Tajemnica zawodowa w erze cyfrowej

Gdy komunikacja między profesjonalistą a jego klientem odbywa się za pośrednictwem technicznie nieodpowiedniego kanału, tajemnica nie zostaje złamana w dniu wycieku. Została złamana znacznie wcześniej, w momencie wyboru narzędzia.

Problem, którego prawie nikt nie widzi

Prawnik otrzymuje na telefon wrażliwy dokument od klienta. Lekarz omawia z kolegą delikatną diagnozę. Psycholog koordynuje z psychiatrą leczenie pacjenta. Doradca podatkowy przesyła dane deklaracji czekającej na rewizję. Wszyscy robią to przez komunikatory. I prawie nikt nie zatrzymuje się, by pomyśleć, gdzie te wiadomości naprawdę trafiają.

Odpowiedź w większości przypadków jest taka sama: na serwer, którego profesjonalista nie kontroluje, w kraju, którego ustawodawstwa niekoniecznie zna, zarządzany przez firmę, której modelem biznesowym jest – w bezpośrednich kategoriach ekonomicznych – gromadzenie danych. Wiadomość może być szyfrowana w przesyłaniu. Ale gdy trafi na serwer, jest kopią przechowywaną w infrastrukturze osoby trzeciej, podlegającą operacyjnym, prawnym i komercyjnym decyzjom tej osoby trzeciej. Nie profesjonalisty.

Co mówią przepisy

Europejskie Ogólne Rozporządzenie o Ochronie Danych jest jednoznaczne w swoim artykule 32: każdy, kto przetwarza dane osobowe, musi wdrożyć "odpowiednie" środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku. Odpowiedniości środków nie ocenia się według tego, "co aplikacja mówi, że robi", ale według rzeczywistego ryzyka. Jeśli dane klienta trafiają na serwer, którego jurysdykcja nie gwarantuje stopnia ochrony odpowiadającego Europejskiemu Obszarowi Gospodarczemu, administrator danych – czyli profesjonalista – podejmuje ryzyko, z którego prawdopodobnie nie zdaje sobie w pełni sprawy.

I nie chodzi tylko o RODO. Tajemnica zawodowa, uregulowana w sposób szczególny dla prawników, lekarzy, psychologów, audytorów, dziennikarzy i innych, wymaga, aby komunikacja z klientem była poufna. Nie "poufna w miarę możliwości". Poufna bez wyjątków. Jeśli używany kanał techniczny nie może tego zagwarantować, profesjonalista podejmuje ryzyko, na które etyka jego zawodu nie pozwala.

Paradoks polega na tym, że ryzyko jest niewidoczne. Nikt nie audytuje komunikatorów w biurze. Nikt nie prosi o umowę powierzenia przetwarzania danych od dostawcy czatu. Ryzyko ujawnia się dopiero, gdy jest już za późno: wyciek, opublikowane włamanie, nakaz sądowy wykonany na innym kontynencie bez powiadomienia użytkownika.

Czego technicznie potrzebuje profesjonalista

To, czego potrzebuje osoba objęta tajemnicą zawodową, jest w rzeczywistości zaskakująco proste z punktu widzenia wymagań:

- Kanału, w którym wiadomości trafiają bezpośrednio z urządzenia nadawcy na urządzenie odbiorcy, bez przechodzenia przez serwer pośredniczący, który przechowuje kopie.
- Infrastruktury, której jurysdykcja i polityka są zgodne z RODO poprzez konstrukcję, a nie przez deklarację.
- Sposobu identyfikacji z rozmówcą bez konieczności przekazywania osobie trzeciej kontaktów zawodowych (nazwisk klientów, numerów telefonów, książki adresowej).
- Systemu możliwego do zweryfikowania – nie opartego na słowie dostawcy – w celu potwierdzenia, że wiadomość dotarła do właściwej osoby.

