Report S2-L1
Mitigazione del rischio

Traccia

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.

Utilizzando **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 la mitigazione del rischio

Controlli	**Salvaguardia**		**Contromisura**		
	Deterrent (Deterrente)	**Preventive** (Preventivo)	**Successivo** (Detective)	**Correttivo** (Corrective)	**Compensativo** (Compensative)
	AC-2 Account Management: Implementare controllo per monitorare gli accessi.	**SC-23 Autenticità della sessione:** Generare ID di sessione unici per ogni sessione.	**AU-12:** Monitoraggio e analisi dei registri	**IR-1:** Implementare una politica di gestione completa dell'Incident Response	**CM-2:** Crittografia dei dati.
Azione di mitigazione del rischio	Riduce il rischio che un hacker o insider malevolo attacchi la Web app.	Riduce il rischio di furto di identità del dispositivo limitando la minaccia di accesso non autorizzato ai dati	Permette di verificare errori o comportamenti anomali.	Aumenta la probabilità di fronteggiare al meglio il rischio nell'ottica del continuo miglioramento	Limita il rischio di intercettazione dei dati sensibili nelle comunicazioni tra la Web App e i clienti.