DIGITAL RISK MANAGER -ALEX FIORILLO

RISK MANAGEMENT
TRATTAMENTO DEL RISCHIO

Introduzione

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 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.

Controllo

Mezzo di gestione del rischio che include le politiche, le procedure, le linee guida, le pratiche o le strutture organizzative che possono essere di natura amministrativa, tecnica, gestionale o legale.

I controlli possono essere suddivisi in tre tipologie:

AMMINISTRATIVI

- Politiche, procedure o linee guida che definiscono il personale o le pratiche aziendali in conformità con gli obiettivi di sicurezza dell'organizzazione.

- Uso navigazione web, uso del proprio dispositivo, definizione dei ruoli e dei compiti, classificazione dei dati, ecc ecc.

TECNICI

- Meccanismi hardware o software utilizzati per proteggere le risorse.

- Firewall, IDS, controllo degli accessi, crittografia, ecc ecc.

FISICI

- Mezzo tangibile utilizzato per prevenire o rilevare l'accesso non autorizzato ad aree fisiche, sistemi o risorse.

- Cancelli, controllo accesso biometrico, recinzioni, guardie, telecamere, badge, ecc ecc.

Funzioni di controllo

Definisce a cosa serve il controllo e come funziona:

DETERRENTE (Deterrent)

- Controllo utilizzato come dissuadere gli individui dal violare policy o commettere atti illegali.

PREVENTIVO (Preventive)

- Controllo utilizzato per evitare eventi indesiderati, errori e altre situazioni che l'impresa ha stabilito possano avere un effetto negativo materiale su un processo o un prodotto finale.

RILEVATORE (Detective)

- Controllo utilizzato per rilevare e segnalare errori, omissioni e utilizzi o inserimenti autorizzati.

CORRETTIVO (Corrective)

- Controllo utilizzato temporaneamente per correggere una problematica di sicurezza

COMPENSATIVO (Compensative)

- Controllo utilizzato per ridurre il rischio che una debolezza di controllo esistente o potenziale possa causare errori e omissioni.

Come agisce il controllo sul rischio

Fonte: NIST SP 800-53

FUNZIONE DI CONTROLLO	CONTROLLO NIST SP 800-53	AZIONE SUL RISCHIO
DETERRENT	AC-2: Controllo accessi	Riduce la probabilità che un threat agent avvii una minaccia limitando l'accesso all'applicazione web solo agli utenti autorizzati. (Es: autenticazione a due fattori, firewall)
PREVENTIVE	AC-12: Separazione dei segmenti di rete	Riduce la probabilità che una minaccia sfrutti una vulnerabilità segmentando la rete per isolare l'applicazione web da altri sistemi e dati sensibili.
DETECTIVE	AU-12: Monitoraggio e analisi dei registri	Riduce la vulnerabilità rilevando attività sospette e potenziali intrusioni nell'applicazione web analizzando i registri di sistema e di applicazione.
CORRECTIVE	IA-2: Risposta a incidenti	Riduce l'impatto se la minaccia ha successo definendo procedure per il contenimento, l'eradicazione e il ripristino in caso di violazione dei dati.

COMPENSATING	CM-2: Crittografia dei dati	Riduce l'impatto se la minaccia ha successo proteggendo i dati sensibili in caso di violazione, rendendoli inutilizzabili per gli attaccanti. (Es: crittografia AES, crittografia TLS)