TRATTAMENTODEL RISCHIO S2L1

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. UtilizzandoNIST SP 800-53, seleziona5 controlli, uno per ognifunzionedi 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

DETERRENT (PE-20) ASSET MONITORING AND TRACKING

- **MONITORAGGIO E TRACCIAMENTO DEGLI ASSET** Controllo: Utilizza Assegnazione: tecnologie di localizzazione degli asset definite dall'organizzazione] per tracciare e monitorare la posizione e il movimento di Assegnazione: asset definiti dall'organizzazione] all'interno di Assegnazione: aree controllate definite dall'organizzazione.

Le tecnologie di localizzazione degli asset possono aiutare a garantire che gli asset critici, inclusi veicoli, attrezzature e componenti di sistema, rimangano in posizioni autorizzate. Le organizzazioni consultano l'Ufficio del Consigliere Generale e il funzionario senior dell'agenzia per la privacy riguardo al dispiegamento e all'uso delle tecnologie di localizzazione degli asset per affrontare potenziali preoccupazioni sulla privacy.

Questo controllo agisce sul rischio in vari modi, potrebbe essere anche una combinazione di questi:

- **Diminuendo la probabilità che un agente minaccioso avvii una minaccia**: Monitorando la posizione e il movimento degli asset, si può rilevare un comportamento sospetto in anticipo e prendere misure preventive.
- **Diminuendo la probabilità che una minaccia sfrutti una vulnerabilità**: Conoscendo la posizione esatta degli asset, si può garantire che siano protetti adeguatamente, riducendo così le opportunità per una minaccia di sfruttare una vulnerabilità.
- Diminuendo la vulnerabilità: Mantenendo gli asset in aree controllate, si limita l'esposizione a potenziali minacce, riducendo così la vulnerabilità.
- Diminuendo l'impatto se la minaccia riesce a sfruttare la vulnerabilità: Nel caso in cui una minaccia riesca a sfruttare una vulnerabilità, il monitoraggio e il tracciamento degli asset possono aiutare a mitigare l'impatto, permettendo un intervento rapido e limitando la portata del danno.

PREVENTIVE (AC-6) SEPARAZIONE DEI DOVERI

- **Preventivo (Preventive)**: Questo controllo impiega il principio del privilegio minimo, consentendo solo accessi autorizzati per gli utenti (o processi che agiscono per conto degli utenti) che sono necessari per svolgere i compiti organizzativi assegnati.
- Le organizzazioni applicano il privilegio minimo per specifici doveri e sistemi. Il principio del privilegio minimo viene applicato anche ai processi di sistema, garantendo che i processi abbiano accesso ai sistemi e operino a livelli di privilegio non superiori al necessario per realizzare missioni organizzative o funzioni aziendali. Le organizzazioni considerano la creazione di ulteriori processi, ruoli e account come necessario per raggiungere il privilegio minimo. Le organizzazioni applicano il privilegio minimo allo sviluppo, all'implementazione e all'operatività dei sistemi organizzativi.

- **Come agisce il controllo sul rischio**:

- **Diminuendo la probabilità che un threat agent avvii una minaccia**: Limitando le capacità di un singolo utente, si riduce la possibilità che un agente minaccioso possa avviare una minaccia.
- **Diminuendo la probabilità che una minaccia sfrutti una vulnerabilità**: Prevenendo l'accesso non autorizzato ai dati sensibili, si riduce la probabilità che una minaccia possa sfruttare una vulnerabilità.
- **Diminuendo la vulnerabilità**: Implementando il principio del privilegio minimo, si riduce la vulnerabilità del sistema.
- **Diminuendo l' impatto se la minaccia riesce a sfruttare la vulnerabilità**: Se una minaccia riesce a sfruttare una vulnerabilità, l'impatto è ridotto poiché l'accesso dell'utente è limitato solo a ciò che è necessario per svolgere i compiti assegnati.

DETECTIVE(AU-11) CONSERVAZIONE DEI REGISTRI DI AUDIT

Controllo: Conservare i registri di audit per un periodo di tempo definito dall'organizzazione, in linea con la politica di conservazione dei registri, per fornire supporto alle indagini a posteriori degli incidenti e per soddisfare i requisiti di conservazione delle informazioni regolamentari e organizzativi.

