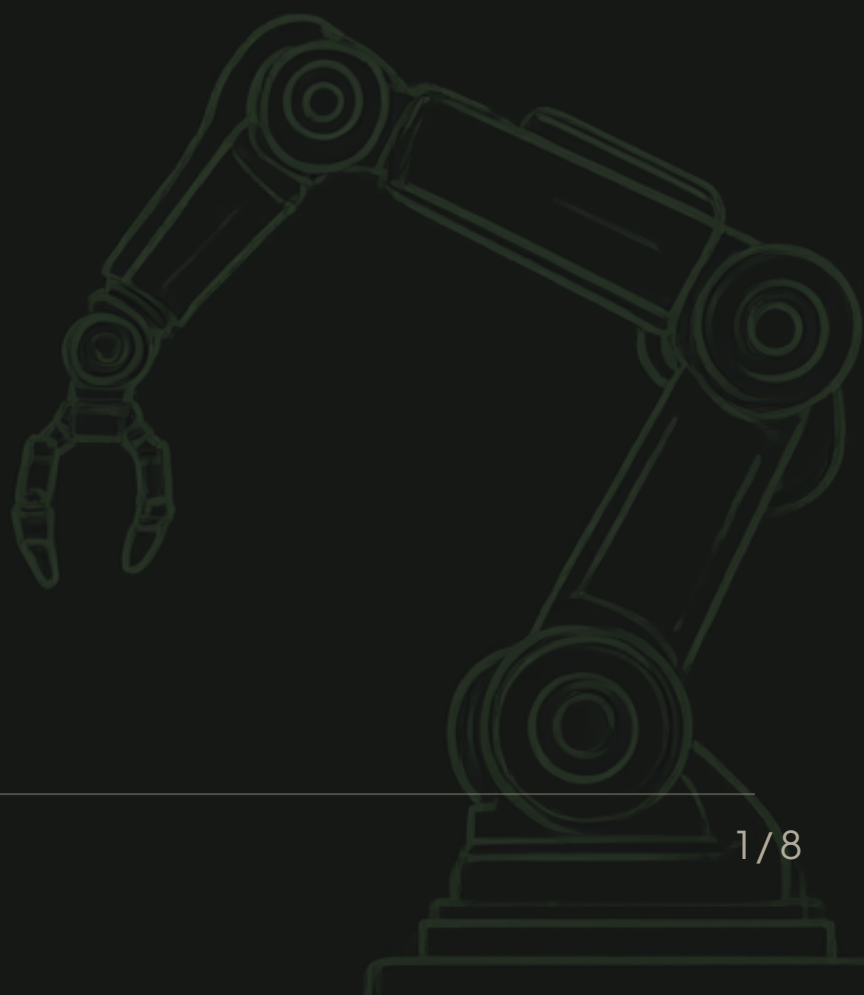
TECNICAI

Il login della tua app generata con l'AI è una decorazione?

Oltre 1.000 record con dati di passaporto, leggibili da chiunque. Nessun hacker, nessun attacco. Come è possibile?



IL FATTO

2 novembre 2026. Il Handelsblatt pubblica l'inchiesta di Crissy Field sulle app generate con Lovable.

La società di sicurezza di Amburgo ha analizzato 159.041 progetti pubblicati online.

34.545 usavano il database Supabase. Di questi, 24.664 spedivano record già al caricamento della pagina, senza login.

Su 7.403 siti, il 30 per cento, le tabelle contenevano indirizzi email: 10.560 tabelle in tutto.

Non hanno hackerato nulla: hanno trovato i siti in un archivio pubblico e interrogato i database con la chiave pubblica che il sito stesso espone. Chi era il colpevole?

Fonte: ricerca Crissy Field GmbH, in collaborazione con Handelsblatt (Lina Knees), 2/11/2026

IL MECCANISMO

Nessuno ha violato Lovable o Supabase.

L'app parla col database direttamente dal browser. La chiave che usa è incorporata nella pagina: è pubblica per progetto. Premi F12, la copi.

L'unica barriera sono le regole di accesso dentro il database: quali righe può leggere chi arriva senza login.

Se la tabella è nata senza regole, chiunque abbia quella chiave legge tutto. I dati non sono dietro il login: sono a una richiesta di distanza.

Perché nessuno se n'era accorto?

La pubblicità dice: nessuna competenza tecnica necessaria. Il contratto dice: la responsabilità dei dati è tua.

Crissy Field lo scrive nero su bianco: «Lovable's Terms & Conditions place responsibility for applications and data handling on the customers themselves».

E il responsabile sicurezza di Lovable, il 10 novembre, dichiara: «The most common issue we see in Lovable apps is data access rules that are too open».

Traduzione: il problema più frequente sono le regole di accesso troppo permissive. Allora la piattaforma è pericolosa?

Citazioni verbatim dall'inglese. Sintesi: il contratto scarica la responsabilità sui clienti (Crissy Field); il problema più comune sono le regole di accesso troppo aperte (blog Lovable, Igor Andriushchenko, 10/11/2026). La promessa «nessuna competenza tecnica» è quella che Crissy Field attribuisce al marketing di Lovable citandone i post

COSA NON CAMBIA

Non è una violazione della piattaforma. E non riguarda il gestionale che usi da dieci anni.

Riguarda le app appena generate da chi non sa programmare, pubblicate con i parametri di fabbrica mai verificati.

La ricerca lo dichiara per prima: il campione non è rappresentativo, il 30 per cento non è un tasso di perdita confermato (le email possono essere contatti pubblici o dati di test) e i record scaricati erano solo una parte: i dataset interessati possono contenerne altri.

Chi deve preoccuparsi, e di cosa?

LA LETTURA DEL PERITO

Un'app è una macchina. Nessuno la mette in produzione senza verifica di accettazione.

Nessuno accende un braccio meccanico senza controllare le protezioni. Poi si pubblica un'app che legge i dati dei clienti senza controllare chi può leggerli.

La logica di accettazione è la stessa: prima della messa in servizio, si verifica chi può accedere a cosa, e si mette per iscritto.

> **In pratica,**
> se nell'app finiscono dati personali, il titolare del trattamento è l'azienda che la pubblica. Non la piattaforma che l'ha generata: lo stabilisce il GDPR, titolare è chi decide finalità e mezzi del trattamento. Il contratto con la piattaforma lo conferma.

STASERA

Se in azienda c'è un'app nata con l'AI: prenotazioni, ordini, moduli, anagrafiche.

1. Chiedi a chi l'ha fatta: quali regole di accesso hanno le tabelle del database? Risultato per iscritto?

2. Prova a chiedere i dati all'app usando solo la chiave pubblica della pagina. Se arrivano, li legge anche uno sconosciuto.

3. Chiedi chi risponde della sicurezza di quell'app. Il contratto dice: l'azienda.

Test solo su app tue o che sei autorizzato a testare: provare la chiave pubblica sulle app altrui può configurare accesso abusivo. Dieci minuti, due query nel pannello del database.

MI PRESENTO:

Le app vanno trattate come le macchine. L'accettazione le rende verificabili.

Dubbi sulle app che la tua azienda genera con l'AI? Scrivici: info@tecnicai.it

Iscritto all'Ordine dei Periti Industriali di Padova · RSPP · Professionista antincendio n° PD01774P00344 · Docente dal 2012 · Fondatore TecnicAI · Co-fondatore Omeda Studios.

Contenuto informativo, non consulenza legale. Altri documenti gratuiti su tecnicai.it/news