Self-hosting jako praktyka zawodowa

Serwer to nic innego jak komputer. Pytanie nie brzmi, czy go mieć, ale gdzie mieszkają dane Twoich klientów, kto je utrzymuje i kto ponosi odpowiedzialność, gdy coś zawiedzie.

Abyśmy się zrozumieli: Twoje dane zawsze mieszkają na czyimś komputerze: na komputerze giganta, któremu wszystko powierzasz, na komputerze wynajętym, którym zarządzasz Ty, lub na komputerze Twoim własnym. Im więcej kontroli chcesz, tym więcej odpowiedzialności przejmujesz. Delegowanie zadań dużej stronie trzeciej uspokaja, ale nie zdejmuje odpowiedzialności: informacje są Twoje — i Twoich klientów — a osobą odpowiedzialną jesteś Ty.

Pytanie między chmurą a piwnicą

Warto zacząć od odczarowania słowa, które niepotrzebnie straszy: serwer. Serwer nie jest tajemniczą maszyną w chłodzonym pomieszczeniu. To po prostu komputer innej osoby — lub Twój — który przechowuje informacje i udostępnia je temu, kto o nie poprosi. Przez dziesięciolecia przechowywaliśmy dane naszych klientów w folderach, szafach kartotekowych, na biurkach i nikt nie tracił przez to snu. Informacje nie były przerażające, bo były na papierze; nie muszą być takie tylko dlatego, że są na dysku.

„Chmura” również nie jest eteryczna. To komputer firmy, prawie zawsze daleko i prawie zawsze należący do kogoś innego. Nauczyłem się tego mimowolnie w dniu, w którym będąc pewnym, że moje pliki są bezpieczne na Google Drive, odkryłem, że folder na moim komputer nie zawierał moich dokumentów, lecz skróty do dokumentów znajdujących się gdzie indziej. Gdyby to inne miejsce zdecydowało się na zamknięcie, zmianę ceny lub rezygnację z usługi, mój spokój zniknąłby wraz z nim. Nie posiadałem swoich rzeczy; miałem jedynie pozwolenie na dostęp do nich.

Stąd rodzi się pytanie tego Zeszytu, łatwiejsze do postawienia niż do odpowiedzi: gdzie powinny mieszkać dane twoich klientów? A twoje własne? Publiczna debata stawia je tak, jakby istniały tylko dwie przeciwstawne odpowiedzi — chmura wielkich platform albo zrobienie tego samemu —, niemal jak kwestia obozu. Ale to nie są dwie drogi: są trzy i żadna nie jest aktem wiary. Czytane powoli, mają więcej odcieni i wymagają więcej, niż się wydaje.

To dotyczy Ciebie, niezależnie od tego, co sprzedajesz

Łatwo pomyśleć, że poufność to sprawa prawników, lekarzy czy dziennikarzy, a reszta nie ma nic do ukrycia. To błąd, i to kosztowny. Prawie każda firma przechowuje dane swoich klientów podlegające przepisom prawa, a wiele z nich przechowuje, nie wiedząc o tym, informacje znacznie bardziej wrażliwe, niż mogłoby się wydawać.

Sklep z sofami zapisuje imię, adres i telefon tego, kto kupuje; jeśli jest finansowanie, to także jego dane ekonomiczne. Firma remontowa lub dekoratorska przechowuje zdjęcia wnętrz domów swoich klientów i kompletne plany ich mieszkań. Firma sprzątająca operuje planami biur, które sprząta, często oznaczonymi kolorami i numerami wskazującymi, który pracownik wchodzi gdzie, o której godzinie i jakim kluczem. Nic z tego nie wydaje się wielką rzeczą, dopóki człowiek nie zada sobie pytania, dla kogo jeszcze miałoby to wartość: te plany sprzątania są, widziane innymi oczami, idealną mapą dla kogoś, kto chce się włamać, żeby kraść.

To, że firma jest mała lub sprzedaje sofy zamiast bronić spraw w sądzie, nie sprawia, że jej dane tracą wartość, ani nie powoduje, że prawo przestaje jej dotyczyć. Sprawia jedynie, że jej właściciel ma tendencję do mniejszego myślenia o tym. A brak myślenia o czymś, co jest Twoją odpowiedzialnością, jest dokładnie tym miejscem, w którym zaczynają się problemy.

