IT RISK ASSESSMENT PLAN

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

• 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.

PROJECT OWNERSHIP

Project Ownership Document

Titolo del Progetto: Risk Assessment per TechnoCorp nel settore IT

Obiettivo del Progetto: Condurre un'analisi dettagliata dei rischi per TechnoCorp, un'azienda nel settore IT, identificando e valutando potenziali minacce alla sicurezza dei dati e dei servizi IT critici. Il progetto mira a fornire raccomandazioni per migliorare le misure di sicurezza esistenti e ridurre al minimo l'impatto di potenziali vulnerabilità.

Milestone del Progetto:

1. Analisi degli asset e delle vulnerabilità (durata stimata: 2 settimane)
2. Identificazione delle minacce e modellazione dei rischi (durata stimata: 3 settimane)
3. Scenari di rischio e analisi del rischio qualitativa (durata stimata: 2 settimane)
4. Raccomandazioni e presentazione dei risultati (durata stimata: 1 settimana)

Note Aggiuntive:

- Il progetto sarà svolto in conformità alle normative sulla privacy e alla politica aziendale.
- Tutti i dati sensibili e le informazioni aziendali saranno trattati in modo confidenziale e protetti da accessi non autorizzati.
- Durante lo svolgimento del progetto, si farà riferimento alle normative e alle linee guida riconosciute a livello internazionale per la gestione dei rischi informatici, inclusi il NIST SP800-30 Revision 1, il NIST SP800-53 Revision 4 e il NIST SP800-53A Revision 4 per definire le metodologie di risk assessment e le misure di sicurezza consigliate.

- Inoltre, per la valutazione dei rischi, si farà riferimento alle tabelle dell'Appendice D della normativa ISO/IEC 27005:2018 per garantire un approccio completo e accurato alla gestione dei rischi informatici e alla protezione dei dati sensibili.

Definizione del contesto

Obiettivi Aziendali

Gli obiettivi aziendali di TechnoCorp riflettono una serie di priorità chiave per l'azienda, tutte finalizzate a garantire un ambiente operativo sicuro e affidabile.

Questi si concentrano sulla protezione dei dati dei clienti, l'affidabilità dei servizi IT, la conformità normativa, la gestione dei rischi e la continuità operativa, al fine di mantenere la fiducia dei clienti, garantire la sicurezza delle informazioni e promuovere la crescita e la sostenibilità dell'azienda nel lungo termine.

Protezione dei dati dei clienti: La massima priorità è garantire la protezione e la riservatezza dei dati sensibili dei nostri clienti, inclusi quelli finanziari e personali.

Affidabilità dei servizi IT: Un altro obiettivo chiave è fornire servizi IT affidabili e di alta qualità ai nostri clienti. La nostra reputazione dipende dalla capacità di offrire soluzioni tecnologiche che siano stabili, efficienti e all'avanguardia

Conformità normativa: Dato il nostro ruolo nella gestione di dati sensibili, garantire la conformità alle normative e alle regolamentazioni del settore IT è fondamentale. Ci impegniamo a rispettare rigorosamente le leggi e i regolamenti pertinenti per proteggere la privacy e la sicurezza delle informazioni.

Gestione dei rischi: Cerchiamo di identificare e mitigare attivamente i rischi potenziali per la sicurezza dei dati e dei servizi IT.

Continuità operativa: Infine, un obiettivo critico è garantire la continuità operativa dell'azienda in qualsiasi circostanza, comprese situazioni di emergenza o crisi.

Analisi degli asset

Lo scopo di un documento per l'identificazione degli asset è fornire una guida dettagliata e strutturata per individuare e catalogare tutti gli asset rilevanti per un'organizzazione. Questo documento serve a garantire una comprensione chiara e completa degli asset disponibili, consentendo all'organizzazione di gestirli in modo efficace, proteggerli adeguatamente e assegnare loro le risorse necessarie per massimizzare il loro valore e mitigare i rischi associati.

