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 sfruttura la vulnerabilità;

Per affrontare il rischio di potenziali attacchi informatici e garantire la sicurezza dell'applicazione web e dei dati dei clienti, l'azienda potrebbe adottare i seguenti controlli utilizzando il NIST SP 800-53:

1. ***Deterrent*** (Dissuasivo): Controllo che dissuade gli individui dal violare policy o commettere atti illegali.

- ***Controllo***: Implementazione di avvisi di sicurezza visibili e chiari sull'applicazione web che informano gli utenti delle possibili conseguenze legali e delle azioni punitive per tentativi di accesso non autorizzato.
- ***Azione sul rischio***: Diminuisce la probabilità che un threat agent avvii una minaccia, agendo come deterrente per gli attaccanti.

2. ***Preventive*** (Preventivo): Controllo utilizzato per evitare eventi indesiderati o situazioni che potrebbero avere un effetto negativo.

- ***Controllo***: Implementazione di un sistema di autenticazione multi-fattore (MFA) per l'accesso all'applicazione web, richiedendo ai clienti di confermare la propria identità utilizzando più di un metodo, come password e codici OTP.
- ***Azione sul rischio***: Diminuisce la probabilità che una minaccia sfrutti una vulnerabilità, migliorando la sicurezza dell'accesso.

3. ***Detective*** (Rilevatore): Controllo utilizzato per rilevare e segnalare errori, omissioni o attività sospette.

- ***Controllo***: Implementazione di sistemi di monitoraggio e rilevamento delle anomalie sull'applicazione web, che analizzano costantemente il traffico e le attività per individuare comportamenti non autorizzati o potenzialmente dannosi.

- ***Azione sul rischio***: Diminuisce la probabilità che una minaccia sfrutti una vulnerabilità, rilevando tempestivamente attività anomale e permettendo una risposta rapida.

4. ***Corrective*** (Correttivo): Controllo temporaneo utilizzato per correggere una problematica di sicurezza.

- ***Controllo***: Implementazione di un sistema di gestione degli incidenti di sicurezza che definisce procedure per rispondere prontamente a eventuali violazioni della sicurezza dell'applicazione web, incluso l'isolamento delle aree compromesse e la correzione delle vulnerabilità.
- ***Azione sul rischio***: Diminuisce l'impatto se la minaccia riesce a sfruttare la vulnerabilità, riducendo il tempo di inattività e il potenziale danno derivante da un attacco.

5. ***Compensating*** (Compensativo): Controllo utilizzato per ridurre il rischio che una debolezza di controllo possa causare errori o omissioni.

- ***Controllo***: Implementazione di una politica di backup e ripristino regolare dei dati dell'applicazione web, assicurando che in caso di compromissione dei dati, sia possibile recuperare rapidamente e ripristinare lo stato precedente.
- ***Azione sul rischio***: Diminuisce l'impatto se la minaccia riesce a sfruttare la vulnerabilità, garantendo la disponibilità e l'integrità dei dati anche in caso di incidente.