Traccia:

La vostra organizzazione vi ha incaricato di svolgere un risk assessment sulla seguente azienda.

Nome azienda: TechnoCorp

Settore: Tecnologia dell'informazione e servizi IT

Descrizione: TechnoCorp è un'azienda di medie dimensioni che opera nel settore IT, fornendo servizi di consulenza, sviluppo software e gestione di infrastrutture tecnologiche a clienti di diverse industrie. Fondata 15 anni fa, l'azienda conta circa 500 dipendenti distribuiti tra la sede centrale e 3 filiali regionali.

Infrastruttura IT:

• Rete aziendale con server interni che ospitano applicazioni aziendali critiche, database e sistemi di archiviazione dati

• Utilizzo di cloud pubblici (AWS, Azure) per alcune applicazioni e servizi

• Rete wireless per dipendenti e guest

• Dispositivi personali (Bring Your Own Device) utilizzati dai dipendenti

• Numerosi laptop e workstation per sviluppatori e consulenti

• Sito web aziendale ospitato esternamente

• Firewall perimetrale

• EDR/xDR su tutti i sistemi

Clienti e dati sensibili:

• TechnoCorp gestisce dati sensibili di clienti, come informazioni finanziarie, dati personali di dipendenti/clienti, proprietà intellettuale

• I principali clienti includono banche, assicurazioni, aziende sanitarie e produttori

Personale e accessi:

• Amministratori di sistema con accesso totale all'infrastruttura • Sviluppatori con accesso ai sistemi di sviluppo

• Personale di supporto tecnico con accesso limitato • Consulenti e collaboratori esterni con credenziali di accesso

• Politica di password e autenticazione a due fattori implementata

Partendo dalla descrizione fornita, procedere con l'identificazione di uno scenario di rischio (Top-down) fino ad arrivare all'analisi del rischio di questo scenario.

• Identificazione del rischio

• Analisi degli asset

• Analisi delle vulnerabilità

• Analisi delle minacce

• Modellazione delle minacce

• Scenari di rischio

• Analisi del rischio qualitativa o semi-quantitativa

Per le probabilità di occorrenza, statistiche e stime, affidatevi a fonti note o studi di settore.

- **Identificazione del rischio:**

1. Analisi degli asset:

Dati sensibili dei clienti:

Questi dati possono includere informazioni finanziarie, come numeri di conto bancario o informazioni sulla carta di credito, che sono estremamente sensibili e richiedono una protezione rigorosa per conformarsi alle normative sulla privacy, come GDPR o HIPAA, a seconda del contesto geografico e dell'industria.

I dati personali dei dipendenti e dei clienti includono informazioni come nomi, indirizzi, numeri di telefono, indirizzi email e altre informazioni identificative che potrebbero essere utilizzate per scopi fraudolenti se compromesse.

La proprietà intellettuale dell'azienda può includere codice sorgente, design, brevetti o segreti commerciali che, se esposti, potrebbero compromettere la competitività dell'azienda e portare a perdite finanziarie significative.

Infrastruttura IT:

I server interni che ospitano applicazioni aziendali critiche e database sono essenziali per il funzionamento quotidiano dell'azienda e potrebbero essere bersagli primari per attacchi informatici.

L'utilizzo di servizi cloud pubblici aggiunge un livello di complessità alla sicurezza, poiché i dati possono essere distribuiti su più provider e le configurazioni di sicurezza devono essere attentamente gestite per evitare violazioni.

La rete wireless può essere vulnerabile agli attacchi di tipo "man-in-the-middle" o di spoofing se non adeguatamente protetta.

I dispositivi personali (BYOD) possono rappresentare un rischio significativo se non sono correttamente gestiti, poiché potrebbero essere compromessi da malware o essere soggetti a perdite fisiche.

Servizi e applicazioni:

Le applicazioni aziendali critiche sono essenziali per le operazioni quotidiane e devono essere protette per garantire la continuità del business.