Dopo un confronto con i responsabili dei vari reparti aziendali è stato possibile definire in questo report i vari asset presenti in azienda. Questi sono stati classificati in 5 categorie:

- Dati sensibili aziendali e dei clienti
- Dispositivi aziendali : Server interni, Laptop e Workstation
- Dispositivi personali dei dipendenti
- Infrastruttura di rete e sistemi di sicurezza

Ogni categorie è stata riportata in tabella, per ogni asset definito vengono riportati una serie di parametri, questi possono differire a seconda della categoria di asset in considerazione.

Dati sensibili dei clienti

Questa categoria di asset include i dati sensibili dei clienti come informazioni finanziarie, personali e la proprietà intellettuale dei clienti. I dati sensibili dell’azienda comprendono informazioni finanziarie interne, piani strategici e operativi, documentazione confidenziale e dettagli sui dipendenti. Queste informazioni sono gestite e trattate dall'azienda nell'ambito delle sue attività di consulenza, sviluppo software e gestione di infrastrutture tecnologiche. La protezione di tali dati è di fondamentale importanza per TechnoCorp, in quanto la loro compromissione potrebbe avere gravi conseguenze sia per la fiducia dei clienti che per la conformità normativa.

Categorie	Informazioni
Dati sensibili dei clienti	▪ informazioni finanziarie ▪ informazioni personali ▪ proprietà intellettuale
Dati sensibili dell’azienda	▪ Informazioni finanziarie ▪ Piani strategici e operativi ▪ Documentazione confidenziale ▪ Informazione sui dipendenti

Dispositivi Aziendali : Server interni, Laptop e workstation

Gli asset classificati come Dispositivi aziendali rappresentano componenti cruciali dell'infrastruttura IT di TechnoCorp. Questi includono i nostri server interni, che costituiscono l'elemento vitale per le nostre applicazioni aziendali e i nostri database, insieme ai laptop e alle workstation utilizzati dai nostri dipendenti per lo sviluppo software e le attività di consulenza.

Server Interni

TechnoCorp, essendo un'azienda di medie dimensioni con circa 500 dipendenti, presenta una configurazione di server interni composta da un numero sufficiente di unità per gestire le applicazioni aziendali critiche e i database.

La configurazione di base include 8 server, suddivisi :

Server dei Database (2):

Due server dedicati rispettivamente alla gestione del database aziendale e quello dei clienti, garantendo prestazioni ottimali e affidabilità per le operazioni di archiviazione e accesso ai dati.

Server delle Applicazioni (1):

Un server dedicato all'esecuzione delle applicazioni aziendali critiche, fornendo un ambiente stabile e scalabile per garantire la disponibilità dei servizi IT.

Server di Archiviazione (1):

Un server dedicato alla gestione e all'archiviazione dei dati, assicurando una conservazione sicura e organizzata delle informazioni aziendali.

Server di Backup (1):

Un server dedicato ai backup dei dati critici dell'azienda, garantendo la disponibilità di copie di sicurezza per la ripristino in caso di perdita o danneggiamento dei dati primari.

Server di Gestione di Rete (1):

Un server dedicato alla gestione e al monitoraggio della rete aziendale, assicurando un controllo efficace e una sicurezza ottimale delle comunicazioni e dei dati trasmessi.

Server di Autenticazione e Autorizzazione (1):

Un server dedicato alla gestione delle credenziali di accesso e delle autorizzazioni degli utenti, garantendo la sicurezza e l'integrità dell'accesso ai sistemi e ai dati aziendali.