Gdzie mieszkają Twoje dane?

Na to pytanie istnieją w istocie trzy odpowiedzi. I warto pamiętać, że „dane" to nie tylko teczka klienta czy zbiór faktur i kosztorysów: są nimi również twoje rozmowy z nim — przez WhatsApp, przez profesjonalną usługę czatu, przez Solo2 —. Trzy odpowiedzi, które następują, nie są stopniami czystości ani drabiną od dobrych do złych: to trzy sposoby rozdzielenia tego samego, kontroli i odpowiedzialności.

Powierzyć wszystko jednemu dostawcy. To najczęstsze i dla większości jedyne, co zna. Wkładam wszystko do Google Workspace lub do Microsoft 365 i powierzam to w całości dostawcy. Płacę swój abonament i przestaję o tym myśleć. Najbardziej skrajną formą tego są usługi, w których nawet nie posiadasz swoich danych: niektóre programy do fakturowania w chmurze na przykład przechowują ci faktury i kosztorysy — i działają bardzo dobrze —, ale informacje żyją w ich systemie, nie w twoim. Dopóki płacisz, masz dostęp; w dniu, w którym odchodzisz, odkrywasz, że zabranie własnej historii jest trudne lub niemożliwe. Trzymanie twoich danych na poły jako zakładnika jest dla niejednego dostawcy właśnie tym, co powstrzymuje cię przed odejściem do konkurencji. W zamian za wygodę oddaję kontrolę i — nie mówiąc tego na głos — poczucie, że odpowiedzialność nie jest już moja. Tu mieści się odcień, którego prawie nigdy się nie robi: delegować to nie to samo co amerykańskie. Mogę wszystko równie wygodnie powierzyć europejskiemu dostawcy — na przykład Infomaniak — i jednym pociągnięciem rozwiązać znaczną część wątpliwości co do transferów międzynarodowych, które widzieliśmy w „Schrems II", nie hostując niczego samemu. To nie Stany Zjednoczone przeciwko reszcie wszechświata: nawet w czystym delegowaniu są już decyzje, które mają znaczenie.

Wynajęcie i zarządzanie własnym serwerem. Mam to samo, co dałby mi Microsoft lub Google, ale konfiguruję to sam. Wynajmuję serwer u europejskiego dostawcy — Hetzner, OVH, Scaleway — instaluję wolne oprogramowanie (na przykład Nextcloud do plików) i sam zarządzam rezultatem. Zyskuję rzeczywistą kontrolę: wiem, co działa, gdzie i dlaczego. Ale maszyna nadal znajduje się w centrum danych strony trzeciej i, co najważniejsze, zmienia się to, kto ponosi konsekwencje. Delegując, jeśli coś zawiedzie, masz kogo obwinić. Zarządzając samemu, najprawdopodobniej wina będzie Twoja.

Posiadanie danych na własnym komputerze. To opcja, o której prawie nikt nie opowiada, a jest ona sercem tego zeszytu. Nie potrzebujesz ogromnego serwera włączonego przez dwadzieścia cztery godziny na dobę w makrocentrum danych, aby hostować swoje zasoby. Twój komputer biurowy jest już serwerem: służy Tobie. Zostawiasz go włączonego w biurze i łączysz się z nim z laptopa u klienta lub z telefonu, gdy jesteś w domu. Nazywamy go „komputerem biurowym", nie „serwerem", ale robi on dokładnie to samo, co dwie poprzednie opcje. Kontrola jest maksymalna, podobnie jak bliskość: Twoje dane są tam, gdzie Ty. Drugą stroną, powiedzianą bez upiększeń, jest to, że odpowiedzialność jest również maksymalna. Jeśli zgaśnie światło, w Norymberdze nie ma dyżurnego technika: to Ty musisz włączyć bezpiecznik. A żeby ten komputer był dostępny z zewnątrz, potrzebne jest coś, co przerzuci most między Twoim laptopem a nim. To nie magia i warto o tym wiedzieć przed wyborem tej drogi.