To nie jest wygórowana lista. W rzeczywistości jest to to, co było oczywiste w profesjonalnej komunikacji przed-cyfrowej. List polecony spełniał wszystkie te kryteria. Rozmowa telefoniczna z centrali biura do centrali klienta również. Dziwne nie jest to, że te gwarancje są wymagane dzisiaj: dziwne jest to, że zostały utracone przy przejściu na kanał cyfrowy, bez niczyjej uwagi.

Różnica między szyfrowaniem a nie-przechowywaniem

Istnieje użyteczna metafora. Zaszyfrowanie wiadomości i zapisanie jej na serwerze to odpowiednik włożenia dokumentu do sejfu i zostawienia sejfu w domu nieznajomego. Sejf jest dobry. Dokumentu w zasadzie nie da się odczytać. Ale dokument *nadal znajduje się w cudzym domu*. A ten ktoś może otrzymać nakaz sądowy, może paść ofiarą ataku informatycznego, może zmienić warunki świadczenia usług, może zostać kupiony przez inną firmę o innej etyce lub może jutro zniknąć.

Alternatywą strukturalną – nie proceduralną, nie opartą na zaufaniu – jest to, by dokument nigdy nie opuścił biura. By podróżował bezpośrednio z biurka profesjonalisty na biurko klienta, bez żadnego pośrednika. To właśnie robi technicznie komunikacja punkt-punkt między urządzeniami: eliminuje pośrednika. Nie chodzi o to, że pośrednik jest zły. Chodzi o to, że w przypadku tajemnicy zawodowej pośrednik jest *niepotrzebny*. A to, co niepotrzebne, w każdym systemie aspirującym do bycia bezpiecznym, musi zostać wyeliminowane z zasady.

Kwestia odpowiedzialności

W ostatecznym rozrachunku pytanie, na które każdy profesjonalista z obowiązkiem zachowania tajemnicy powinien móc odpowiedzieć stanowczym "tak", brzmi następująco:

> Jeśli jutro wycieknie rozmowa z jednym z moich klientów, a sąd lub izba zawodowa zapyta mnie, jak zarządzam poufnością, czy mogę wykazać technicznie, że kanał, którego użyłem, nie przechowuje kopii w infrastrukturze osób trzecich? Czy mogę udowodnić, że dane nigdy nie opuściły urządzeń dwóch osób biorących udział w rozmowie? Czy mogę udowodnić, nie polegając na słowie firmy z innego kontynentu, że poufność była gwarantowana przez architekturę, a nie przez obietnicę?

Jeśli odpowiedź brzmi nie, problemem nie jest konkretne narzędzie. Problemem jest to, że narzędziu powierzono odpowiedzialność, której narzędzie nie zostało zaprojektowane udźwignąć. To jak wkładanie poufnych akt do przezroczystej koperty i ufanie, że listonosz nie zajrzy.

Narzędzie, które profesjonalista wybiera do komunikacji ze swoimi klientami, mówi wiele o tym, jak ceni ich zaufanie. Istnieją narzędzia zaprojektowane tak, aby to zaufanie nie zależało od obietnic, ale od architektury. I są narzędzia, które takie nie są. Znajomość różnicy jest częścią pracy.

Cytowane ramy prawne

- Rozporządzenie UE 2016/679 (RODO), w szczególności art. 5, 25 (ochrona danych w fazie projektowania) i 32 (bezpieczeństwo przetwarzania).
- Ustawa z dnia 26 maja 1982 r. Prawo o adwokaturze, art. 6 (tajemnica zawodowa).

- Ustawa z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty, art. 40 (obowiązek zachowania tajemnicy lekarskiej).
- Ustawa z dnia 8 czerwca 2001 r. o zawodzie psychologa i samorządzie zawodowym psychologów, art. 14 (obowiązek zachowania tajemnicy zawodowej).

← PoprzedniSzyfrowanie to nie prywatność: co mówią o Tobie metadaneNastępny →RODO i komunikacja profesjonalna: dlaczego większość narusza przepisy nie wiedząc o tym

Ostatnie lektury

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

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 f3f06db3927f87e5a2372e0c72226b4bc80098d4a949fe25150a5ab19ff6c032

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