RISK MANAGEMENT

ANALISI DEL RISCHIO

MARIA HUAPAYA

INDICE

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

INTRODUZIONE

Scopo del Report

Questo documento è stato redatto con lo scopo di esaminare e migliorare le misure di sicurezza informatica per l'applicazione web di un'azienda di servizi finanziari. Attraverso l'analisi dettagliata del rischio e l'applicazione dei controlli raccomandati dal NIST SP 800-53, il report mira a fornire una strategia efficace per proteggere i dati sensibili dei clienti e mitigare i rischi di attacchi informatici.

Rilevanza della Cybersecurity nel Settore Finanziario

Nell'era digitale, la sicurezza delle applicazioni web che gestiscono transazioni finanziarie è cruciale. Un attacco riuscito può non solo comportare perdite economiche significative ma anche danneggiare la reputazione dell'azienda e la fiducia dei clienti. Pertanto, è essenziale adottare un approccio proattivo nella gestione dei rischi informatici, specialmente in un settore altamente regolamentato e vulnerabile come quello finanziario.

DESCRIZIONE DELL'AZIENDA E DELL'APPLICAZIONE WEB

Panoramica dell'Azienda di Servizi Finanziari

L'azienda è un istituto di servizi finanziari con una solida reputazione nel mercato, specializzata nell'offrire una vasta gamma di servizi finanziari, inclusi conti correnti, risparmio, investimenti e prestiti. Fondata oltre un decennio fa, ha sede principale in [Inserire la città] e serve migliaia di clienti, sia privati che aziende.

Funzionalità e Caratteristiche dell'Applicazione Web

L'applicazione web è un pilastro fondamentale per l'operatività dell'azienda, consentendo ai clienti di accedere ai loro account da remoto, effettuare transazioni, gestire investimenti e ottenere supporto clienti. È accessibile tramite browser e app mobile, garantendo massima accessibilità e comodità.

Tipi di Dati Sensibili Gestiti L'applicazione gestisce vari tipi di dati sensibili, che includono:

- Informazioni Personali: nome, indirizzo, data di nascita, numero di previdenza sociale.
- Dettagli Finanziari: numeri di conto, informazioni su carte di credito, dettagli degli investimenti.
- Credenziali di Accesso: username e password, dati per l'autenticazione a più fattori.

DISCUSSIONE SULLA GESTIONE DEI DATI SENSIBILI DEI CLIENTI

Tipologie di Dati Sensibili Raccolti

L'azienda raccoglie e gestisce una varietà di dati personali e finanziari dei clienti, che sono essenziali per l'erogazione dei suoi servizi. Questi dati includono informazioni identificative, dettagli finanziari e credenziali di sicurezza, che sono strettamente tutelati per prevenire accessi non autorizzati e frodi.

Politiche di Protezione Dati Implementate

Per garantire la sicurezza dei dati sensibili, l'azienda adotta diverse politiche e procedure, che includono:

- Crittografia dei Dati: tutti i dati sensibili trasmessi o salvati sono criptati utilizzando standard avanzati.
- Autenticazione Multi-Fattore (MFA): per accedere all'applicazione, i clienti devono verificare la loro identità attraverso più metodi di autenticazione, aumentando così la sicurezza degli accessi.
- Formazione Continua sui Rischi di Sicurezza: i dipendenti sono regolarmente formati sulle migliori pratiche di sicurezza e sul riconoscimento delle minacce informatiche.

Responsabilità Legale e Conformità Normativa

L'azienda è soggetta a rigorose normative relative alla protezione dei dati, inclusi regolamenti locali e internazionali come il GDPR. Questo impone l'adozione di misure di sicurezza adeguate e la trasparenza nella gestione dei dati. Inoltre, l'azienda deve sottostare a frequenti audit di conformità per garantire il rispetto continuo di queste normative.

IDENTIFICAZIONE DEL RISCHIO PRINCIPALE: ATTACCHI INFORMATICI

Scenari di Rischio Associati agli Attacchi Informatici

L'applicazione web, essendo un elemento centrale nell'operatività della banca, è un target primario per gli attacchi informatici. I principali scenari di rischio includono:

- Attacchi di Phishing: tramite email o messaggi fraudolenti, gli aggressori tentano di ottenere credenziali di accesso dai clienti.
- Attacchi Man-in-the-Middle (MitM): gli attaccanti possono intercettare le comunicazioni tra l'utente e l'applicazione per rubare o manipolare i dati.
- Violazioni dei Dati: accesso non autorizzato ai database dell'applicazione per sottrarre dati sensibili.
- Attacchi di Ransomware: blocco dell'accesso ai sistemi dell'azienda richiedendo un riscatto per il loro sblocco.

