Report sulla modellazione delle minacce

24/04/2024

Traccia

Utilizzando il framework di modellizzazione delle minacce di Adam Shostack, identifica una minaccia per un'azienda di sviluppo software.

Su cosa stiamo lavorando?

Cosa può andare storto?

Che cosa faremo al riguardo?

Abbiamo fatto un buon lavoro?

Ripeti il processo, eseguendo una gap analysis per trovare i punti di miglioramento. I controlli NIST SP 800-53 Rev. 5. possono aiutare nella modellizzazione delle minacce

Scenario

Nome dell'Azienda: TechFusion Solutions

Settore: Sviluppo di software per la gestione intelligente delle risorse umane.

Descrizione dell'Azienda: TechFusion Solutions è un'azienda innovativa nel campo della tecnologia che si specializza nello sviluppo di soluzioni software avanzate per l'ottimizzazione della gestione delle risorse umane. Con sede nel cuore della Silicon Valley, l'azienda si impegna a fornire strumenti tecnologici all'avanguardia per aiutare le aziende a gestire in modo efficiente e intelligente i loro processi HR.

Software Prodotti: Il principale prodotto di TechFusion Solutions è "HRMaster", una suite completa di software per la gestione delle risorse umane progettata per soddisfare le esigenze delle aziende di tutte le dimensioni. HRMaster offre una vasta gamma di funzionalità, tra cui:

Gestione del Personale: Strumenti per la gestione delle assunzioni, della formazione, delle valutazioni delle prestazioni e della gestione delle assenze.

Amministrazione del Personale: Funzionalità per la gestione delle retribuzioni, delle prestazioni, dei benefit e delle politiche aziendali.

Pianificazione delle Risorse: Moduli per la pianificazione delle risorse umane, la gestione dei turni e la pianificazione della successione.

Analisi dei Dati: Strumenti avanzati di analisi dei dati per monitorare le metriche HR chiave e identificare tendenze e opportunità di miglioramento.

Automazione dei Processi: Automazione dei processi HR per ridurre i tempi di elaborazione e migliorare l'efficienza operativa.

Clientela: TechFusion Solutions serve una vasta gamma di clienti, dalle piccole imprese alle grandi aziende multinazionali, operanti in settori diversi come tecnologia, sanità, finanza, manifattura e servizi.

Obiettivi: L'obiettivo principale di TechFusion Solutions è quello di diventare il leader di mercato nel settore della gestione intelligente delle risorse umane, offrendo soluzioni software innovative e altamente personalizzabili che consentono alle aziende di ottimizzare le loro operazioni HR e migliorare le prestazioni complessive del personale.

Introduzione

Questo report si propone di condurre un'analisi delle minacce al fine di identificare e mitigare i rischi per la sicurezza e l'integrità dei processi aziendali presso TechFusion Solutions, un'azienda immaginaria specializzata nello sviluppo di soluzioni software per la gestione delle risorse umane. La modellazione delle minacce sarà condotta utilizzando il framework di Adam Shostack, che si concentra su quattro domande chiave: "A cosa sto lavorando?", "Cosa può andare storto?", "Che cosa faremo a riguardo?" e "Abbiamo fatto un buon lavoro?".