Asset	Quantità	Funzione	Priorità	Criticità
Server	1	Database 1	Alta	Critico
Server	1	Database 2	Alta	Critico
Server	1	applicazioni	Media	Alto
Server	1	Archiviazione	Alta	Medio
Server	1	Backup	Media	Basso
Server	1	Gestione della Rete	Media	Medio
Server	1	Autenticazione e Autorizzazione	Media	Alto

Laptop e workstation

Per quanto riguarda i laptop e le workstation, data la varietà di attività svolte dai nostri dipendenti e la necessità di fornire strumenti di lavoro adeguati, l'azienda presenta un quantitativo di dispositivi abbastanza ampio. L'azienda dispone di 400 laptop e workstation in totale, distribuiti tra i dipendenti nelle nostre varie sedi.

Laptop per sviluppatori dipendenti e consulenti: 220 unità

Questi laptop sono destinati ai dipendenti che svolgono attività di sviluppo software, ufficio e consulenza tecnologica.

Workstation per dipendenti amministrativi e sviluppatori: 120 unità

Queste workstation sono destinate ai dipendenti che svolgono principalmente compiti amministrativi nei vari reparti, come la gestione dei documenti, lo sviluppo software, la contabilità e le comunicazioni interne.

Laptop per personale di supporto tecnico: 40 unità

Questi laptop sono destinati al personale addetto al supporto tecnico, che potrebbe necessitare di dispositivi portatili per assistere i clienti in loco o per risolvere problemi tecnici in diversi ambienti.

Laptop per la direzione e il personale dirigenziale: 20 unità

Questi laptop sono riservati alla direzione e al personale dirigenziale dell'azienda, che potrebbero richiedere dispositivi con caratteristiche specifiche per supportare le loro responsabilità decisionali e di gestione.

Asset	Quantità	Funzione	Priorità	Criticità
Laptop	220	Sviluppo software Office Conculenti	Alta	Alta
Workstation	120	Attività amministrative Sviluppo Software	Media	Critico
Laptop	40	Supporto e Assistenza tecnica	Media	Bassa
Laptop	20	Personale dirigenziale, Direzione	Alta	Alta

Dispositivi personali dei dipendenti

I dispositivi personali dei dipendenti, noti come dispositivi Bring Your Own Device (BYOD), rappresentano una componente significativa dell'ambiente IT di TechnoCorp.

La suddivisione e la classificazione di tali dispositivi in base al ruolo dei dipendenti può essere organizzata come segue:

- Dispositivi BYOD per Sviluppatori e Consulenti
- Dispositivi BYOD per Personale Amministrativo
- Dispositivi BYOD per Supporto Tecnico

Asset	Quantità	Criticità
Dispositivi BYOD per Sviluppatori e Consulenti	140	Media
Dispositivi BYOD per Personale Amministrativo	50	Alta
▪ Dispositivi BYOD per Supporto Tecnico	10	Bassa

Infrastruttura di Rete e Protezioni di Sicurezza

Gli asset classificati come infrastruttura di rete e sistemi di sicurezza sono fondamentali per garantire la sicurezza e il corretto funzionamento dell'ambiente IT all'interno dell'azienda.

La rete aziendale, che collega i vari server ospitanti applicazioni critiche, database e sistemi di archiviazione dati, costituisce il fondamento su cui si basano le operazioni aziendali. In aggiunta alla rete aziendale, la presenza di una rete wireless per dipendenti e ospiti offre flessibilità e accessibilità ai servizi aziendali, consentendo ai dipendenti di connettersi da dispositivi mobili e agli ospiti di accedere temporaneamente alla rete.

Il firewall perimetrale svolge un ruolo cruciale nella protezione della rete aziendale, filtrando il traffico in entrata e in uscita per prevenire attacchi informatici e intrusioni non autorizzate. Inoltre, l'implementazione di sistemi di rilevamento e risposta agli endpoint (EDR/xDR) su tutti i sistemi aziendali consente di monitorare e proteggere attivamente i dispositivi endpoint da minacce informatiche.

