

# Carta fedeltà in sicurezza: la resilienza digitale di CherryChain

3 Marzo 2026

**Il Centro per la Cybersecurity di FBK ha accompagnato l'azienda in un percorso di analisi tecnica e governance del rischio, nell'ambito di InnovAction.**

Nel mese di dicembre 2025, il [Centro per la Cybersecurity](#) di FBK ha concluso un'importante analisi tecnica e strategica per consolidare la piattaforma di servizi realizzata da [CherryChain](#) dedicata ai partner industriali per la gestione dei flussi di condivisione dei dati sui clienti finali. Identificando e valutando le risorse aziendali da proteggere, ad esempio servizi, database con dati dei clienti e software specifici, l'attività ha trasformato i punti di attenzione in opportunità di rafforzamento, garantendo una protezione solida ai dati degli utenti.

Il progetto si inserisce all'interno di EDIH SoE [InnovAction](#), un'iniziativa che fa parte del European Digital Innovation Hubs network per l'innovazione tecnologica finanziato dall'Unione Europea (Next Generation EU). Un'opportunità per i Centri Cybersecurity e Digital Industry della **Fondazione Bruno Kessler** (FBK) di continuare a supportare le PMI italiane nella loro "Twin Transition".

Il lavoro, articolato tra luglio e dicembre 2025, è stato condotto dai ricercatori **Matteo Brosolo**, **Umberto Morelli** e **Matteo Rizzi**, coprendo sia la verifica tecnica dell'applicazione (Servizio 1) sia la definizione di una strategia di governance del rischio (Servizio 2).

## **Pensare come un attaccante: l'analisi tecnica**

Per testare l'efficacia delle difese, i ricercatori hanno adottato la prospettiva di un potenziale avversario esterno (**approccio black-box**). L'analisi ha previsto:

- **Analisi Statica:** Esame del codice dell'app mobile Android tramite strumenti come JADX e MobSF.
- **Analisi Dinamica:** Verifica della tenuta delle difese lato client e server in scenari d'uso reale.

- **Stress Test delle API:** Valutazione della robustezza dei protocolli di comunicazione e dei meccanismi di scambio dati.

Presentati i risultati, si è passati a una verifica più approfondita del codice insieme al team di sviluppo (approccio **white-box**) per identificare un insieme di raccomandazioni e migliorare la postura di sicurezza in accordo al paradigma Zero Trust, che si fonda sul principio “non fidarsi mai, verificare sempre” per ogni utente, dispositivo o applicazione che tenta di accedere a una risorsa aziendale.

## Dalle vulnerabilità alle mitigazioni

CherryChain ha risposto prontamente ai feedback tecnici, implementando un piano di rientro immediato che ha elevato significativamente il profilo di sicurezza. Tra i principali interventi figurano un’analisi statica e dinamica dell’applicazione, e una verifica dei servizi web da essa contattati.

La resilienza generale è aumentata e rimane alta l’attenzione per tutti gli asset identificati come critici. Per questi, il gruppo di lavoro ha suggerito misure concrete da poter applicare in futuro per migliorare ulteriormente nel lungo periodo la sicurezza delle soluzioni. In questo modo è stata delineata una roadmap basata su una difesa multi-livello che include l’adozione del modello Zero Trust, il monitoraggio continuo tramite sistemi SIEM/UEBA, il rafforzamento degli endpoint con soluzioni EDR e programmi ricorrenti di formazione per il personale.

## L’importanza dell’analisi della postura di sicurezza delle PMI

Iniziative come InnovAction sono cruciali per il tessuto economico nazionale e locale. Le micro, piccole e medie imprese (PMI) rappresentano il cuore del sistema produttivo italiano, ma sono spesso le più vulnerabili a causa di un significativo gap di competenze interne in ambito cybersecurity.

A livello nazionale, la protezione di queste realtà è diventata una priorità di sicurezza collettiva: l’entrata in vigore della direttiva NIS2 (recepita in Italia col D.Lgs 138/2024) impone obblighi rigorosi di governance del rischio. A livello locale, il Centro per la Cybersecurity di FBK funge da nodo centrale di una rete di innovazione che mira a rendere la sicurezza digitale accessibile e sostenibile per il territorio.

Il modello “Test Before Invest”, consultabile al catalogo [seguito](#), offerto da InnovAction, permette alle piccole e medie imprese di sperimentare tecnologie avanzate in un ambiente protetto prima di procedere all’implementazione definitiva, riducendo i rischi associati agli investimenti. Analizzare la propria postura di sicurezza non significa solo “mettere una toppa” ai problemi riscontrati, ma allineare la gestione aziendale ai più alti standard internazionali (come ISO/IEC 27001), trasformando la cybersecurity da costo a vantaggio competitivo.

### LINK

<https://magazine.fbk.eu/it/news/carta-fedelta-in-sicurezza-la-resilienza-digitale-di-cherrychain/>

### TAG

- #cherrychain
- #cybersicurezza
- #edih
- #EDIHSoE
- #industriadigitale
- #innovaction
- #innovazione
- #PMI
- #twin transition

#### **AUTORI**

- Martina Cicaloni