I servizi cloud pubblici devono essere attentamente configurati e gestiti per evitare esposizioni indesiderate dei dati o delle risorse.

Il sito web aziendale ospitato esternamente può essere soggetto a attacchi come DDoS o injection di SQL, che potrebbero compromettere la reputazione dell'azienda e la fiducia dei clienti.

Il firewall perimetrale svolge un ruolo critico nella protezione dell'infrastruttura interna da accessi non autorizzati e attacchi esterni.

2. Analisi delle vulnerabilità:

Per valutare le vulnerabilità, possiamo utilizzare il Common Vulnerability Scoring System (**CVSS**), uno standard industriale per assegnare un punteggio numerico alle vulnerabilità e valutarne il livello di rischio. Ogni vulnerabilità viene valutata su una scala da 0 a 10, dove 0 rappresenta un rischio insignificante e 10 rappresenta un rischio critico.

Accesso privilegiato:

CVSS Score: 7-9 (alto rischio)

Gli amministratori di sistema e gli sviluppatori con accesso totale all'infrastruttura rappresentano un rischio significativo se i loro account vengono compromessi o se agiscono malevolmente.

Le credenziali di accesso privilegiate possono essere oggetto di furto o compromissione tramite tecniche come phishing o ingegneria sociale.

Dispositivi personali non controllati (BYOD):

CVSS Score: 5-8 (rischio moderato-alto)

L'uso di dispositivi personali per accedere ai dati aziendali aumenta il rischio di esposizione dei dati a causa di malware o di perdita fisica dei dispositivi.

La mancanza di controlli adeguati sui dispositivi BYOD potrebbe permettere a utenti non autorizzati di accedere ai dati aziendali o di compromettere la sicurezza della rete.

Rischi legati al cloud:

CVSS Score: 6-9 (rischio moderato-alto)

Le configurazioni errate o non sicure nei servizi cloud pubblici possono esporre i dati aziendali a rischi di accesso non autorizzato.

La mancanza di visibilità e controllo diretto sull'infrastruttura cloud può rendere difficile la rilevazione e la risposta agli incidenti di sicurezza.

Minacce interne:

CVSS Score: 4-7 (rischio basso-moderato)

Anche se meno comuni, le minacce interne rappresentano un rischio significativo, specialmente da parte di dipendenti disgraziati o ex dipendenti con accesso privilegiato.

Queste minacce possono includere azioni intenzionali, come il furto di dati o la sabotaggio dell'infrastruttura, o azioni non intenzionali, come l'apertura di email di phishing o la caduta vittima di attacchi di social engineering.

Attacchi esterni:

CVSS Score: 6-9 (rischio moderato-alto)

Gli attacchi esterni possono sfruttare vulnerabilità nella rete, nei servizi cloud o nei dispositivi personali per ottenere accesso non autorizzato ai dati o compromettere l'infrastruttura.

Le tecniche comuni utilizzate includono attacchi di phishing, exploit di vulnerabilità software, attacchi DDoS e intrusioni tramite reti wireless non protette.

3. Analisi delle minacce:

Le vulnerabilità identificate all'interno dell'azienda TechnoCorp possono essere sfruttate da una varietà di minacce che mettono a rischio la sicurezza dei dati, l'integrità dell'infrastruttura IT e la reputazione dell'azienda stessa.

Potenziali minacce legate alle vulnerabilità identificate:

Accesso non autorizzato: Rappresenta una minaccia significativa attraverso tecniche come il phishing, l'uso di credenziali rubate o l'exploit di vulnerabilità software.

Dispositivi personali non controllati (BYOD): Aumentano il rischio di esposizione dei dati a causa di malware o accesso non autorizzato da parte di terzi.

Rischi legati al cloud: Configurazioni errate o non sicure nei servizi cloud pubblici possono esporre i dati aziendali a accesso non autorizzato o compromettere la sicurezza dell'ambiente cloud.