I nie trzeba nawet ponownie wykorzystywać komputera biurowego: istnieje urządzenie zaprojektowane właśnie do tego, NAS (produkowane przez Synology, QNAP i innych). Jak prawie wszystko, co widzieliśmy w tych Cuadernos, w środku nie ma żadnej magii: to wyspecjalizowany komputer, ten sam rodzaj maszyny, jaki wynająłbyś w centrum danych, tylko zbudowany do przechowywania danych i udostępniania ich przez sieć, bez monitora i klawiatury pomiędzy. Podłącz do niego ekran i klawiaturę, a masz zwykły komputer; zainstaluj odpowiednie oprogramowanie na swoim komputerze, a masz NAS. Różnica polega na tym, że NAS jest już gotowy do użycia. Kupujesz go, podłączasz w domu lub w biurze, i jest twój. Nie płacisz miesięcznego abonamentu; płacisz raz i należy do ciebie, jak każde inne narzędzie twojej firmy. Włączasz go, wyłączasz, zabierasz w inne miejsce, jeśli chcesz. A ponieważ jest twój, nic nie stoi na przeszkodzie, żeby mieć dwa —jeden w domu, jeden w biurze— albo trzy, dodając jeden w bezpiecznym miejscu, zsynchronizowane ze sobą: twoja

własna redundancja, bez uzależnienia od tego, że utrzymuje ją osoba trzecia. Samodzielny hosting ostatecznie nie jest jedną rzeczą: to połączenie maszyn, własności, lokalizacji i oprogramowania.

Tu nieuniknione jest nazwanie tego, co robimy, i robimy to bez przebrania: w Solo2 ten most stawia sama aplikacja. Komputer w twoim biurze pozostaje dostępny tylko dla twoich zaufanych urządzeń, i zawsze pod szyfrowaniem, a twoje pozostałe urządzenia same się z nim łączą. Kiedy klient rozmawia z tobą, to twój komputer — nie komputer osoby trzeciej — rozmawia z klientem. Nie rozwiązujemy przerwy w dostawie prądu; rozwiązujemy ten most. I nie jesteśmy jedyni: na niemal każdą potrzebę istnieją dziś programy — wolne lub własnościowe —, które pozwalają właśnie na to, mieć dane na swoim sprzęcie i docierać do nich z zewnątrz. Nasze jest przykładem; ważna jest idea, nie marka.

Redundancja nie jest supermocą

Tutaj pojawia się natychmiastowy sprzeciw, który jest uzasadniony: jeśli mam wszystko na komputerze biurowym, to co się stanie, gdy on się zepsuje? Pytanie jest dobre. Odpowiedź brzmi: siatka bezpieczeństwa, którą wyobrażamy sobie u wielkich dostawców, jest skromniejsza — i łatwiejsza do naśladowania — niż się wydaje.

Kiedy zostawiam swoje dane w centrum danych międzynarodowej korporacji, ufam, że posiada ona kopie w kilku miejscach. I prawdopodobnie je posiada: w drugiej lokalizacji, być może w trzeciej. Ale ta redundancja nie jest nieskończona, a przede wszystkim nie jest moja: to nadal dysk twardy, którego nie jestem właścicielem, zarządzany przez kogoś, komu ufam, a czego prawie nigdy nie weryfikuję.

Tę samą siatkę mogę upleść sam, i to z decydującą przewagą. Moja codzienna usługa znajduje się na komputerze biurowym. Stamtąd przechowuję zaszyfrowaną kopię na komputerze zaprzyjaźnionej firmy — kolegi po fachu, innego zaufanego biura — oraz kolejną zaszyfrowaną kopię, jeśli chcę, u tego samego europejskiego dostawcy, o którym mówiliśmy. Różnica zmienia wszystko: to, co zostawiam na zewnątrz, nie jest moją usługą ani moimi jawnymi danymi, lecz zaszyfrowaną kopią, którą tylko ja mogę otworzyć. Dostawca zewnętrzny przechowuje zamkniętą skrzynię, do której nie ma klucza. Nie powierzam mu swoich informacji: powierzam mu kilka bajtów, które beze mnie nic nie znaczą.

