Analyse · 25. maj 2026

← Forrige·Næste →

Self-hosting som professionell praksis

En server er intet andet end en computer. Spørgsmålet er ikke, om man skal have en, men hvor kundernes data bor, hvem der vedligeholder dem, og hvem der bærer ansvaret, når noget svigter.

Kort fortalt: Dine data bor altid på nogens computer: på en gigants, som du betror alt til, på en lejet som du selv administrerer, eller på din egen. Jo mere kontrol du ønsker, jo mere ansvar påtager du dig. At delegere til en stor tredjepart beroliger, men fritager ikke: informationen er din —og dine kunders—, og den ansvarlige er dig.

Spørgsmålet mellem skyen og kælderen

Det er godt at starte med at afmystificere et ord, der skræmmer uden grund: server. En server er ikke en mystisk maskine i et kølet rum. Det er slet og ret en anden persons computer —eller din egen— der gemmer information og leverer den til dem, der beder om den. I årtier opbevarede vi vores kunders informationer i en mappe, i et arkivskab, på skrivebordet, og ingen lå søvnløs over det. Information var ikke skræmmende, fordi den var på papir; den behøver heller ikke være det, fordi den er på en disk.

«Skyen» er heller ikke æterisk. Det er en virksomheds computer, næsten altid langt væk og næsten altid en andens. Jeg lærte det utilsigtet den dag, hvor jeg, i tillid til at mine filer var i sikker forvaring i Google Drive, opdagede, at mappen på min computer ikke indeholdt mine dokumenter, men genveje til dokumenter, der boede et andet sted. Hvis det andet sted besluttede at lukke, ændre prisen eller opsige tjenesten, ville min ro være forsvundet med det. Jeg ejede ikke mine ting; jeg havde tilladelse til at få adgang til dem.

Derfra opstår spørgsmålet i dette Hæfte, lettere at formulere end at besvare: hvor bør dine klienters data bo? Og dine egne? Den offentlige samtale stiller det op, som om der kun var to modstridende svar — de store platformes sky eller selv at sætte det op —, nærmest et spørgsmål om hvilken lejr man tilhører. Men det er ikke to veje: det er tre, og ingen af dem er en trosakt. Læst i ro og mag har de flere nuancer og kræver mere, end det ser ud til.

Dette angår dig, uanset hvad du sælger

Det er let at tro, at fortrolighed er noget for advokater, læger eller journalister, og at resten ikke har noget at skjule. Det er en fejl, og en af de dyre. Næsten enhver virksomhed gemmer data om sine kunder, der er omfattet af loven, og mange gemmer, uden at vide det, informationer, der er langt mere følsomme, end det ser ud til.

En sofabutik noterer navn, adresse og telefonnummer på den, der køber; er der finansiering, også vedkommendes økonomiske oplysninger. En renoverings- eller indretningsvirksomhed gemmer billeder af indersiden af sine klienters hjem og de fuldstændige plantegninger af deres boliger. Et rengøringsfirma håndterer plantegningerne over de kontorer, det gør rent, ofte markeret med farver og tal, der angiver, hvilken medarbejder der kommer ind hvor, på hvilket tidspunkt og med hvilken nøgle. Intet af det virker som noget særligt, før man spørger, for hvem det ellers ville have værdi: de rengøringsplaner er, set med andre øjne, det perfekte kort for den, der vil bryde ind og stjæle.

At en virksomhed er lille, eller at den sælger sofaer i stedet for at føre retssager, gør ikke dens data mindre værdifulde eller at loven holder op med at gælde for den. Det gør bare, at ejeren plejer at tænke mindre over det.

Og at tænke lidt over noget, der er dit ansvar, er præcis der, hvor problemerne starter.

Hvor bor dine data?

På det spørgsmål er der i bund og grund tre svar. Og det er værd at huske, at »dataene« ikke kun er en klients dossier eller bunken af fakturaer og tilbud: det er også dine samtaler med ham — via WhatsApp, via en professionel chattjeneste, via Solo2. De tre svar, der følger, er ikke renhedsgrader eller en stige fra gode til onde: de er tre måder at fordele det samme på, kontrollen og ansvaret.