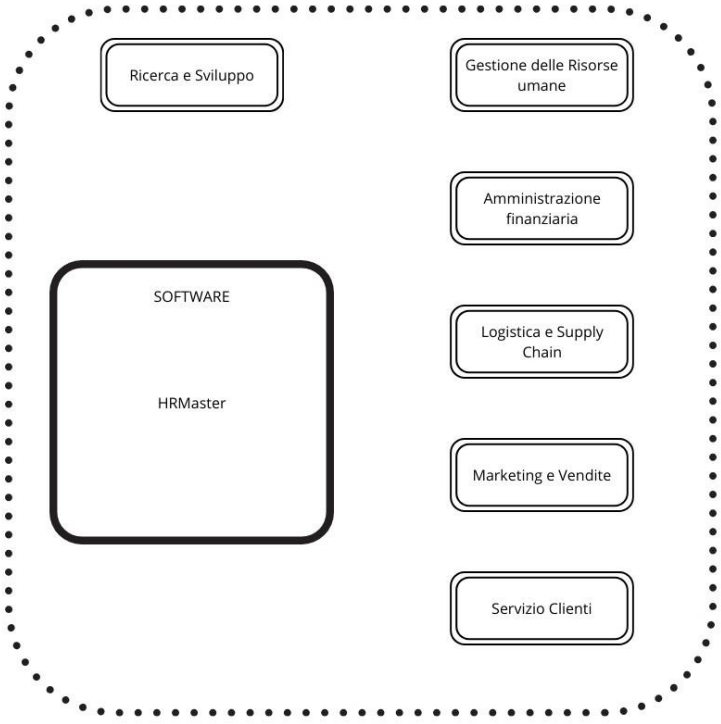
Contesto

TechFusion Solutions è un'azienda innovativa nel campo della tecnologia che sviluppa soluzioni software avanzate per la gestione delle risorse umane. L'azienda si impegna a garantire la sicurezza e l'integrità dei suoi processi aziendali al fine di proteggere i dati sensibili dei clienti e mantenere la fiducia dei suoi stakeholder.

La modellazione delle minacce sarà condotta seguendo il framework di Adam Shostack, che comprende le seguenti fasi:

A cosa sto lavorando?

L’azienda lavora allo sviluppo di software, in particolare una suite di software per la gestione delle risorse umane. Un’analisi del modello aziendale ha permesso di creare un diagramma di flusso che raffigura i processi aziendali di TechFusion:



Cosa può andare storto? Identificazione delle minacce potenziali che potrebbero compromettere la sicurezza e l'integrità dei processi aziendali.

Durante il processo di modellazione delle minacce sono state identificate diverse categorie di minacce che potrebbero influenzare la sicurezza e l'integrità dei processi aziendali di TechFusion Solutions. Queste includono:

Minacce Legate all'Accesso e alla sicurezza dei dati

Le minacce legate all'accesso non autorizzato ai sistemi e ai dati aziendali rappresentano una seria preoccupazione per l'integrità e la confidenzialità delle informazioni aziendali. Queste minacce possono originarsi sia da fonti esterne che interne.

Le minacce esterne sono associate a individui malintenzionati come hacker o gruppi di criminali informatici, che possono utilizzare modelli noti di attacco o tecniche avanzate per compromettere la sicurezza dei sistemi informatici aziendali. Tali attacchi possono mettere a rischio la riservatezza e l'integrità dei dati aziendali, minacciando la sicurezza complessiva dell'azienda.

D'altro canto, le minacce interne sono legate ai dipendenti dell'azienda stessa. I dipendenti potrebbero abusare del loro accesso autorizzato ai sistemi per scopi illeciti, come il furto o la manipolazione dei dati aziendali. Questo tipo di minaccia è particolarmente significativo in quanto gli attacchi interni possono risultare più difficili da individuare e prevenire rispetto agli attacchi esterni.

I processi aziendali critici che sono vulnerabili a questo tipo di minacce includono:

Ricerca e Sviluppo: I dati riservati e intellettuali associati alla ricerca e allo sviluppo possono essere compromessi da accessi non autorizzati, mettendo a rischio la proprietà intellettuale dell'azienda.

Amministrazione Finanziaria: I dati finanziari sensibili dell'azienda, inclusi bilanci, transazioni e informazioni sui clienti, sono particolarmente vulnerabili agli accessi non autorizzati che potrebbero portare a frodi finanziarie o furti di identità.

Gestione delle Risorse Umane: I dati sensibili dei dipendenti, compresi informazioni personali, dati di pagamento e informazioni fiscali, possono essere soggetti a accessi non autorizzati, con conseguenti rischi di violazione della privacy e di furto di identità.

Logistica e Supply Chain: I dati relativi ai clienti e ai fornitori, inclusi dettagli sui contratti, ordini e transazioni, possono essere esposti a rischi di accesso non autorizzato che potrebbero compromettere la relazione con i clienti e la reputazione aziendale.

Minacce Legate alla Sicurezza Fisica

Le minacce legate alla sicurezza fisica rappresentano un aspetto critico della protezione dei sistemi informatici e dei dati aziendali. Queste minacce possono derivare da una serie di situazioni che coinvolgono danni fisici ai dispositivi, ai sistemi o all'ambiente circostante. Nel contesto di TechFusion Solutions, un'azienda che sviluppa software per la gestione delle risorse umane, le minacce legate alla sicurezza fisica possono avere un impatto significativo sulla continuità operativa e sulla protezione dei dati sensibili.

Le minacce fisiche includono:

Furti: Il furto di dispositivi informatici o di hardware contenenti dati sensibili rappresenta una minaccia diretta alla sicurezza fisica dell'azienda. Il furto può compromettere non solo l'integrità dei dati, ma anche la disponibilità dei sistemi necessari per le operazioni aziendali.