Minacce interne: Sebbene meno comuni, possono causare danni significativi, con dipendenti malintenzionati o inconsapevoli che compromettono la sicurezza dei dati o sabotano l'infrastruttura IT.

Attacchi esterni: Gli attaccanti potrebbero sfruttare vulnerabilità nella rete, nei servizi cloud o nei dispositivi personali per ottenere accesso non autorizzato ai dati o compromettere l'infrastruttura.

4. Modellazione delle minacce e Gap Analysis:

La modellazione delle minacce implica l'identificazione e la valutazione dei potenziali scenari in cui le minacce possono manifestarsi e causare danni all'azienda.

Una gap analysis, o analisi dei divari, è un processo che viene utilizzato per valutare e identificare le differenze ("gap") tra lo stato attuale di un'organizzazione e il suo obiettivo desiderato. In sostanza, si tratta

di una valutazione comparativa che aiuta a comprendere dove ci si trova rispetto a dove si vorrebbe essere, consentendo all'organizzazione di individuare i punti deboli e le aree di miglioramento.

Nella mia gap analysis legata alle minacce identificate, utilizzo i controlli del NIST SP 800-53 Rev. 5.

l NIST SP 800-53 Rev. 5 (Special Publication 800-53, Revision 5) è un documento pubblicato dal National Institute of Standards and Technology (NIST) degli Stati Uniti. Questo documento fornisce linee guida e raccomandazioni per la sicurezza dell'informazione e la gestione dei rischi nel contesto dei sistemi informativi e delle organizzazioni.

Accesso non autorizzato:

- ***Minaccia***: Un attaccante esterno sfrutta un attacco di phishing per ottenere le credenziali di accesso di un dipendente, quindi utilizza queste credenziali per accedere al sistema interno dell'azienda.
- ***Gap***: Manca un'implementazione efficace del controllo AC-2 (Limit Access to Authorized Users) del NIST SP 800-53 Rev. 5 per limitare l'accesso solo agli utenti autorizzati e monitorare gli accessi non autorizzati.
- ***Azioni correttive***: Implementare l'autenticazione multi-fattore (MFA) per tutti gli utenti conforme al controllo AC-2, e stabilire una procedura per il monitoraggio e la risposta agli accessi non autorizzati.

Dispositivi personali non controllati (BYOD):

- ***Minaccia***: Un dipendente perde il proprio dispositivo personale contenente dati aziendali sensibili in un luogo pubblico, e il dispositivo viene recuperato da un individuo non autorizzato che accede ai dati.
- ***Gap***: Manca una politica BYOD ben definita e controlli per gestire in modo sicuro l'accesso e l'utilizzo dei dispositivi personali, conforme al controllo AC-20 (Use of External Information Systems).
- ***Azioni correttive***: Implementare una politica BYOD conforme al controllo AC-20, fornire strumenti di gestione dei dispositivi mobili per applicare politiche di sicurezza sui dispositivi personali, e fornire formazione ai dipendenti sull'uso sicuro dei dispositivi personali.

Rischi legati al cloud:

- ***Minaccia***: Un attaccante sfrutta una vulnerabilità nella configurazione di un servizio cloud pubblico per ottenere accesso non autorizzato ai dati sensibili dell'azienda ospitati nel cloud.
- ***Gap***: Manca una valutazione completa dei rischi legati all'utilizzo dei servizi cloud conforme al controllo SA-9 (External Information System Services), e controlli per mitigare questi rischi, come la crittografia dei dati sensibili.
- ***Azioni correttive***: Condurre una valutazione dettagliata dei rischi legati all'utilizzo dei servizi cloud conforme al controllo SA-9, implementare misure di sicurezza aggiuntive come la crittografia dei dati sensibili, e stabilire processi per il monitoraggio continuo delle configurazioni di sicurezza dei servizi cloud.