Dane były bezpieczne, dopóki przestały takie być

Pozwolę sobie na osobistą historię, ponieważ ilustruje ona tę kwestię lepiej niż jakikolwiek argument. Przez ponad dziesięć lat byłem oddanym klientem CrashPlan, technicznie niezwykłej usługi kopii zapasowych. Tworzyłem w ich chmurze kopie zapasowe wszystkich moich komputerów i komputerów mojej rodziny — biurowych i domowych, wszystkiego — z wersjami, które mogłem odzyskać z dowolną częstotliwością, cofając się w czasie do konkretnego pliku sprzed miesięcy. Po pierwszej kopii usługa przesyłała tylko zmiany, zaszyfrowane i skompresowane, dzięki czemu bez większego wysiłku utrzymywałem ogromną kopię zapasową w aktualności. Ratowało mnie to wiele razy, od głupiego dokumentu po cały dysk. Cena rosła z biegiem lat i nie dbałem o to: płaciłem z radością.

Czego nie wiedziałem, to fakt, że CrashPlan popełnił błąd w obliczeniach: obiecali w umowie nieograniczone miejsce do przechowywania, zarówno pod względem przestrzeni, jak i czasu. A przestrzeń pomnożona przez czas — lata historii, wersje co kilka minut — rośnie, aż staje się nie do utrzymania. Pewnego dnia poinformowali nas wszystkich, że usługa zostaje zakończona. Zrobili to z klasą i z hojnym terminem, prawie rok, oraz dali nam środki na pobranie naszych danych. Ale dokąd się udać z ponad dziesięcioletnią historią kopii wszystkich swoich dysków? Wtedy odkrywasz, że nie masz ani jak wszystkiego pobrać, ani gdzie tego umieścić, a nawet gdybyś mógł, nowa przestrzeń kosztowałaby majątek.

Uratowałem cztery niezbędne rzeczy. Reszta przepadła, gdy wyłączyli przełącznik. Byłem spokojny, moje informacje były bezpieczne... dopóki nie przestały być. I nie z powodu zdrady: CrashPlan zachował się nienagannie — w przeciwieństwie do Evernote, który lata później zachował się haniebnie —; po prostu mój

anioł stróż w chmurze postanowił, mając pełne prawo, przestać nim być. Wynik był dla mnie identyczny: to, co uważałem za bezpieczne, zniknęło.

To, czego ta historia naprawdę uczy, ma więcej wspólnego z naturą ludzką niż z technologią. Kiedy ktoś czuje, że coś jest jego odpowiedzialnością, działa zapobiegawczo: robi kopie, zabezpiecza się, jest podejrzliwy z zachowaniem zdrowego rozsądku. Kiedy wierzy — błędnie — że odpowiedzialność spoczywa na dużej i wypłacalnej stronie trzeciej, rozluźnia się i pozwala rzeczom się dziać. Ten wydelegowany spokój nie jest roztropnością: jest on, bez makijażu, formą nieodpowiedzialności.

Płacenie nie jest tym samym, co dopełnianie obowiązków

Ta cicha nieodpowiedzialność bardzo przypomina rodziców, którzy zapisują syna do najdroższej szkoły, płacą mu potem za studia magisterskie i wierzą, że tym samym dopełnili swojego obowiązku. Nie dopełnili go. Bycie rodzicem to troska o to, czego się dzisiaj nauczył, czego nie rozumie, o jego wartości, o jego pewność siebie. Jeśli w wieku dwudziestu pięciu lat ten syn nie potrafi pracować ani się zachować, wina nie leży po stronie szkoły, która pobrała pieniądze: leży po stronie tego, kto wydelegował zadania i zapłacił, wierząc, że to wystarczy. Płacenie stronie trzeciej nie zdejmuje odpowiedzialności. Nigdy tego nie robiło.

Z danymi jest tak samo, a niedawna historia to potwierdza. Pięćdziesiąt czy sto lat temu profesjonalista przechowywał rzeczy swoich klientów w teczkach, w swoim gabinecie lub w domu, i czuł się za nie odpowiedzialny. Rzadko coś ginęło. Przeszliśmy do świata cyfrowego i z zadziwiającą łatwością wrzucamy wszystko do „chmury” — która jest niczym innym jak komputerem jakiejś korporacji — i przestajemy się martwić. I często zdarzają się wypadki, są firmy, które tracą wszystko, i wtedy mówi się: winny był Google, winny był Microsoft. Nie. Informacje są twoje albo twoich klientów, ale odpowiedzialny jesteś ty.

