apple Фото і які залишилися ні з чим: ця історія повертається кожні кілька місяців, бо вони вірили, що все в безпеці. Google Фото береже ваші фотографії, певна річ; але береже їх не так, як батьки бережуть альбом, де закарбовані їхні діти й онуки. Цю різницю не виправить жоден дата-центр: відповідальність, коли вона ваша, — не лише тягар; це ще й найкраща гарантія.

Чотири питання перед прийняттям рішення

Якщо ви подумуєте про те, щоб зробити цей крок у будь-якій з його форм, варто спочатку безсторонньо і чесно відповісти на чотири питання:

1. Яку частину ваших даних вам було б боляче втратити або не мати змоги забрати? І обережніше з тим, щоб списувати з рахунків «рутинне»: історія рахунків здається найпрозаїчнішою річчю на світі, доки ви не зміните програму й не виявите, що ці рахунки належали провайдерові, а не вам — що ви можете, щонайбільше, роздрукувати їх у PDF, уже не маючи змоги шукати всередині них. Річ не лише в чутливості: річ у тому, кому насправді належить те, що вам потрібно зберегти.
2. Який варіант співмірний із вашими реальними технічними можливостями? Власний, добре доглянутий комп’ютер під силу будь-кому; адмініструвати цілий сервер — уже не так. Будьте чесні в тому, що ви вмієте, а що ні. І пам’ятайте, що між тим, щоб підняти цілий сервер, і тим, щоб передати все, є дуже розумна проміжна територія: програми — вільні або пропрієтарні, — які зберігають ваші дані на вашому власному обладнанні й дозволяють діставатися до них іззовні. Для багатьох людей це найкращий баланс.
3. Який у вас план на найгірший день? Злам, смерть диска, закриття провайдера, технік на лікарняному. Якщо план починається зі слів «цього не повинно статися», це не план.
4. Чи зуміли б ви довести, що дотримуєтеся правил, якби завтра до вас прийшли з перевіркою? Робити добре і мати можливість довести, що робиш добре, — це не одне й те саме. Закон вимагає другого.

Немає універсальної відповіді. Є пропорційна відповідь, прийнята з чесністю щодо того, що купується і що успадковується. І вище за всю техніку — одна проста істина: ваші дані живуть у чиємусь комп'ютері. Єдине питання, яке дійсно важливе: чий це комп'ютер, за вашим бажанням.

Селф-хостинг не є ні чеснотою, ні вадою: це інструмент з конкретним набором можливостей та обов'язків. Питання ніколи не полягало в тому, чи варто хостити свої дані, а в тому, які дані, як і з якою мережею підтримки. Повернення контролю над даними — це не повернення у підвал і не недовіра до всього: це повернення до відчуття відповідальності за те, що належить нам, як це було в ті часи, коли дані зберігалися у папці на столі. Ця відповідальність, при правильному розумінні, і є справжня послуга, яку професіонал надає своїм клієнтам.

Джерела та додаткова література

- Регламент (ЄС) 2016/679 — стаття 28 (обробник), стаття 32 (безпека обробки), стаття 33 (повідомлення про злам), стаття 37 (призначення відповідального за захист даних).
- Іспанське агентство з захисту даних — *Практичний посібник з аналізу ризиків при обробці персональних даних* (діюча редакція). Рамки для контролерів, що приймають на себе власні технічні функції.
- Європейська рада з захисту даних — *Guidelines 1/2024 on processing of personal data based on legitimate interests*. Застосовується також для перевірки пропорційності в рішеннях щодо власної інфраструктури.
- Європейська комісія — публічний довідник постачальників інформаційних послуг, створених у європейській юрисдикції. Адміністративна відправна точка для виявлення європейських варіантів

керованого хостингу.
- Nextcloud GmbH (Німеччина) — *Архітектура Nextcloud Enterprise та документація з відповідності*. Задокументований випадок вільного ПЗ з варіантами селф-хостингу та керування європейським провайдером; корисно як технічний довідник проекту, що підтримується в європейській юрисдикції з 2016 року.

← Попередній24 слова: що таке криптографічна ідентичністьНаступний →Реальна vs уявна конфіденційність: питання, які варто собі поставити

Останні матеріали

- Роздуми · 29 червня 2026 р. Ви не анонімні
- Рефлексія · 27 травня 2026 р. Те, що підпис не може виправити
- Аналіз · 26 травня 2026 р. Реальна vs уявна конфіденційність: питання, які варто собі поставити

Візьміть цю статтю з собою куди завгодно.

↓ Markdown ↓ Звичайний текст ↓ PDF

Файл буде завантажено на ваш пристрій. Звідти ви можете зберегти його, імпортувати в Solo2 або поділитися ним де завгодно. Cuadernos не вирішує місце призначення за вас.

Сургучна печатка · SHA-256 dbd85a7df100099a19e5fde8b70b65460407d89bc75419b8215e5d309dc855b0

Cuadernos Lacre · Видання Menzuri Gestión S.L. ·
автор R.Eugenio · під редакцією команди Solo2.