Minacce interne:

- ***Minaccia***: Un dipendente licenziato con accesso privilegiato all'infrastruttura IT dell'azienda decide di danneggiare i sistemi aziendali cancellando o modificando dati critici.
- ***Gap***: Manca una protezione efficace contro le minacce interne conforme al controllo AC-2. Potrebbero mancare controlli per rilevare comportamenti anomali degli utenti e limitare l'opportunità di abusi interni.
- ***Azioni correttive***: Implementare controlli di monitoraggio avanzati per rilevare comportamenti anomali degli utenti conforme al controllo SI-4 (Information System Monitoring), migliorare la formazione dei dipendenti sulla sicurezza informatica e rafforzare i controlli di accesso e di autorizzazione per limitare l'opportunità di abusi interni.

Attacchi esterni:

- ***Minaccia***: Un attaccante esegue un attacco DDoS contro il sito web dell'azienda, causando un'interruzione del servizio e rendendo il sito inaccessibile agli utenti legittimi.
- ***Gap***: Manca una protezione efficace contro gli attacchi esterni conforme al controllo CA-7 (Continuous Monitoring). Potrebbero mancare controlli per mitigare gli attacchi DDoS e difendersi dalle tecniche di phishing e di spoofing.
- ***Azioni correttive***: Implementare soluzioni anti-DDoS per mitigare gli attacchi distribuiti conforme al controllo SI-7 (Software, Firmware, and Information Integrity), implementare una gestione delle vulnerabilità per identificare e correggere le vulnerabilità dei sistemi esposti su Internet conforme al controllo RA-5 (Vulnerability Scanning), e fornire formazione continua ai dipendenti sulla consapevolezza della sicurezza informatica per riconoscere e prevenire gli attacchi di phishing.

5. Scenari di rischio:

Scenari di rischio basati sulle minacce identificate e sulle lacune nei controlli di sicurezza:

Scenario di rischio: Accesso non autorizzato ai dati sensibili:

- ***Descrizione***: Un attaccante esterno utilizza un attacco di phishing per ottenere le credenziali di accesso di un dipendente dell'azienda TechnoCorp. Sfruttando queste credenziali, l'attaccante accede al sistema interno dell'azienda e ottiene accesso non autorizzato ai dati sensibili dei clienti.
- ***Impatto potenziale***: Violazione della privacy dei dati, danni alla reputazione dell'azienda, perdita di fiducia dei clienti, conseguenze legali e finanziarie.

Scenario di rischio: Compromissione dei dati aziendali attraverso dispositivi personali non controllati:

- ***Descrizione***: Un dipendente di TechnoCorp utilizza un dispositivo personale non gestito per accedere ai dati aziendali sensibili, come e-mail o documenti aziendali, senza l'implementazione di misure di sicurezza adeguate sul dispositivo personale. Successivamente, il dispositivo viene compromesso da un attaccante, consentendo l'accesso non autorizzato ai dati aziendali.
- ***Impatto potenziale***: Esposizione dei dati aziendali sensibili, perdita di proprietà intellettuale, rischio di violazioni della conformità normativa, danni alla reputazione dell'azienda.

Scenario di rischio: Violazione della sicurezza del cloud pubblico:

- ***Descrizione***: Un attaccante sfrutta una vulnerabilità nella configurazione di un servizio cloud pubblico utilizzato da TechnoCorp per ottenere accesso non autorizzato ai dati aziendali ospitati nel cloud. L'attaccante potrebbe modificare o eliminare dati sensibili, causando gravi danni all'azienda.
- ***Impatto potenziale***: Perdita di dati aziendali sensibili, compromissione della sicurezza delle informazioni, perdita di reputazione e fiducia dei clienti, possibili conseguenze legali e finanziarie.