Hostowanie własnych danych nie jest technicznym kaprysem: jest to odzyskanie tego spokoju sprzed dziesięcioleci, wiedzy o tym, gdzie co jest i dlaczego. Ochrona danych w międzyczasie przeżyła gwałtowne wychylenie wahadła — od braku jakichkolwiek norm, kiedy ktokolwiek bez zastanowienia eksponował dane klienta, do wymogu, który spada z nieproporcjonalną surowością na najmniejszych, na samozatrudnionego, który podaje telefon klienta kurierowi. Nie kwestionuję celu; zauważam niedopasowanie. Ale niedopasowanie nas nie rozgrzesza: w dniu, w którym administracja będzie miała środki do śledzenia i nakładania sankcji na dużą skalę, wielkość przestanie kogokolwiek chronić i warto nie czekać na ten dzień z nieuporządkowanym domem. Posiadanie danych pod własną kontrolą pomaga zachować zgodność z przepisami i pomaga to udowodnić. A przede wszystkim przywraca rzeczy na swoje miejsce: kiedy informacja jest Twoja, odpowiedzialność jest całkowicie Twoja — nie ma strony trzeciej, którą można by obwinić, ani strony trzeciej, której awaria naraziłaby Cię na ryzyko.

Odpowiedzialność też chroni

Byłoby nieuczciwe malować to bez cieni. Zająć miejsce pośrednika znaczy dźwigać jego brzemię: utrzymywać aktualne kopie zapasowe, stosować aktualizacje i odpowiedzialność prawną — tę z RGPD —, która w istocie nigdy nie przestała być całkowicie twoja (odnośniki u dołu wyszczególniają konkretne artykuły). Jest praca i jest dzień, w którym coś zawodzi w nieodpowiedniej chwili. Nie ukrywamy tego.

Ale strach, który otacza to słowo, odpowiedzialność, jest źle wyważony. Znacznie łatwiej jest stracić swoje pliki w usłudze chmurowej, która się zamyka, lub swoje zdjęcia w Zdjęciach Google, niż stracić tę teczkę ważnych dokumentów, którą masz na własnym komputerze: tę, o której wiesz, gdzie jest, i której brak zauważyłbyś, gdy tylko by zniknęła. To, co czujesz jako swoje, pielęgnujesz; to, co uważasz za bezpieczne w cudzych rękach, zaniedbujesz.

Pomyśl o dawnych albumach ze zdjęciami, tych z wywołanego papieru chowanych w szufladzie. Czy słyszałeś kiedyś, żeby ktoś powiedział, że „zgubił” swój album rodzinny? Słyszy się o domu, który spłonął z albumem w środku; ale stracić go ot tak, nie. A z drugiej strony ludzie, którzy mieli wszystkie swoje zdjęcia w Zdjęciach

Google lub w Zdjęciach Apple i zostali bez niczego: ta historia wraca co kilka miesięcy, bo wierzyli, że są bezpieczne. Zdjęcia Google dbają o twoje zdjęcia, oczywiście; ale nie dbają o nie tak, jak rodzice dbają o album, w którym są ich dzieci i wnuki. Tej różnicy nie naprawi żadne centrum danych: odpowiedzialność, kiedy jest twoja, to nie tylko ciężar; to także najlepsza gwarancja.

Cztery pytania przed podjęciem decyzji

Jeśli rozważasz podjęcie tego kroku w jakiejkolwiek formie, warto najpierw odpowiedzieć na cztery pytania z beznamiętną szczerością:

1. Którą część swoich danych bolałoby cię stracić albo nie móc zabrać? I uważaj z odrzucaniem tego, co „rutynowe”: historia faktur wydaje się najbardziej prozaiczną rzeczą na świecie, dopóki nie zmienisz programu i nie odkryjesz, że te faktury należały do dostawcy, nie do ciebie — że co najwyżej możesz je wydrukować do PDF, nie mogąc już w nich szukać —. To nie tylko kwestia wrażliwości: to kwestia tego, do kogo naprawdę należy to, co potrzebujesz zachować.
2. Która opcja jest proporcjonalna do twojej rzeczywistej zdolności technicznej? Własny, dobrze utrzymany komputer jest w zasięgu każdego; administrowanie całym serwerem już nie tak bardzo. Bądź szczery wobec siebie co do tego, co umiesz, a czego nie. I pamiętaj, że między postawieniem całego serwera a powierzeniem wszystkiego jest bardzo rozsądny obszar pośredni: programy — wolne lub własnościowe —, które przechowują twoje dane na twoim własnym sprzęcie i pozwalają ci docierać do nich z zewnątrz. Dla wielu ludzi to najlepsza równowaga.
3. Jaki masz plan na najgorszy dzień? Wyciek danych, awaria dysku, zamknięcie dostawcy, choroba technika. Jeśli plan zaczyna się od słów „to nie powinno się zdarzyć”, to nie jest to plan.
4. Czy wiedziałbyś, jak udowodnić, że przestrzegasz przepisów, gdybyś jutro został skontrolowany? Robienie tego dobrze a możliwość udowodnienia, że robi się to dobrze, to nie to samo. Prawo wymaga tego drugiego.