Potenziali Conseguenze per l'Azienda e i Clienti

Le conseguenze di un attacco informatico riuscito sono molteplici:

- Perdite Finanziarie Dirette: furto di fondi dai conti dei clienti o pagamento di riscatti.
- Danno alla Reputazione: perdita di fiducia dei clienti e danneggiamento dell'immagine aziendale.
- Costi Legali e di Conformità: sanzioni per mancata protezione dei dati e costi legati a cause legali da parte dei clienti colpiti.
- Interruzione dell'Operatività: disagi nell'erogazione dei servizi bancari, con possibili impatti negativi sull'attività commerciale.

ANALISI DEL RISCHIO

Dettagli dell'Analisi del Rischio Già Effettuata

L'analisi del rischio per l'applicazione web è stata condotta seguendo metodologie standardizzate che valutano sia la probabilità che l'impatto di ogni scenario di rischio identificato. I seguenti passaggi sono stati inclusi nell'analisi:

- Valutazione delle Vulnerabilità: identificazione delle debolezze tecniche e procedurali che potrebbero essere sfruttate dagli attaccanti.
- Analisi delle Minacce: determinazione dei potenziali attaccanti e delle loro capacità, obiettivi e metodi di attacco.
- Valutazione dell'Impatto: stima delle conseguenze finanziarie, operative e di immagine in caso di attacchi riusciti.
- Calcolo della Probabilità: stima della frequenza con cui potrebbero verificarsi specifici scenari di attacco, basata su dati storici e tendenze del settore.

Metodologie e Strumenti Utilizzati nell'Analisi

Per garantire un'analisi accurata e approfondita, sono stati utilizzati diversi strumenti e metodologie, tra cui:

- Software di Scanning di Vulnerabilità: per identificare automaticamente le vulnerabilità nella sicurezza dell'applicazione.
- Tecniche di Threat Modeling: per mappare e comprendere come gli attaccanti potrebbero penetrare o compromettere il sistema.
- Analisi Basata su Scenari: utilizzo di scenari ipotetici per valutare l'impatto e la probabilità di eventi di sicurezza.

DECISIONE DELL'AZIENDA DI NON ACCETTARE IL RISCHIO

Motivazioni della Decisione

L'azienda ha valutato che i rischi associati agli attacchi informatici superano la soglia di tolleranza accettabile per la sicurezza operativa e la protezione dei dati dei clienti. Considerate le severe implicazioni di potenziali violazioni dei dati, come danni economici, perdita di reputazione e sanzioni legali, è stata presa la decisione di non accettare il rischio e di procedere con misure di mitigazione avanzate.

Implicazioni di questa Scelta per la Strategia di Sicurezza

La decisione di non accettare il rischio comporta l'adozione di un approccio proattivo alla sicurezza informatica, con l'implementazione di controlli di sicurezza rafforzati e la realizzazione di un ambiente operativo resiliente.
Questo include l'investimento in tecnologie avanzate, la formazione continua del personale e la revisione periodica delle politiche di sicurezza per adattarsi all'evoluzione delle minacce informatiche.

MITIGAZIONE DEL RISCHIO

Introduzione alla Mitigazione del Rischio

La decisione di non accettare il rischio ha guidato l'azienda verso l'implementazione di strategie di mitigazione mirate a ridurre sia la probabilità che l'impatto degli attacchi informatici. Questo approccio si basa sulla comprensione che, mentre il rischio zero non è realizzabile, è essenziale minimizzare i rischi fino a livelli gestibili.

Strategie Generali di Mitigazione Adottate

Le strategie adottate includono:

- Rafforzamento delle Infrastrutture IT: aggiornamento e manutenzione regolare dei sistemi per prevenire vulnerabilità.
- Formazione e Consapevolezza del Personale: programmi continui di formazione sulla sicurezza per assicurare che tutti i dipendenti siano informati su come prevenire e reagire a incidenti di sicurezza.
- Piani di Risposta agli Incidenti: sviluppo di piani dettagliati per rispondere efficacemente a eventuali violazioni di sicurezza, minimizzando l'impatto e ripristinando rapidamente le operazioni normali.

APPLICAZIONE DI ULTERIORI CONTROLLI

Descrizione dei Nuovi Controlli Implementati

L'azienda ha identificato e implementato una serie di controlli di sicurezza aggiuntivi per rafforzare la protezione dell'applicazione web contro gli attacchi informatici. Questi controlli sono stati selezionati in base alle raccomandazioni del NIST SP 800-53 e sono stati personalizzati per adattarsi alle specifiche esigenze e rischi dell'azienda.