La distribuzione dei dispositivi di rete è come segue:

- Switch: 20 unità
- Router: 5 unità
- Access Point Wireless: 10 unità
- Firewall Perimetrale: 1 unità

Asset	Priorità	Criticità
Switch	Alta	Medio
Router	Alta	Medio
Access Point Wireless	Media	Alto
Firewall	Alta	Critico
EDR/XDR	Alta	Alta

Analisi delle Vulnerabilità

Nella seguente sezione, analizzeremo le vulnerabilità che possono minacciare la sicurezza degli asset informatici identificati all'interno dell'azienda. Attraverso questa analisi, faremo presente le potenziali vulnerabilità che possono compromettere la sicurezza degli asset e forniremo raccomandazioni per mitigare tali rischi e proteggere l'integrità, la riservatezza e la disponibilità delle risorse aziendali.

L'analisi delle vulnerabilità nell'ambiente IT di TechnoCorp riveste un ruolo fondamentale nella valutazione complessiva della sicurezza dell'azienda. Considerando la complessità e la varietà dei sistemi e delle infrastrutture presenti, è essenziale identificare e valutare accuratamente le possibili vulnerabilità che potrebbero compromettere la sicurezza dei dati e delle risorse aziendali. Tra le principali vulnerabilità identificate, si evidenziano le seguenti:

Configurazioni errate o non ottimali: Le impostazioni di configurazione di sistema e/o servizi non corrette o non ottimali su dispositivi di rete, server e sistemi di sicurezza potrebbero esporre l'azienda a rischi di sicurezza, consentendo a potenziali attaccanti di sfruttare falle nel sistema.

Mancanza di patch e aggiornamenti: La mancata applicazione di patch e aggiornamenti di sicurezza su sistemi operativi, applicazioni e dispositivi di rete potrebbe lasciare l'azienda vulnerabile a minacce informatiche note e sfruttabili.

Compromissione del fornitore cloud: Un possibile attacco al fornitore dei servizi cloud potrebbe rendere i dati sensibili accessibili, ciò renderebbe vulnerabile l’azienda.

Minacce interne: Anche le minacce interne, come gli errori umani o il comportamento scorretto dei dipendenti, rappresentano un rischio significativo per la sicurezza dell'azienda e devono essere considerate nell'analisi delle vulnerabilità.

Furto/perdita dei dispositivi personali: Il furto o la perdita di un dispositivo personale aziendale può rendere vulnerabile l’azienda compromettendo la riservatezza dei dati.

Un vulnerability assessment o un penetration testing effettuati dall’aziende o da aziende terze possono aiutare a identificare possibili vulnerabilità non riscontrate.

Analisi delle minacce

Diverse minacce possono compromettere la sicurezza degli asset identificati. Queste minacce possono provenire da fonti esterne o interne e rappresentare un rischio significativo per l'integrità, la riservatezza e la disponibilità dei dati e delle risorse aziendali.

Minacce esterne

Potenziali attaccanti esterni potrebbero mirare a compromettere la rete aziendale di TechnoCorp al fine di accedere ai dati sensibili dei clienti o interrompere le operazioni aziendali. Le minacce potrebbero includere :

- Attacchi DDoS: sovraccaricare i server aziendali, limitandone o bloccando il servizio.
- Phishing: campagna di phishing ai dipendenti attraverso le e-mail o campagna di spearphishing verso le figure senior dell'azienda
- Sniffing di Rete: lo sniffing dei pacchetti di rete delle comunicazioni wireless potrebbe essere utilizzato per ottenere credenziali di accesso o altri dati riservati
- Ransomware: questo tipo di malware potrebbe compromettere la reputazione e i dati aziendali

Come minacce esterne vengono considerati anche i disastri naturali, quali terremoto e alluvioni.

