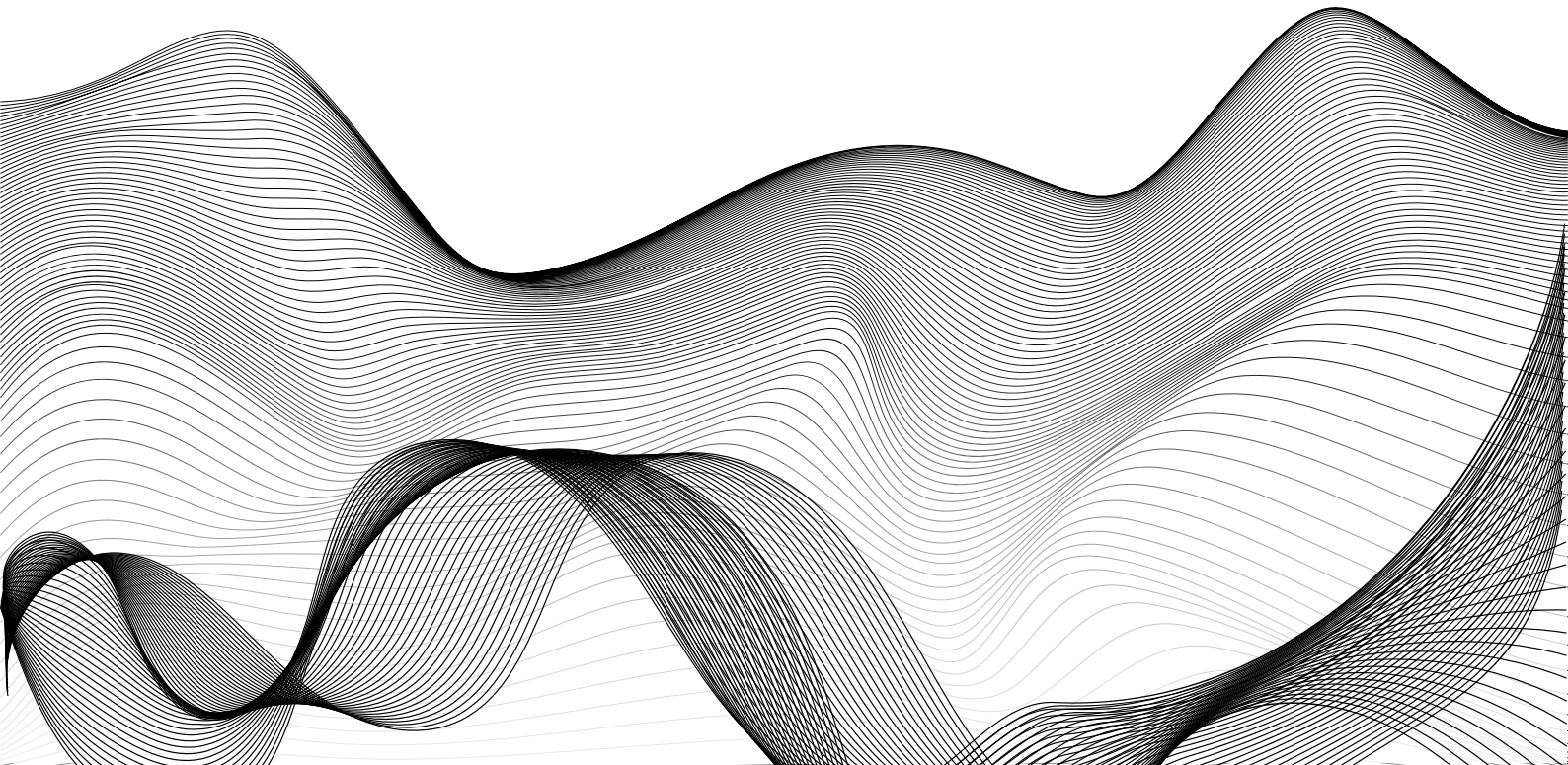
TRATTAMENTO DEI RISCHI

EPICODE / BCC ICCREA



TRACCIA

Descrizione

Un'azienda di servizi finanziari gestisce un'applicazione web che consente ai clienti di accedere ai propri account e effettuare transazioni finanziarie online. L'applicazione web memorizza e gestisce dati sensibili dei clienti, come informazioni personali, dettagli finanziari e credenziali di accesso. Il rischio principale è rappresentato da potenziali attacchi informatici volti a compromettere la sicurezza dell'applicazione web e a ottenere l'accesso non autorizzato ai dati dei clienti.

Supponendo di aver già effettuato l'analisi del rischio per lo scenario identificato, l'azienda decide di non accettare il rischio e procedere con la mitigazione del rischio applicando degli ulteriori controlli.

Compito

Utilizzando il NIST SP 800-53, seleziona 5 controlli, uno per ogni funzione di controllo (Deterrent, Preventive, Detective, Corrective, Compensating) e stabilisci come agisce il controllo sul rischio (può essere anche una combinazione):

- diminuendo la probabilità che un Threat agent avvii una minaccia;
- diminuendo la probabilità che una minaccia sfrutti una vulnerabilità;
- diminuendo la vulnerabilità;
- diminuendo l'impatto se la minaccia riesce a sfruttare la vulnerabilità

CONTROLLI PER FUNZIONE

(Deterrent - Preventive - Detective - Corrective - Compensating)

1 Deterrent

Controllo AC-2:

- Controllo dell'accesso logico, è un principio fondamentale della sicurezza informatica che mira a limitare e monitorare l'accesso alle risorse di un sistema.

2 Preventive

Controllo AC-12:

- Protezione contro malware, è un insieme di misure volte a prevenire, rilevare e contrastare le minacce informatiche rappresentate da software dannoso, come virus, worm, Trojan e ransomware

3 Detective

Controllo AU-12:

- Implementare un sistema di monitoraggio centralizzato per l'applicazione web. Registra e analizza i dati di attività degli utenti, i tentativi di accesso e altri eventi di sicurezza per identificare potenziali minacce e attività sospette.

4 Corrective

Controllo IA-2:

- Sviluppare un piano di risposta agli incidenti per l'applicazione web. Definisce le procedure da seguire in caso di un attacco informatico, come la notifica alle autorità competenti, il ripristino dei sistemi interessati e la comunicazione con i clienti.

5 Compensating

Controllo SC-8:

- Implementare la crittografia SSL/TLS per tutte le comunicazioni tra l'applicazione web e i browser degli utenti. Protegge i dati sensibili dei clienti, come le informazioni finanziarie e le credenziali di accesso, durante la trasmissione.