Università degli Studi di Milano Facoltà di Scienze e Tecnologie Dipartimento di Informatica

Implementazione della Cybersecurity in una Startup Fintech: Il Caso Finanz

Relatore: Prof. Giovanni Degli Antoni
Correlatori: Prof. Brian W. Kernighan, Prof. Dennis M. Ritchie

Elaborato Finale di:
Andrea Ferraboli
Matr. Nr. 09985a

Anno Accademico 2024-2025

Questo lavoro è dedicato ai miei genitori

«*What I cannot create, I do not understand* » – Richard Feynman
«*It's not only powerful, but it's also inadequate* » – Miller Puckette

Ringraziamenti

Questa sezione, facoltativa, contiene i ringraziamenti.

Indice

Capitolo 1

Introduzione

1.1 Contesto e motivazioni

1.2 Obiettivi della tesi

1.3 Struttura del lavoro

Capitolo 2

Panoramica sulla Cybersecurity nel Settore Fintech

2.1 Definizione di Fintech e sue peculiarità

2.2 Minacce e vulnerabilità nel settore Fintech

2.3 Regolamentazioni e standard di sicurezza

Capitolo 3

Sicurezza a Livello di Codice

3.1 Introduzione alla Secure Coding

3.2 Principi di Secure Coding

3.2.1 Validazione degli input

3.2.2 Gestione sicura delle sessioni

3.2.3 Prevenzione delle vulnerabilità comuni (es. SQL Injection, XSS)

3.3 Approccio SecDevOps

3.3.1 Integrazione della sicurezza nel ciclo di sviluppo

3.3.2 Strumenti per l'analisi statica e dinamica del codice

3.3.3 Automazione dei test di sicurezza

Capitolo 4

Sicurezza a Livello di Infrastruttura

4.1 Architettura sicura per una startup Fintech

4.1.1 Design dell'infrastruttura cloud

4.1.2 Segmentazione della rete e controllo degli accessi

4.2 Gestione sicura dei dati

4.2.1 Crittografia dei dati a riposo e in transito

4.2.2 Gestione delle chiavi crittografiche

4.2.3 Backup e ripristino dei dati

4.3 Monitoraggio e risposta agli incidenti

4.3.1 Sistemi di rilevamento delle intrusioni (IDS)

4.3.2 Piani di risposta agli incidenti

Capitolo 5

Ingegneria Sociale e Sensibilizzazione

5.1 Definizione e tipologie di attacchi di ingegneria sociale

5.1.1 Phishing

5.1.2 Pretexting

5.1.3 Baiting

5.2 Simulazione di attacchi ai dipendenti

5.2.1 Metodologie di simulazione

5.2.2 Analisi dei risultati e miglioramenti

5.3 Diffusione della cultura della sicurezza

5.3.1 Formazione e awareness

5.3.2 Politiche aziendali e best practices

Capitolo 6

Aspetti Legali e di Compliance

6.1 Normative di riferimento (es. GDPR, PSD2)

6.2 Valutazione del rischio e audit di sicurezza

6.3 Conformità e certificazioni

Capitolo 7

Conclusioni

7.1 Risultati raggiunti

7.2 Prospettive future

Bibliografia

[1] Richard Feynman. *What I cannot create, I do not understand.*

[2] Miller Puckette. *It's not only powerful, but it's also inadequate.*