Le organizzazioni conservano i registri di audit fino a quando non si determina che i registri non sono più necessari per scopi amministrativi, legali, di audit o altri scopi operativi. Ciò include la conservazione e la disponibilità dei registri di audit relativi alle richieste della Freedom of Information Act (FOIA), alle citazioni in giudizio e alle azioni delle forze dell'ordine. Le organizzazioni sviluppano categorie standard di registri di audit relativi a tali tipi di azioni e processi di risposta standard per ogni tipo di azione. Le General Records Schedules della National Archives and Records Administration (NARA) forniscono la politica federale sulla conservazione dei registri.

Miglioramenti del controllo: (1) CONSERVAZIONE DEI REGISTRI DI AUDIT CAPACITÀ DI RECUPERO A LUNGO TERMINE Impiegare misure definite dall'organizzazione per garantire che i registri di audit a lungo termine generati dal sistema possano essere recuperati.

Discussione: Le organizzazioni hanno bisogno di accedere e leggere i registri di audit che richiedono una conservazione a lungo termine (nell'ordine degli anni). Le misure impiegate per facilitare il recupero dei registri di audit includono la conversione dei registri in formati più recenti, la conservazione dell'attrezzatura in grado di leggere i registri e la conservazione della documentazione necessaria per aiutare il personale a capire come interpretare i registri.

Questo controllo agisce sul rischio in vari modi:

Diminuendo la probabilità che un agente di minaccia avvii una minaccia: mantenendo un registro dettagliato delle attività, si può scoraggiare un potenziale agente di minaccia sapendo che le sue azioni saranno registrate.

Diminuendo la probabilità che una minaccia sfrutti una vulnerabilità: con un'analisi approfondita dei registri di audit, si possono identificare modelli o attività sospette che potrebbero indicare un tentativo di sfruttare una vulnerabilità.

Diminuendo la vulnerabilità: la conservazione dei registri di audit aiuta a identificare le aree di vulnerabilità nel sistema o nella rete, permettendo all'organizzazione di apportare le necessarie modifiche o aggiornamenti per rafforzare la sicurezza.

Diminuendo l'impatto se la minaccia riesce a sfruttare la vulnerabilità: se una minaccia dovesse riuscire a sfruttare una vulnerabilità, i registri di audit possono fornire informazioni preziose per comprendere come è avvenuto l'attacco, aiutando a mitigare l'impatto e a prevenire incidenti futuri.

CORRECTIVE: CONTROLLO DI SICUREZZA (IR-4) GESTIONE DEGLI INCIDENTI"

- Questo controllo può ridurre l'impatto se la minaccia riesce a sfruttare la vulnerabilità, permettendo un'azione rapida per contenere e correggere l'incidente. GESTIONE DEGLI INCIDENTI

Controllo: a. Implementare una capacità di gestione degli incidenti per gli incidenti che sia coerente con il piano di risposta agli incidenti e che includa preparazione, rilevamento e analisi, contenimento, eradicazione e recupero; b. Coordinare le attività di gestione degli incidenti con le attività di pianificazione di emergenza; c. Incorporare le lezioni apprese dalle attività di gestione degli incidenti in corso nelle procedure di risposta agli incidenti, nella formazione e nei test, e implementare le modifiche risultanti di conseguenza; e d. Assicurarsi che il rigore, l'intensità, l'ambito e i risultati delle attività di gestione degli incidenti siano comparabili e prevedibili in tutta l'organizzazione.

Le organizzazioni riconoscono che le capacità di risposta agli incidenti dipendono dalle capacità dei sistemi organizzativi e dai processi di missione e di business supportati da tali sistemi. Le organizzazioni considerano la risposta agli incidenti come parte della definizione, progettazione e sviluppo di processi e sistemi di missione e di business. Le informazioni relative agli incidenti possono essere ottenute da una varietà di fonti, tra cui il monitoraggio degli audit, il monitoraggio dell'accesso fisico e il monitoraggio della rete; rapporti degli utenti o degli amministratori; e eventi della catena di fornitura segnalati. Una capacità efficace di gestione degli incidenti include il coordinamento tra molte entità organizzative (ad esempio, proprietari di missioni o di business, proprietari di sistemi, funzionari autorizzanti, uffici delle risorse umane, uffici di sicurezza fisica, uffici di sicurezza del personale, dipartimenti legali, funzione esecutiva del rischio, personale operativo, uffici di approvvigionamento). Gli incidenti di sicurezza sospetti includono la ricezione di comunicazioni e-mail sospette che possono contenere codice maligno. Gli incidenti sospetti della catena di fornitura includono l'inserimento di hardware contraffatto o codice maligno nei sistemi organizzativi o nei componenti del sistema. Per le agenzie federali, un incidente che coinvolge informazioni personali identificabili è considerato una violazione. Una violazione comporta la divulgazione non autorizzata, la perdita di controllo, l'acquisizione non autorizzata, il compromesso o un evento simile in cui una persona diversa da un utente autorizzato accede o potenzialmente accede a informazioni personali identificabili o un utente autorizzato accede o potenzialmente accede a tali informazioni per scopi diversi da quelli autorizzati.

