

Vibe Coding **under attack**

Challenges induced by AI coding and how to secure the software development process

AI îți dă viteză. Nu îți dă arhitectură, acces controlat și date protejate.

Nu mai e greu să construiești

A DEVENIT UȘOR

**Cod, aplicație, domeniu, plăți.
Într-o seară.**

A RĂMAS GREU

**Cine are acces, la ce date
și cine verifică.**

S-a scurtat drumul până la lansare. Nu drumul până la o aplicație sigură.

Ce s-a întâmplat în 2025

28,6 mil.

chei și parole publicate în cod public, într-un singur an

+81%

creșterea scurgerilor de chei către servicii AI

64%

din cheile scurse în 2022 funcționează și astăzi

Ce vede atacatorul

01

Aplicația

02

Conturile

03

Datele clienților

04

API-urile

05

Cheile și token-urile

06

Automatizările

Nimeni nu atacă modelul. Se atacă ce ai pus online în jurul lui.

CAZ DOCUMENTAT PUBLIC · IULIE 2025

Tea: o aplicație virală și o stocare lăsată publică

72.000 imagini descărcate de oricine

13.000 selfie-uri și acte de identitate

1,1 mil. mesaje private, câteva zile mai târziu

/verification/

PUBLIC · FĂRĂ PAROLĂ

id_front_10432.jpg 2,1 MB

selfie_10432.jpg 1,4 MB

id_front_10433.jpg 2,4 MB

dm_att_88213.jpg 0,8 MB

...

RECONSTITUIRE PENTRU PREZENTARE

Nu a fost spart nimic. Fișierele se descărcau fără parolă.

Cele mai comune greșeli

- 01 **Chei și token-uri rămase în cod**
- 02 **Stocare și baze de date fără parolă**
- 03 **Drepturile verificate doar în ecran, nu pe server**
- 04 **Un singur cont, folosit de toată echipa**
- 05 **Datele reale ale clienților, folosite la teste**

Niciuna nu ține de AI. Toate țin de ce ai lăsat în urmă.

Cum se sparge, pas cu pas

PASUL 01

Scanează

Automat, tot ce e
public

PASUL 02

Încearcă

Conturi, adrese,
formulare

PASUL 03

Intră

Cu o cheie găsită,
nu spartă

PASUL 04

Rămâne

Zile, până observi
ceva

Nu e nevoie de geniu. E nevoie de o uşă lăsată deschisă.

Ce chei primește un agent AI

Email

CRM

Plăți

Fișiere

Un agent compromis nu dă un răspuns greșit.
Face, în numele tău, exact ce i s-a cerut.

24.008

chei găsite în fișierele de setări ale
agenților, în 2025

REGULA

Nu se sparge AI-ul. Se intră prin ce ai lăsat pornit.

În cazurile de mai sus nu a fost furat nimic. Totul a fost lăsat la vedere.

Trei lucruri înainte de producție

01

Închide accesul

Parole unice, 2FA, un cont pentru fiecare om și fiecare agent

02

Scoate cheile din cod

Schimbă-le pe cele care au fost deja acolo

03

Testează intrarea

Cineva din afară încearcă, înainte să ceri bani prin aplicație

O jumătate de zi acum, înainte de primul client real.

TEHNOLOGIE EMERGENTĂ · CE URMEAZĂ

Provocarea și mai mare: calculatorul cuantic

HARVEST NOW, DECRYPT LATER

**Datele criptate furate azi pot fi
decriptate mâine.**

RSA și ECC, folosite implicit în codul generat azi,
nu rezistă unui calculator cuantic suficient de
mare.

CRİPTOGRAFIE POST-CUANTICĂ (PQC)

2024	NIST publică primele standarde PQC FIPS 203 · 204 · 205 (ML-KEM, ML-DSA, SLH-DSA)
2026	UE: statele membre încep tranziția
2030	UE: infrastructurile critice, migrate la PQC
2035	UE: cât mai multe sisteme, migrate

Codul scris azi cu AI va rula și în era cuantică. Construiți-l cripto-agil.

CONCLUZIA

Păstrați controlul asupra datelor.

AI-ul și calculatorul cuantic schimbă doar viteza cu care îl pierdeți.

Unde sunt

Știți fiecare loc în care ajung datele

Cine are acces

Fiecare om și fiecare agent, cu drepturi minime

Cum sunt protejate

Azi și după venirea calculatorului cuantic

Nu opriți AI-ul

Doar nu construiți orbește cu el

Parole bune și 2FA

Nicio cheie în cod

Criptografie pregătită pentru PQC

Acces separat, pentru fiecare om și agent

Testat înainte să ceri bani

Controlul asupra datelor, la voi

Cristian Iosub

cristian.iosub@cybershield.org