Uddelegere alt til en udbyder. Det er det mest almindelige, og for de fleste er det det eneste, de kender. Jeg lægger alt i Google Workspace eller Microsoft 365 og betror det helt og holdent til udbyderen. Jeg betaler mit abonnement og holder op med at tænke på det. Den mest ekstreme form for dette er de tjenester, hvor du end ikke kommer til at have dine egne data: visse faktureringsprogrammer i skyen gemmer for eksempel dine fakturaer og tilbud — og fungerer rigtig godt —, men informationen lever i deres system, ikke i dit. Så længe du betaler, har du adgang; den dag du forlader dem, opdager du, at det er svært eller umuligt at tage din egen historik med dig. At holde dine data halvt som gidsel er for mere end én udbyder netop det, der forhindrer dig i at gå til konkurrenten. Til gengæld for bekvemmelighed afgiver jeg kontrollen og — uden at sige det højt — fornemmelsen af, at ansvaret ikke længere er mit. Her er der plads til en nuance, som man næsten aldrig gør: at uddelegere er ikke synonymt med amerikansk. Jeg kan uddelegere alt lige så bekvemt til en europæisk udbyder — Infomaniak, for eksempel — og med ét slag løse en stor del af tvivlen om internationale overførsler, som vi så i »Schrems II«, uden at hoste noget selv. Det er ikke USA mod resten af universet: inden for den rene uddelegering er der allerede beslutninger, der betyder noget.

Leje og administrere din egen server. Jeg har det samme, som Microsoft eller Google ville give mig, men jeg sætter det op selv. Jeg lejer en server hos en europæisk udbyder —Hetzner, OVH, Scaleway—, installerer fri software (Nextcloud til filer, for eksempel) og administrerer selv resultatet. Jeg opnår reel kontrol: jeg ved, hvad der kører, hvor og hvorfor. Men maskinen befinder sig stadig i datacenteret hos en tredjepart, og frem for alt ændres det, hvem der bærer konsekvenserne. Ved at delegere har du nogen at klandre, hvis noget går galt. Ved at administrere det selv er det højst sandsynligt, at fejlen er din.

Have det på din egen computer. Dette er den mulighed, som næsten ingen fortæller om, og det er hjertet i dette hæfte. Man behøver ikke en enorm server, der står tændt 24 timer i døgnet i et makro-datacenter for at hoste sine ting. Din kontorcomputer er allerede en server: den tjener dig. Du lader den stå tændt på kontoret, og du kobler dig til den fra din bærbare computer hos en kunde, eller fra mobilen, når du er hjemme. Vi kalder den «kontorcomputeren», ikke «serveren», men den gør præcis det samme som de to foregående muligheder. Kontrollen er maksimal, og det samme er nærheden: dine data er der, hvor du er. Bagsiden, sagt uden omsvøb, er, at ansvaret også er maksimalt. Hvis strømmen går, er der ingen tekniker på vagt i Nürnberg: det er dit job at slå sikringen til. Og for at den computer skal være tilgængelig udefra, kræves der noget, der bygger bro mellem din bærbare computer og den. Det er ikke magi, og det er godt at vide, før man vælger denne vej.

Og du behøver ikke engang at genbruge kontorets computer: der findes en enhed designet netop til dette, NAS'en (fremstillet af Synology, QNAP og andre). Som næsten alt det, vi har set i disse Cuadernos, er der ingen magi indeni: det er en specialiseret computer, samme slags maskine, som du ville leje i et datacenter, blot bygget til at gemme data og servere dem over netværket, uden skærm eller tastatur imellem. Sæt en skærm og et tastatur til den, og du har en almindelig computer; installer den rette software på din pc, og du har en NAS. Forskellen er, at NAS'en kommer klar til brug. Du køber den, du sætter den til derhjemme eller på kontoret, og den er din. Du betaler ikke et månedligt gebyr; du betaler én gang, og den tilhører dig, ligesom ethvert andet redskab i din virksomhed. Du tænder den, slukker den, tager den med et andet sted hen, hvis du vil. Og da den er din, er der intet til hinder for at have to —en derhjemme, en på kontoret— eller tre, ved at tilføje en på et sikkert sted, synkroniseret indbyrdes: din egen redundans, uden at være afhængig af, at en tredjepart vedligeholder den. Selvhosting er i sidste ende ikke én enkelt ting: det er en kombination af maskiner, af ejerskab, af placeringer og af software.

Her er det uundgåeligt at nævne, hvad vi gør, og vi gør det uden forklædning: hos Solo2 er det selve applikationen, der slår den bro. Computeren på dit kontor forbliver kun tilgængelig for dine betroede enheder, og altid under kryptering, og dine øvrige apparater genforbinder til den af sig selv. Når en klient taler med dig, er det din computer — ikke en tredjeparts — der taler med klienten. Vi løser ikke strømafbrydelsen; vi løser broen. Og vi er ikke de eneste: til næsten ethvert behov findes der i dag programmer — frie eller proprietære — der tillader netop dette, at have dataene på dit eget udstyr og nå dem udefra. Vores er et eksempel; det vigtige er idéen, ikke mærket.