Minacce interne

Le minacce interne, come errori umani o comportamenti scorretti dei dipendenti, potrebbero rappresentare un rischio significativo per la sicurezza dell'azienda. Queste minacce potrebbero includere:

- la condivisione non autorizzata di informazioni sensibili
- mancata adozione delle politiche di sicurezza dell'azienda
- Danni intenzionali e non ai dispositivi aziendali
- Possibili Incendi

Minacce di terze parti

Le minacce di terze parti rappresentano una preoccupazione significativa per la sicurezza informatica di TechnoCorp, specialmente considerando l'utilizzo di servizi cloud per alcune delle sue operazioni IT. Il trasferimento di dati e risorse aziendali verso ambienti cloud esterni espone l'azienda a diverse minacce potenziali.

Tra queste, vi sono rischi legati alla compromissione della sicurezza da parte dei fornitori di servizi cloud, che potrebbero includere

- violazioni dei dati,
- accessi non autorizzati ai sistemi
- interruzioni del servizio.

Modellazione delle minacce

Nel processo di modellazione delle minacce utilizziamo il framework DREAD per valutare le potenziali minacce identificate nel contesto di TechnoCorp:

Minacce esterne

Attacchi DDoS (Denial of Service):

D (Damage Potential - Potenziale Danno): Questa minaccia presenta un alto potenziale di danni in quanto può interrompere o limitare significativamente i servizi aziendali, causando perdite finanziarie e danni reputazionali.

R (Reproducibility - Riproducibilità): Gli attacchi DDoS sono riproducibili e possono essere eseguiti da più fonti contemporaneamente, aumentando la probabilità di successo.

E (Exploitability - Sfruttabilità): Gli attacchi DDoS sono relativamente facili da eseguire, con strumenti e metodi ampiamente disponibili online per perpetrare l'attacco.

A (Affected Users - Utenti Colpiti): L'intera azienda e i suoi clienti possono essere colpiti dagli attacchi DDoS, con un impatto diffuso e significativo sull'accessibilità dei servizi.

D (Discoverability - Facilità di Rilevamento): Gli attacchi DDoS sono generalmente facili da rilevare poiché causano anomalie nei flussi di traffico di rete.

Phishing e Spearphishing:

D (Damage Potential - Potenziale Danno): Queste minacce hanno un alto potenziale di danni poiché possono portare al furto di credenziali sensibili e alla compromissione dei dati aziendali.

R (Reproducibility - Riproducibilità): Le campagne di phishing e spearphishing sono facilmente riproducibili e possono essere indirizzate a un vasto pubblico o a individui specifici all'interno dell'azienda.

E (Exploitability - Sfruttabilità): Gli attacchi di phishing richiedono l'inganno delle vittime per avere successo, ma sono spesso efficaci a causa della manipolazione psicologica e dell'ingegneria sociale.

A (Affected Users - Utenti Colpiti): Gli utenti aziendali a tutti i livelli, in particolare quelli con accesso a informazioni sensibili, sono potenzialmente vulnerabili a queste minacce.

D (Discoverability - Facilità di Rilevamento): Il phishing può essere difficile da rilevare in quanto gli attaccanti cercano di mascherare le loro attività e rendere le e-mail di phishing simili a quelle legittime.

Sniffing di Rete:

D (Damage Potential - Potenziale Danno): Il sniffing di rete può portare al furto di dati sensibili e all'esposizione delle comunicazioni aziendali, con potenziali conseguenze finanziarie e reputazionali.

R (Reproducibility - Riproducibilità): Gli attacchi di sniffing possono essere eseguiti in modo continuo e ripetuto su reti vulnerabili, con un alto grado di riproducibilità.

E (Exploitability - Sfruttabilità): Il sniffing di rete richiede un accesso fisico o logico alla rete aziendale, ma è relativamente semplice da eseguire con strumenti software appropriati.

A (Affected Users - Utenti Colpiti): Tutti gli utenti della rete aziendale sono potenzialmente colpiti dallo sniffing di rete, con un'ampia esposizione dei dati e delle comunicazioni.