Giustificazione della Scelta dei Controlli Specifici

Ciascun controllo è stato scelto per affrontare specifici aspetti del rischio identificato, contribuendo a:

- Diminuire la Probabilità di Attacchi: implementazione di controlli deterrenti e preventivi per scoraggiare gli attacchi e bloccare gli attaccanti prima che possano causare danni.
- Ridurre la Vulnerabilità del Sistema: miglioramento delle politiche di accesso e delle tecnologie di sicurezza per ridurre le debolezze che gli attaccanti potrebbero sfruttare.
- Limitare l'Impatto degli Attacchi: controlli correttivi e compensativi per rispondere rapidamente agli incidenti e ripristinare le operazioni, minimizzando l'interruzione del servizio e la perdita di dati.

SELEZIONE DEI CONTROLLI (UTILIZZANDO NIST SP 800-53)

Controllo Deterrent:

- Controllo PE-13: controllo di sorveglianza fisica

Questo controllo prevede l'implementazione di misure di sorveglianza fisica come telecamere di sicurezza e guardie di sicurezza per monitorare le aree sensibili e prevenire accessi non autorizzati.

Come Diminuisce il Rischio: scoraggia attività non autorizzate aumentando il rischio di rilevamento e conseguenze per gli intrusi, riducendo così la probabilità di tentativi di attacco fisico o digitale.

Controllo Preventive:

- Controllo AC-2: controllo dell'accesso logico

Questo controllo è fondamentale per limitare e monitorare l'accesso alle risorse del sistema informatico, impedendo l'accesso non autorizzato a dati sensibili.

Come Diminuisce il Rischio: limita l'accesso solo agli utenti autorizzati, riducendo la probabilità che una minaccia sfrutti una vulnerabilità.

Controllo Detective:

- Controllo AU-12: monitoraggio centralizzato

Implementazione di un sistema di monitoraggio centralizzato per tracciare e analizzare i dati di attività degli utenti, tentativi di accesso, e altri eventi di sicurezza.

Come Diminuisce il Rischio: identifica e segnala attività sospette rapidamente, permettendo interventi tempestivi per mitigare il danno.

Controllo Corrective:

- Controllo IA-2: piani di risposta agli incidenti

Questo controllo include lo sviluppo di procedure dettagliate per la gestione degli incidenti di sicurezza, assicurando un'azione rapida e coordinata in risposta a

violazioni o attacchi.

Come Diminuisce il Rischio: minimizza l'impatto degli attacchi ripristinando rapidamente le operazioni sicure e comunicando efficacemente con le parti interessate.

Controllo Compensating:

- Controllo SC-8: crittografia dei dati di trasmissione

Implementazione della crittografia SSL/TLS per tutte le comunicazioni sensibili, proteggendo i dati durante il loro trasferimento tra l'utente e l'applicazione.

Come Diminuisce il Rischio: mantiene la confidenzialità e l'integrità dei dati sensibili, rendendo inefficaci gli sforzi degli attaccanti di intercettare o alterare i dati durante la trasmissione.

CONCLUSIONI

Discussione sull’Efficacia dei Controlli Selezionati

La selezione dei controlli NIST SP 800-53 implementati offre una copertura completa delle funzioni di sicurezza necessarie per proteggere l'applicazione web da attacchi informatici. L'approccio multidimensionale adottato assicura che le minacce siano non solo prevenute ma anche rapidamente identificate e mitigated, garantendo una risposta efficace in caso di incidenti. Questi controlli collaborano per formare un sistema di difesa in profondità, che è fondamentale in un ambiente ad alto rischio come quello finanziario.

Considerazioni Finali sulla Gestione del Rischio nell’Azienda

L'implementazione di questi controlli dimostra un impegno serio dell'azienda nel gestire proattivamente i rischi di sicurezza informatica. È essenziale che l'azienda continui a valutare e aggiornare le sue politiche di sicurezza per adattarsi all'evoluzione delle minacce e delle tecnologie. Un monitoraggio continuo e revisioni periodiche dei controlli di sicurezza saranno cruciali per mantenere l'integrità e la sicurezza dell'applicazione web e dei dati sensibili dei clienti.
La resilienza e la sicurezza dell'azienda dipendono non solo dall'efficacia dei controlli tecnici ma anche dal mantenimento di una cultura di sicurezza consapevole e reattiva tra tutti i dipendenti. Investire in formazione e consapevolezza sulla sicurezza continuerà ad essere una delle difese più efficaci contro le minacce emergenti.

GRAZIE

MARIA HUAPAYA