Danni fisici ai dispositivi: Incidenti come cadute, urti o danni accidentali possono danneggiare fisicamente i dispositivi informatici, causando la perdita irreparabile di dati o la compromissione del funzionamento dei sistemi.

Danni ambientali: Eventi naturali come incendi, alluvioni o catastrofi ambientali possono causare danni estesi ai sistemi informatici e all'infrastruttura aziendale, mettendo a rischio la sicurezza e la disponibilità dei dati.

Minacce Legate alle Pratiche Aziendali

Minacce correlate a errori umani, mancanza di consapevolezza sulla sicurezza, processi aziendali non sicuri o politiche di sicurezza inefficaci.

La mancanza di consapevolezza tra i dipendenti riguardo alle potenziali minacce informatiche e alle pratiche migliori per la prevenzione degli attacchi rappresenta un serio rischio per l'azienda. In particolare, la mancanza di formazione e informazione sulle migliori pratiche di sicurezza informatica può esporre l'azienda a possibili vettori di attacco e compromettere la sicurezza dei sistemi e dei dati aziendali.

Nel contesto dello sviluppo del software, il processo del ciclo di vita prevede una serie di controlli progettati per eliminare o mitigare le vulnerabilità intrinseche al software. Tuttavia, la mancanza di attenzione da parte degli sviluppatori nell'adottare e seguire rigorosamente le migliori pratiche di sviluppo del software può portare a gravi problemi di sicurezza e compromettere la reputazione dell'azienda.

Le vulnerabilità critiche non risolte possono non solo compromettere la sicurezza dell'azienda stessa, ma anche creare rischi per gli utenti finali che utilizzano il software. Pertanto, è fondamentale che gli sviluppatori adottino pratiche di sviluppo sicure e che l'azienda promuova

una cultura della sicurezza informatica tra tutti i dipendenti per garantire la protezione dei dati e dei sistemi aziendali.

Che cosa faremo a riguardo?

Valutazione dell'impatto potenziale e della probabilità di realizzazione delle minacce identificate.

Basandoci sulle minacce identificate, è essenziale implementare una serie di controlli e misure di sicurezza per mitigare i rischi e proteggere l'azienda dai potenziali attacchi. I

controlli/misure di sicurezza sono stati scelti secondo le normative del NIST, le normative prese in considerazione sono:

- NIST SP800-53r
- NIST SP800-53Ar

Di seguito sono elencati i controlli consigliati, suddivisi per categoria di minacce:

Minacce Legate all'Accesso e alla Sicurezza dei Dati:

Controllo/Misura di Sicurezza	**Riferimento NIST SP800-53r**	**Riferimento NIST SP80053Ar**
Implementazione di controlli di accesso basati su ruoli per limitare l'accesso ai dati solo al personale autorizzato	AC-2, AC-3	AC-2, AC-3
Monitoraggio e registrazione degli accessi ai dati sensibili per individuare e rispondere tempestivamente agli accessi non autorizzati	AC-6, AU-3	AC-6, AU-3
Implementazione di procedure di autenticazione multi-fattore per garantire un livello aggiuntivo di sicurezza nell'accesso ai sistemi e ai dati sensibili	AC-7	AC-7
Sensibilizzazione e formazione periodica del personale sulla sicurezza informatica e sulle best practice per prevenire l'accesso non autorizzato e la manipolazione dei dati	AT-2, AT-3	AT-2, AT-3

Minacce Legate alla Sicurezza Fisica:

Controllo/Misura di Sicurezza	**Riferimento NIST SP800-53r**	**Riferimento NIST SP80053Ar**
Implementazione di misure di sicurezza fisica come sistemi di sorveglianza, controllo degli accessi e allarmi per proteggere l'ambiente fisico dei sistemi informatici	PE-4, PE-6	PE-4, PE-6
Backup regolari dei dati aziendali e archiviazione in un'area sicura esterna per proteggerli da eventi catastrofici o danni fisici	CP-9	CP-9

Minacce Legate alle Pratiche Aziendali:

Controllo/Misura di Sicurezza	**Riferimento NIST SP800-53r**	**Riferimento NIST SP80053Ar**
Implementazione di politiche e procedure aziendali per promuovere la consapevolezza sulla sicurezza informatica e per garantire l'adesione alle best practice di sicurezza	SA-1, SA-2, SA-7	SA-1, SA-2, SA-7
Revisione periodica dei processi aziendali per identificare e correggere eventuali vulnerabilità o lacune nella sicurezza	SA-11	SA-11
Utilizzo di strumenti di analisi statica e dinamica del codice per identificare e correggere potenziali vulnerabilità nel software durante il processo di sviluppo	SA-11, SA-12	SA-11, SA-12

Implementando questi controlli e misure di sicurezza, TechFusion Solutions sarà in grado di mitigare i rischi identificati e proteggere efficacemente i suoi processi aziendali dalla minaccia delle violazioni della sicurezza.