D (Discoverability - Facilità di Rilevamento): Il rilevamento dello sniffing di rete può essere difficile poiché gli attacchi avvengono spesso in modo silenzioso e non lasciano tracce evidenti.

Ransomware:

D (Damage Potential - Potenziale Danno): Il ransomware rappresenta una minaccia grave in termini di potenziale danno, poiché può crittografare i dati aziendali rendendoli inaccessibili e richiedere un pagamento per il ripristino. Ciò può causare perdite finanziarie, danni reputazionali e interruzioni delle operazioni aziendali.

R (Reproducibility - Riproducibilità): Questa minaccia è altamente riproducibile, poiché il ransomware può essere distribuito in modo automatizzato tramite e-mail di phishing, exploit di vulnerabilità o altri mezzi. Una volta che un sistema è compromesso, il ransomware può diffondersi rapidamente attraverso la rete aziendale.

E (Exploitability - Sfruttabilità): Il ransomware è relativamente semplice da sfruttare, poiché richiede solo l'esecuzione di un file dannoso da parte dell'utente o l'exploit di una vulnerabilità nel sistema. Gli attaccanti possono utilizzare kit di exploit pronti all'uso o metodi di ingegneria sociale per distribuire il ransomware.

A (Affected Users - Utenti Colpiti): Tutti gli utenti aziendali che utilizzano i sistemi compromessi sono potenzialmente colpiti dal ransomware. Ciò include dipendenti di tutti i livelli, amministratori di sistema e altri utenti con accesso ai dati critici.

D (Discoverability - Facilità di Rilevamento): Il ransomware può essere difficile da rilevare fino a quando non cifra i dati e visualizza il messaggio di richiesta di riscatto.

Minacce interne:

Condivisione non autorizzata di informazioni sensibili:

D (Damage Potential - Potenziale Danno): La condivisione non autorizzata di informazioni sensibili può compromettere la riservatezza dei dati e causare danni finanziari e reputazionali all'azienda.

R (Reproducibility - Riproducibilità): Questa minaccia è altamente riproducibile, poiché dipende dall'azione umana e può verificarsi in varie forme e contesti.

E (Exploitability - Sfruttabilità): È relativamente semplice per i dipendenti con accesso ai dati sensibili condividerli in modo non autorizzato, specialmente se le politiche e le procedure aziendali sono deboli.

A (Affected Users - Utenti Colpiti): Gli utenti interni con accesso ai dati sensibili, compresi i dipendenti di tutti i livelli, possono essere coinvolti in questa minaccia.

D (Discoverability - Facilità di Rilevamento): La condivisione non autorizzata di informazioni può essere difficile da rilevare se non ci sono controlli adeguati sui flussi di dati e sui comportamenti degli utenti.

Mancata adozione delle politiche di sicurezza dell'azienda:

D (Damage Potential - Potenziale Danno): La mancata adozione delle politiche di sicurezza può aumentare il rischio di violazioni della sicurezza e compromettere l'integrità dei dati aziendali.

R (Reproducibility - Riproducibilità): Questa minaccia è altamente riproducibile in quanto dipende dal comportamento e dalla conformità dei dipendenti alle politiche di sicurezza.

E (Exploitability - Sfruttabilità): È relativamente semplice per i dipendenti non aderire alle politiche di sicurezza, specialmente se non sono chiaramente comunicate o supportate da una formazione adeguata.

A (Affected Users - Utenti Colpiti): Tutti gli utenti interni dell'azienda sono coinvolti in questa minaccia.

D (Discoverability - Facilità di Rilevamento): Il rilevamento della mancata adozione delle politiche di sicurezza può essere difficile senza monitoraggio attivo e audit delle attività dei dipendenti.

Minacce di terze parti:

Violazioni dei dati nei servizi cloud:

D (Damage Potential - Potenziale Danno): Le violazioni dei dati nei servizi cloud possono causare danni finanziari e reputazionali significativi all'azienda, compromettendo la riservatezza e l'integrità dei dati.