Questo controllo agisce sul rischio in vari modi:

- **Diminuendo la probabilità che un agente di minaccia avvii una minaccia**: Implementando un piano di risposta agli incidenti, si può scoraggiare un agente di minaccia dal tentare di sfruttare una vulnerabilità.
- **Diminuendo la probabilità che una minaccia sfrutti una vulnerabilità**: Attraverso la preparazione, il rilevamento e l'analisi, si può identificare e correggere le vulnerabilità prima che una minaccia possa sfruttarle.
- **Diminuendo la vulnerabilità**: La gestione degli incidenti può aiutare a identificare e correggere le vulnerabilità, riducendo così la vulnerabilità complessiva.
- **Diminuendo l'impatto se la minaccia riesce a sfruttare la vulnerabilità**: Il contenimento, l'eradicazione e il recupero possono limitare l'impatto di un incidente, anche se una minaccia riesce a sfruttare una vulnerabilità.

COMPENSATING: CONTROLLO DI SICUREZZA CP-9: PIANI DI RIPRISTINO DEL SERVIZIO”

- Controllo di backup del sistema: a. Eseguire backup delle informazioni a livello utente contenute nei componenti del sistema definiti dall’organizzazione con una frequenza definita dall’organizzazione, coerente con gli obiettivi di tempo di recupero e punto di recupero; b. Eseguire backup delle informazioni a livello di sistema contenute nel sistema con una frequenza definita dall’organizzazione, coerente con gli obiettivi di tempo di recupero e punto di recupero; c. Eseguire backup della documentazione del sistema, compresa la documentazione relativa alla sicurezza e alla privacy, con una frequenza definita dall’organizzazione, coerente con gli obiettivi di tempo di recupero e punto di recupero; e d. Proteggere la riservatezza, l’integrità e la disponibilità delle informazioni di backup.

- Le informazioni a livello di sistema includono informazioni sullo stato del sistema, software del sistema operativo, middleware, software applicativo e licenze. Le informazioni a livello utente includono informazioni diverse da quelle a livello di sistema. I meccanismi utilizzati per proteggere l’integrità dei backup del sistema includono firme digitali e hash crittografici. La protezione delle informazioni di backup del sistema durante il trasporto è affrontata da MP-5 e SC-8. I backup del sistema riflettono i requisiti nei piani di contingenza così come altri requisiti organizzativi per il backup delle informazioni. Le organizzazioni possono essere soggette a leggi, ordini esecutivi, direttive, regolamenti o politiche con requisiti riguardanti categorie specifiche di informazioni (ad esempio, informazioni sulla salute personale). Il personale dell’organizzazione consulta il funzionario senior dell’agenzia per la privacy e il consulente legale riguardo a tali requisiti.

- Come agisce il controllo sul rischio: Il controllo di backup del sistema agisce sul rischio in vari modi, potrebbe essere anche una combinazione di questi:

- **Diminuendo la probabilità che un agente minaccioso avvii una minaccia**: Eseguendo regolarmente i backup, si riduce la probabilità che un agente minaccioso possa causare danni irreparabili.
- **Diminuendo la probabilità che una minaccia sfrutti una vulnerabilità**: I backup regolari possono prevenire la perdita di dati in caso di sfruttamento di una vulnerabilità.
- **Diminuendo la vulnerabilità**: I backup regolari riducono la vulnerabilità del sistema alle minacce, poiché anche in caso di attacco, i dati possono essere ripristinati.
- **Diminuendo l’impatto se la minaccia riesce a sfruttare la vulnerabilità**: In caso di attacco riuscito, l’impatto è ridotto poiché i dati possono essere ripristinati dal backup.