Redundans er ikke en superkræft

Her opstår den umiddelbare indvending, og den er rimelig: hvis jeg har alt på kontorcomputeren, hvad sker der så, hvis den går i stykker? Spørgsmålet er godt. Svaret er, at det sikkerhedsnet, vi forestiller os hos de store udbydere, er mere beskedent —og lettere at efterligne— end det ser ud til.

Når jeg efterlader mine data i datacenteret hos en multinationale virksomhed, stoler jeg på, at de har kopier på flere steder. Og sandsynligvis har de det: på en anden lokation, måske på en tredje. Men den redundans er ikke uendelig og frem for alt er den ikke min: det forbliver en harddisk, som jeg ikke ejer, håndteret af en person, som jeg viser en tillid, jeg næsten aldrig verificerer.

Det samme net kan jeg væve selv, og med en afgørende fordel. Min daglige tjeneste bor på kontorcomputeren. Derfra gemmer jeg en krypteret kopi på en venlig virksomheds computer —en kollega i faget, et andet betroet kontor— og en anden krypteret kopi, hvis jeg vil, hos den samme europæiske udbyder, som vi talte om. Forskellen er alt: det, jeg efterlader ude, er ikke min tjeneste eller mine data i klartekst, men en krypteret kopi, som kun jeg kan åbne. Den eksterne udbyder opbevarer en lukket kiste, som vedkommende ikke har nøglen til. Jeg betror ham ikke mine informationer: jeg betror ham nogle bytes, som uden mig ikke betyder noget.

Det var sikkert, indtil det ikke var det længere

Lad mig fortælle en personlig historie, for den illustrerer dette bedre end noget argument. I mere end ti år var jeg en trofast kunde hos CrashPlan, en teknisk set ekstraordinær backup-tjeneste. Jeg sikkerhedskopierede alle mine computere og min families computere —firmaets og hjemmets, alt— i deres sky, med versioner som jeg kunne gendanne med den frekvens, jeg ønskede, og rejse tilbage i tiden til en specifik fil fra måneder før. Efter den første kopi overførte den kun ændringerne, krypteret og komprimeret, så jeg holdt en enorm backup opdateret med næsten ingen indsats. Det reddede mig mange gange, fra et banalt dokument til en hel disk. Prisen steg med årene, og det var mig ligegyldigt: jeg betalte med glæde.

Hvad jeg ikke vidste, var, at CrashPlan havde begået en beregningsfejl: de havde lovet ubegrænset lagring ved kontrakt, både i plads og tid. Og plads multipliceret med tid —år med historik, versioner hvert par minutter— vokser, indtil det bliver uholdbart. En dag meddelte de os alle, at tjenesten ophørte. De gjorde det med elegance og med en generøs frist, næsten et år, og de gav os midler til at downloade vores eget. Men hvor går man hen med mere end ti år med versionerede kopier af alle sine diske? Der opdager man, at man hverken har en måde at downloade alt på eller et sted at gøre af det, og at selvom man kunne, ville det nye lager have kostet en formue.

Jeg reddede fire uundværlige ting. Resten forsvandt, da de slukkede for kontakten. Jeg var rolig, mine oplysninger var i sikkerhed... indtil de holdt op med at være det. Og ikke på grund af et forræderi: CrashPlan opførte sig upåklageligt — i modsætning til Evernote, som år senere opførte sig skammeligt —; ganske enkelt besluttede min skytsengel i skyen, med fuld ret, at holde op med at være det. Resultatet var for mig identisk: det, jeg troede var sikkert, forsvandt.

Det, denne historie virkelig lærer os, har mere med menneskelig natur at gøre end med teknologi. Når man føler, at noget er ens eget ansvar, handler man forebyggende: man tager kopier, sikrer sin ryg, er mistroisk med sund dømmekraft. Når man —fejlagtigt— tror, at ansvaret bæres af en stor og solid tredjepart, slapper man af og lader stå til. Den delegerede ro er ikke klogskab: det er, uden makeup, en form for ansvarsløshed.