Scenario di rischio: Attacco DDoS contro il sito web aziendale:

- ***Descrizione***: Un gruppo di hacker esegue un attacco DDoS (Distributed Denial of Service) contro il sito web di TechnoCorp, sovraccaricando i server e rendendo il sito inaccessibile agli utenti legittimi. Questo potrebbe essere un tentativo di estorsione o sabotaggio da parte di concorrenti o attaccanti senza scrupoli.
- ***Impatto potenziale***: Interruzione delle operazioni aziendali, perdita di clienti e opportunità di business, danni alla reputazione dell'azienda, perdite finanziarie dovute alla mancata disponibilità dei servizi online.

Scenario di rischio: Abusi interni di privilegi:

- ***Descrizione***: Un dipendente di TechnoCorp, con accesso privilegiato all'infrastruttura IT dell'azienda, utilizza le proprie credenziali per scopi fraudolenti o dannosi. Questo potrebbe includere la manipolazione o la cancellazione di dati critici, compromettendo la sicurezza e l'integrità dei sistemi aziendali.
- ***Impatto potenziale***: Interruzione delle operazioni aziendali, perdita di dati critici, danni alla reputazione dell'azienda, conseguenze legali e finanziarie, perdita di fiducia dei clienti e dei partner commerciali.

- ***Analisi del rischio semi-quantitativa:***

Identificazione dei rischi:

Possibile accesso non autorizzato ai dati sensibili a causa di vulnerabilità nel software e nelle configurazioni di sicurezza.

Analisi dei rischi:

Probabilità: Utilizzando dati di settore e statistiche sulla frequenza degli incidenti di sicurezza informatica nel settore IT, la probabilità di una violazione dei dati a causa di accesso non autorizzato può essere stimata intorno al 50% all'anno.

Impatto finanziario:

Secondo uno studio condotto da IBM Security, il costo medio di una violazione dei dati nel settore IT può essere di circa 3,86 milioni di dollari. Tuttavia, il costo effettivo potrebbe variare a seconda della gravità e delle circostanze specifiche dell'incidente.

Frequenza delle violazioni dei dati: Analizzando le tendenze del settore, è possibile stimare che un'azienda come TechnoCorp potrebbe subire una violazione dei dati ogni 1-2 anni.

Calcolo dell'ALE (Annualized Loss Expectancy):

Single Loss (SL): Utilizzando il costo medio di una violazione dei dati nel settore IT come riferimento, ad esempio 3,86 milioni di dollari.

Annual Rate of Occurrence (ARO): Stimato intorno a 0,5-1 incidenti all'anno, in base all'analisi delle tendenze del settore.

ALE: ALE = SL x AR0

ALE = 3,86 milioni di dollari x 0,5 = 1,93 milioni di dollari

Quindi, l'Annualized Loss Expectancy (ALE) è stimato essere di circa 1,93 milioni di dollari all'anno.

Analisi dell'impatto (IA):

IA: IA = ALE / Fatturato annuale

Utilizzando il fatturato annuale di TechnoCorp, ad esempio 100 milioni di dollari (dato stimato).

IA = 1,93 milioni di dollari / 100 milioni di dollari = 0,0193

L'Analisi dell'impatto indica che circa il 1,93% del fatturato annuale dell'azienda è potenzialmente a rischio a causa delle violazioni dei dati.

Le tabelle G-4, H-3 e I-2 sono parte del documento NIST SP 800-30 Rev. 1, che è una guida pubblicata dall'National Institute of Standards and Technology (NIST) degli Stati Uniti. Questo documento fornisce linee guida per la gestione del rischio informatico e il ***processo di valutazione del rischio***.

Secondo la tabella G-4, la probabilità del verificarsi di un evento in un anno pari al 50%, rappresenta un ***rischio moderato***.

Secondo la tabella H-3, un'analisi dell'impatto pari a 1,93% rappresenta un ***rischio molto basso***.

Unendo le informazioni ottenute nelle tabelle G-4 e H-3, vediamo come nella tabella I-2, questi dati ci indichino come questa analisi ci ha fatto capire che ***il rischio*** che abbiamo identificato ***ha un valore molto basso***.