Bezpieczeństwo danych osobowych: proces, a nie jednorazowa inwestycja

Posted on 2025-06-21

Zgodnie z zasadą *ochrona danych w fazie projektowania*, już na etapie tworzenia aplikacji webowych należy w szczególności minimalizować przetwarzanie danych, stosować silne mechanizmy uwierzytelniania oraz odpowiednią segregację informacji, tak by dostęp do danych był możliwy wyłącznie dla osób uprawnionych.

Żeby wdrożyć tę zasadę, trzeba:

- • w pełni kontrolować uprawnienia użytkowników,
- • szyfrować dane w transmisji i podczas przechowywania oraz
- • cykliczne przeprowadzać audyty i testy penetracyjne.

Dzięki temu możliwe jest wykrycie podatności, zanim zostaną one wykorzystane przez cyberprzestępców.

Bezpieczeństwo danych osobowych: proces, a nie jednorazowa inwestycja

Zaniedbania w ochronie danych osobowych mogą mieć poważne konsekwencje dla użytkowników. Wyciek informacji medycznych może prowadzić do naruszenia prywatności pacjentów, których diagnozy i historia leczenia stają się dostępne dla osób niepowołanych. Takie incydenty mogą skutkować dyskryminacją, utratą zaufania do systemów ochrony zdrowia oraz stresem związanym z dalszym wykorzystywaniem ich danych. Ujawnienie informacji finansowych może natomiast pro-wadzić do oszustw kredytowych czy przejęcia kont bankowych. Dlatego tak istotne jest traktowanie ochrony danych jako fundamentu każdej aplikacji, a nie jako dodatkowej funkcjonalności wdrażanej po fakcie.

Ochrona danych w fazie projektowania to podejście pozwalające budować systemy odporne na za-grożenia, zamiast łatać luki w zabezpieczeniach po ich wykryciu. Organizacje powinny uwzględniać tę zasadę od początku, stosując rozwiązania technologiczne zapewniające maksymalną ochronę danych użytkowników. Wprowadzanie najlepszych praktyk, takich jak np. rekomendacje OWASP (Open Web Application Security Project), systematyczne testowanie zabezpieczeń oraz szczegółowa kontrola dostawców oprogramowania to kluczowe kroki ograniczające ryzyko wycieku danych. Nie chodzi tylko o zgodność z przepisami, ale przede wszystkim o ochronę osób, których życie może zostać dotknięte skutkami takich naruszeń.

Projektowanie aplikacji webowych musi uwzględniać nie tylko funkcjonalność i wygodę użytkowników, ale przede wszystkim ich bezpieczeństwo. Już na etapie analizy ryzyka należy identyfikować znane zagrożenia i podatności, które mogą wpływać na ochronę danych. Takie podatności jak np. IDOR (Insecure Direct Object References), SQL Injection, Cross-Site Scripting (XSS) czy brak odpowiedniej kontroli dostępu powinny być eliminowane na poziomie projektowania i wdrażania aplikacji. Ich skuteczne zabezpieczenie pozwala uniknąć przyszłych incydentów i zapewnia użytkownikom pełną ochronę ich danych.

Jednym z wyjątkowo niebezpiecznych zagrożeń jest wykorzystanie podatności IDOR, ponieważ wykorzystanie jej nie wymaga specjalistycznej wiedzy ani zaawansowanych

umiejętności hakerskich. W wielu przypadkach wystarczy jedynie ręczna modyfikacja identyfikatora w adresie URL, aby uzyskać dostęp do zasobów, które powinny być chronione. Brak odpowiedniej weryfikacji uprawnień sprawia, że podatność ta może być przypadkowo odkrywana przez zwykłych użytkowników, a także celowo wykorzystywana przez cyberprzestępców do nieautoryzowanego dostępu do danych.

W Polsce podatność IDOR była przyczyną kilku incydentów naruszenia prywatności, np. zmiana identyfikatora zamówienia w URL umożliwiała dostęp do faktur innych klientów.

Każdy taki incydent dowodzi, że ochrona danych osobowych musi być integralną częścią procesu projektowania aplikacji webowych, a nie jedynie dodatkowym mechanizmem wdrażanym po fakcie. Bezpieczeństwo musi być wbudowane w system od początku, aby skutecznie minimalizować ryzyko naruszeń i zapewnić pełną kontrolę nad przetwarzanymi informacjami.

Kluczowe znaczenie ma również systematyczne testowanie zabezpieczeń aplikacji webowych, które stanowi podstawę ochrony danych osobowych. Brak odpowiednich procedur weryfikacji może nara-zić użytkowników na nieuprawniony dostęp, manipulację lub wykorzystanie ich danych przez osoby trzecie. To może prowadzić do oszustw finansowych, kradzieży tożsamości czy ujawnienia informacji zdrowotnych, bezpośrednio wpływając na ich prywatność i bezpieczeństwo. Dbanie o ciągłe monito-rowanie zagrożeń oraz przeprowadzanie audytów i testów penetracyjnych nie tylko minimalizuje ry-zyko, ale zapewnia użytkownikom realne poczucie kontroli nad ich danymi.

Cyberprzestępcy mogą wykorzystywać przejęte informacje do oszustw, szantażu czy uzyskania dostępu do kredytów i świadczeń zdrowotnych. Jednym z podstawowych sposobów zapobiegania takim incydentom jest stosowanie najlepszych praktyk bezpieczeństwa, a jednym z najbardziej cenionych źródeł rekomendacji w tej dziedzinie jest OWASP (Open Worldwide Application Security Project). Jedno z kluczowych źródeł najlepszych praktyk dotyczących autoryzacji w aplikacjach internetowych – OWASP

Authorization Cheat Sheet podkreśla, że każda operacja związana z autoryzacją powinna być weryfikowana po stronie serwera, a dostęp do danych musi być ograniczony zgodnie z zasadą najmniejszych uprawnień.

Skuteczna ochrona aplikacji webowych wymaga także innych mechanizmów zabezpieczeń, takich jak:

- • Regularne testy penetracyjne – aplikacje powinny być testowane nie tylko przed wdrożeniem, ale również okresowo oraz po każdej większej aktualizacji, co pozwala na wykrycie nowych podatności
  i ich eliminację.
- • Tokenizacja danych – zamiast przewidywalnych identyfikatorów warto stosować losowe tokeny dostępowe, które są trudne do odgadnięcia i dodatkowo zabezpieczone warstwą autoryzacji.
- • Monitorowanie i logowanie incydentów – rejestrowanie prób nieautoryzowanego dostępu umożli-wia wykrycie podejrzanych aktywności i reakcję, zanim dojdzie do większych szkód.
- • Szyfrowanie danych w spoczynku i w tranzycie – nawet jeśli informacje zostaną przechwycone, ich zaszyfrowanie znacząco utrudnia ich odczytanie przez osoby niepowołane.