At betale er ikke det samme som at overholde regler

Den stille ansvarsløshed ligner meget forældre, der skriver deres søn ind på den dyreste skole, betaler for en kandidatgrad bagefter, og med det tror de, at de har opfyldt deres pligt. De har ikke opfyldt deres pligt. At være forælder er at bekymre sig om, hvad han har lært i dag, om det han ikke forstår, om hans værdier, om hans selvtillid. Hvis den søn som 25-årig ikke ved, hvordan man arbejder eller opfører sig, er skylden ikke skolens, der tog imod pengene: den ligger hos den, der delegerede og betalte i troen på, at det var nok. At betale en tredjepart fritager ikke for ansvar. Det har det aldrig gjort.

Med data forholder det sig ligesådan, og den nyere historie bekræfter det. For halvtreds eller hundrede år siden opbevarede en fagperson sine klienters ting i mapper, på kontoret eller hjemme, og følte sig ansvarlig for dem. Sjældent gik noget tabt. Vi er trådt ind i den digitale verden og uploader, med forbløffende lethed, alt til »skyen« — som ikke er andet end en multinational virksomheds computer — og holder op med at bekymre os. Og ofte sker der uheld, og der er virksomheder, der mister alt, og så siges der: det var Googles skyld, det var Microsofts skyld. Nej. Informationen er din, eller dine klienters, men den ansvarlige er dig.

At hoste sine egne ting er ikke en teknisk lune: det er at genvinde den ro fra årtier tilbage, den ved at vide, hvor hver ting er og hvorfor. Databeskyttelse har i mellemtiden oplevet et brat pendulsving —fra fraværet af enhver norm, da hvem som helst uden eftertanke udstillede en kundes data, til et krav, der falder med uforholdsmæssig hårdhed på den mindste, den selvstændige, der giver en kundes telefonnummer til buddet. Jeg diskuterer ikke målet; jeg observerer misforholdet. Men misforholdet fritager os ikke: den dag myndighederne har midler til at spore og sanktionere i stor skala, vil størrelse holde op med at beskytte nogen, og det er klogt ikke at vente på den dag med et uorganiseret hus. At have dataene under egen kontrol hjælper med at overholde regler og hjælper med at bevise det. Og frem for alt bringer det tingene tilbage på plads: når informationen er din, er ansvaret fuldt ud dit —der findes ingen tredjepart at give skylden, heller ikke en tredjepart hvis fejl eksponerer dig—.

Ansvar beskytter også

Det ville være uærligt at male dette uden skygger. At indtage mellemleddets plads betyder at bære dets byrde: at holde sikkerhedskopier opdaterede, at anvende opdateringer og et juridisk ansvar — RGPD's — som i virkeligheden aldrig helt holdt op med at være dit (henvisningerne i fodnoten beskriver artiklerne). Der er arbejde, og der er en dag, hvor noget svigter på et ubelejligt tidspunkt. Vi skjuler det ikke.

Men frygten, der omgiver det ord, ansvar, er forkert kalibreret. Det er langt lettere at miste dine filer i en skytjeneste, der lukker, eller dine billeder i Google Fotos, end at miste den mappe med vigtige dokumenter, du har på din egen computer: den, du ved, hvor er, og hvis fravær du ville bemærke, så snart den forsvandt. Det, du føler er dit, passer du på; det, du tror er i sikkerhed i en andens hænder, forsømmer du.

Tænk på fortidens fotoalbummer, dem af fremkaldt papir gemt i en skuffe. Har du nogensinde hørt nogen sige, at de »mistede« deres familiealbum? Man hører om huset, der brændte med albummet indeni; bare at miste det sådan, nej. Og til gengæld folk, der havde alle deres billeder i Google Fotos eller i Apple Fotos og stod tilbage med ingenting: den historie vender tilbage hver par måneder, fordi de troede, det var i sikkerhed. Google Fotos passer på dine billeder, ja bestemt; men det passer ikke på dem, som forældre passer på albummet, hvor deres børn og børnebørn er. Den forskel udbedrer intet datacenter: ansvar, når det er dit, er ikke kun en byrde; det er også den bedste garanti.

Fire spørgsmål før du beslutter dig

Hvis du overvejer at tage skridtet, i en hvilken som helst form, er det godt først at svare på fire spørgsmål med nøgtern ærlighed:

1. Hvilken del af dine data ville det gøre ondt at miste, eller ikke at kunne tage med dig? Og pas på med at afvise det »rutineprægede«: fakturahistorikken virker som det mest prosaiske i verden, indtil du skifter

program og opdager, at de fakturaer tilhørte udbyderen, ikke dig — at du i bedste fald kan udskrive dem til PDF uden længere at kunne søge i dem. Det er ikke kun et spørgsmål om følsomhed: det handler om, hvem det, du har brug for at bevare, i virkeligheden tilhører.
2. Hvilken mulighed står i forhold til din reelle tekniske formåen? En velplejet egen computer er inden for enhvers rækkevidde; at administrere en hel server, ikke i samme grad. Vær ærlig om, hvad du kan, og hvad du ikke kan. Og husk, at der mellem at sætte en hel server op og at uddelegere alt findes et meget rimeligt mellemområde: programmer — frie eller proprietære — der gemmer dine data på dit eget udstyr og lader dig nå dem udefra. For mange mennesker er det den bedste balance.
3. Hvilken plan har du for den værste dag? Et databrud, en disk der dør, en udbyder der lukker, teknikeren er sygemeldt. Hvis planen starter med «det burde ikke ske», er det ikke en plan.
4. Ville du vide, hvordan du beviser, at du overholder reglerne, hvis du blev inspiceret i morgen? At gøre det godt og at kunne bevise, at man gør det godt, er ikke det samme. Loven kræver det sidste.

Der findes intet universelt svar. Der findes et proportionelt svar, vedtaget med ærlighed om, hvad der vindes, og hvad der arves. Og hævet over teknikken, en simpel vished: dine data bor på nogens computer. Det eneste spørgsmål, der virkelig betyder noget, er, hvem du ønsker skal eje den computer.

Selvhosting er hverken en dyd eller en last: det er et værktøj med et konkret aftryk af kapaciteter og ansvar. Spørgsmålet var aldrig, om du skulle hoste dine egne data, men hvilke data, hvordan og med hvilket støttenetværk. At genvinde kontrollen over data er ikke at vende tilbage til kælderen eller at mistro alt: det er at vende tilbage til at føle sig ansvarlig for det, der er vores, ligesom dengang de data boede i en mappe på skrivebordet. Det ansvar er, hvis det forstås rigtigt, den reelle service, som en professionel yder sine klienter.

Kilder og yderligere læsning

- Forordning (EU) 2016/679 — artikel 28 (databehandler), artikel 32 (behandlingssikkerhed), artikel 33 (underretning om brud), artikel 37 (udpegning af databeskyttelsesrådgiver).
- Det spanske datatilsyn (AEPD) — *Praktisk guide til risikoanalyse ved behandling af personoplysninger* (nuværende version). Ramme for dataansvarlige, der påtager sig egne tekniske funktioner.
- Det Europæiske Databeskyttelsesråd — *Guidelines 1/2024 on processing of personal data based on legitimate interests*. Gælder også for proportionalitetsvurdering ved beslutninger om egen infrastruktur.
- Europa-Kommissionen — offentlig fortegnelse over udbydere af informationssamfundstjenester etableret i europæisk jurisdiktion. Administrativt udgangspunkt for identifikation af europæiske administrerede hosting-muligheder.
- Nextcloud GmbH (Tyskland) — *Nextcloud Enterprise architecture and compliance documentation*. Dokumenteret tilfælde af fri software med selvhostede og administrerede løsninger via europæisk udbyder; nyttig som teknisk reference for et projekt støttet i europæisk jurisdiktion siden 2016.

← ForrigeDe 24 ord: hvad en kryptografisk identitet erNæste →Reelt vs. tilsyneladende privatliv: De spørgsmål, man bør stille sig selv

Seneste læsning

- Refleksion · 29. juni 2026 Du er ikke anonym
- Refleksion · 27. maj 2026 Hvad en underskrift ikke kan løse
- Analyse · 26. maj 2026 Reelt vs. tilsyneladende privatliv: De spørgsmål, man bør stille sig selv

Tag denne artikel med dig, hvor du har brug for den.

↓ Markdown ↓ Almindelig tekst ↓ PDF

Filen downloades til din enhed. Derfra kan du gemme den, importere den til Solo2 eller dele den, hvor du vil. Cuadernos beslutter ikke destinationen for dig.

Laksegl · SHA-256 f65ba59c36af2280ace52e11a1e8d79a8d214b36e00002352828bf9e7bbb538c

Cuadernos Lacre · En udgivelse fra Menzuri Gestión S.L. ·
skrevet af R.Eugenio · redigeret af holdet bag Solo2.

Dette websted bruger ikke cookies. Alt, hvad din browser indlæser, er skrevet eller overvåget af os og hostet på vores europæiske servere: den anonyme besøgstæller (Umami, selvhostet) og den mindst mulige JavaScript, der er nødvendig for sprogvælgeren og din præference for lyst/mørkt tema, som gemmes på din egen enhed. Ingen ressourcer fra tredjeparter, ingen trackere, ingen profilering, ingen deling af data. Hvis du vil følge os: RSS.