Nie ma uniwersalnej odpowiedzi. Istnieje odpowiedź proporcjonalna, przyjęta z uczciwością co do tego, co się zyskuje i jakie obowiązki się dziedziczy. A ponad kwestiami technicznymi stoi jedna prosta prawda: Twoje dane żyją na czyimś komputerze. Jedyne pytanie, które naprawdę ma znaczenie, brzmi: czyim komputerem chcesz, by to było.

Samodzielne hostowanie nie jest ani cnotą, ani wadą: to narzędzie o konkretnym profilu możliwości i odpowiedzialności. Pytanie nigdy nie brzmiało, czy hostować swoje zasoby, ale jakie, jak i z jaką siecią wsparcia. Odzyskanie kontroli nad danymi nie oznacza powrotu do piwnicy ani braku zaufania do wszystkiego: to powrót do poczucia odpowiedzialności za to, co nasze, tak jak wtedy, gdy te dane znajdowały się w folderze na biurku. Ta odpowiedzialność, właściwie rozumiana, jest prawdziwą usługą, którą profesjonalista świadczy swoim klientom.

Źródła i dodatkowa lektura

- Rozporządzenie (UE) 2016/679 — artykuł 28 (podmiot przetwarzający), artykuł 32 (bezpieczeństwo przetwarzania), artykuł 33 (zgłaszanie naruszeń), artykuł 37 (wyznaczenie inspektora ochrony danych).
- Hiszpańska Agencja Ochrony Danych — *Praktyczny przewodnik po analizie ryzyka w przetwarzaniu danych osobowych* (aktualna wersja). Ramy dla administratorów przejmujących własne funkcje techniczne.
- Europejska Rada Ochrony Danych — *Guidelines 1/2024 on processing of personal data based on legitimate interests*. Ma zastosowanie również do badania proporcjonalności w decyzjach dotyczących własnej infrastruktury.
- Komisja Europejska — publiczny wykaz dostawców usług informacyjnych z siedzibą w jurysdykcji europejskiej. Administracyjny punkt wyjścia do identyfikacji europejskich opcji hostingu zarządzanego.

- Nextcloud GmbH (Niemcy) — *Architektura Nextcloud Enterprise i dokumentacja zgodności*. Udokumentowany przypadek wolnego oprogramowania z wariantami samodzielnego hostowania i zarządzania przez europejskiego dostawcę; przydatne jako techniczne odniesienie projektu utrzymywanego w jurysdykcji europejskiej od 2016 roku.

← Poprzedni24 słowa: czym jest tożsamość kryptograficznaNastępny →Prywatność rzeczywista vs pozorna: pytania, które warto sobie zadać

Ostatnie lektury

- Refleksja · 29 czerwca 2026 Nie jesteś anonimowy
- Refleksja · 27 maja 2026 Czego podpis nie może naprawić
- Analiza · 26 maja 2026 Prywatność rzeczywista vs pozorna: pytania, które warto sobie zadać

Zabierz ten artykuł tam, gdzie go potrzebujesz.

↓ Markdown ↓ Zwykły tekst ↓ PDF

Plik zostanie pobrany na Twoje urządzenie. Stamtąd możesz go zapisać, zaimportować do Solo2 lub udostępnić w dowolnym miejscu. Cuadernos nie decyduje o miejscu docelowym za Ciebie.

Pieczęć lakowa · SHA-256 d3c3040d23315ead6b6a163a09a6d638a5a63f76b51d4f8c951095dd8d0ddf9f

Cuadernos Lacre · Publikacja Menzuri Gestión S.L. ·
napisana przez R.Eugenio · redagowana przez zespół Solo2.