Abbiamo fatto un buon lavoro?

Per valutare se abbiamo fatto un buon lavoro nella gestione delle minacce identificate, è necessario considerare i seguenti fattori:

- **Implementazione dei Controlli di Sicurezza:** bisogna valutare se i controlli di sicurezza proposti sono stati effettivamente implementati e integrati nei processi aziendali di TechFusion Solutions.

- **Efficacia dei Controlli:** bisogna verificare se i controlli adottati sono efficaci nel mitigare i rischi identificati. Ciò può essere valutato attraverso monitoraggi periodici, test di penetrazione e revisioni dei processi.

- **Conformità alle Normative e Standard di Sicurezza:** È importante assicurarsi che i controlli implementati siano conformi alle normative e agli standard di sicurezza, come quelli proposti dalle normative NIST SP800-53r e NIST SP800-53Ar.

- **Sensibilizzazione e Formazione del Personale:** Dobbiamo valutare se sono state fornite adeguata sensibilizzazione e formazione al personale su questioni di sicurezza informatica e sulle best practice per mitigare i rischi.

- **Gestione delle Minacce Emergenti:** È importante considerare la capacità dell'azienda di identificare e rispondere tempestivamente a minacce emergenti o nuove vulnerabilità.

Valutando questi fattori, possiamo determinare se abbiamo fatto un buon lavoro nella gestione delle minacce. Se i controlli sono stati implementati in modo efficace, se l'azienda è conforme alle normative di sicurezza e se il personale è adeguatamente preparato, possiamo ragionevolmente concludere di aver fatto un buon lavoro nella gestione delle minacce.

Analisi dei Gap

L'analisi dei gap consiste nell'identificare e valutare le discrepanze tra lo stato attuale della sicurezza informatica dell'azienda e lo stato desiderato o le migliori pratiche del settore. Basandoci sulle minacce identificate e sui controlli di sicurezza proposti nel contesto di TechFusion Solutions, possiamo individuare i seguenti gap:

Gap nei Controlli di Accesso e Sicurezza dei Dati:

Attuale: Non è implementato un sistema di controllo degli accessi basato su ruoli per limitare l'accesso ai dati sensibili solo al personale autorizzato.

Desiderato: Implementare controlli di accesso basati su ruoli per garantire che solo gli utenti autorizzati possano accedere ai dati sensibili, riducendo così il rischio di accesso non autorizzato.

Gap nella Sicurezza Fisica:

Attuale: Mancanza di misure di sicurezza fisica come sistemi di sorveglianza, controllo degli accessi e allarmi per proteggere l'ambiente fisico dei sistemi informatici.

Desiderato: Implementare misure di sicurezza fisica per proteggere l'ambiente fisico dei sistemi informatici da potenziali minacce come furti o danni fisici.

Gap nella Sensibilizzazione e Formazione del Personale:

Attuale: Il personale potrebbe non essere adeguatamente sensibilizzato sulla sicurezza informatica e sulle best practice per prevenire l'accesso non autorizzato e la manipolazione dei dati.

Desiderato: Fornire sensibilizzazione e formazione periodica al personale sulla sicurezza informatica, incluso l'accesso sicuro ai dati aziendali e la risposta agli incidenti di sicurezza.

Gap nella Gestione delle Minacce Emergenti:

Attuale: Potrebbe mancare un processo strutturato per identificare e rispondere tempestivamente a minacce emergenti o nuove vulnerabilità.

Desiderato: Implementare un processo di gestione delle minacce che includa la monitoraggio costante dell'ambiente aziendale e l'aggiornamento delle misure di sicurezza in base alle minacce emergenti.

Gap nella Revisione dei Processi Aziendali:

Attuale: Potrebbe mancare una revisione periodica dei processi aziendali per identificare e correggere eventuali vulnerabilità o lacune nella sicurezza.

Desiderato: Implementare una revisione regolare dei processi aziendali per identificare e correggere eventuali vulnerabilità o lacune nella sicurezza informatica.