R (Reproducibility - Riproducibilità): Questa minaccia è altamente riproducibile, poiché dipende dalla sicurezza dei servizi cloud utilizzati e dalla capacità degli attaccanti di sfruttarli.

E (Exploitability - Sfruttabilità): È relativamente semplice per gli attaccanti sfruttare le vulnerabilità nei servizi cloud per accedere ai dati aziendali, specialmente se non sono implementati adeguati controlli di sicurezza.

A (Affected Users - Utenti Colpiti): Gli utenti aziendali che utilizzano o hanno accesso ai dati nei servizi cloud sono potenzialmente colpiti da questa minaccia.

D (Discoverability - Facilità di Rilevamento): Il rilevamento delle violazioni dei dati nei servizi cloud può essere difficile senza una monitoraggio costante dei flussi di dati e delle attività degli utenti.

Scenario di rischio

Gli scenari di rischio presi in esame sono stati valutati a seguito di un analisi qualitativa.

Minaccia	Probabilità di Occorrenza	Livello di Impatto	Rischio
Attacchi DDoS	Alta	Alto	Alto
Phishing	Medio	Alto	Alto
Sniffing di Rete	Medio	Medio	Medio
Ransomware	Medio	Alto	Alto
Disastri Naturali	Basso	Molto Alto	Medio
Condivisione non Autorizzata	Medio	Medio	Medio
Mancata Adozione delle Politiche di Sicurezza	Alto	Alto	Alto
Possibili Incendi	Basso	Molto Alto	Medio
Violazioni dei Dati nei Servizi Cloud	Alto	Alto	Alto

Considerando la tabella che racchiude l’analisi delle minacce sono stati presi in esame gli scenari con la probabilità di occorrenza più alta, questi sono:

- Attacchi DDoS
- Mancata Adozione delle Politiche di Sicurezza
- Violazioni dei Dati nei Servizi Cloud
- Scenario relativo ai dispositivi BYOD

Per ognuno di questi sono state prese di riferimento le normative ISO 27005:2018 e NIST SP800-30r con le rispettive tabelle per definire un quadro di rischio per ogni possibile scenario in esame

Possibile attacco DDoS

Un attacco DDoS (Distributed Denial of Service) è un tipo di attacco informatico in cui un aggressore cerca di sovraccaricare i server, i servizi o le reti di un'organizzazione con una grande quantità di traffico illegittimo. Questo bombardamento di richieste di accesso rende i servizi e le risorse inaccessibili agli utenti legittimi, causando interruzioni significative e danni all'operatività dell'azienda.

I danni causati da un attacco DDoS possono essere estremamente gravi. Possono includere l'interruzione delle operazioni aziendali, la perdita di clienti a causa della mancata disponibilità dei servizi, danni alla reputazione dell'azienda e possibili perdite finanziarie. Inoltre, un attacco DDoS può distrarre le risorse IT dall'affrontare altre minacce o attività critiche, compromettendo ulteriormente la sicurezza complessiva dell'organizzazione.

Per mitigare o prevenire gli attacchi DDoS, è fondamentale implementare controlli e misure di sicurezza efficaci. Prendendo spunto dalle tabelle delle normative NIST SP 800-53r e SP800-53Ar, alcune raccomandazioni potrebbero includere:

Implementazione di Filtri DDoS: Utilizzare dispositivi di rete e firewall (WAF) in grado di rilevare e filtrare il traffico DDoS in arrivo, limitando l'impatto degli attacchi.

Monitoraggio del Traffico di Rete: Utilizzare strumenti di monitoraggio del traffico di rete per rilevare anomalie e pattern di traffico sospetti, consentendo una risposta tempestiva agli attacchi DDoS in corso.

Ridondanza e Bilanciamento del Carico: Distribuire i servizi su più server e infrastrutture per ridurre il rischio di interruzioni dovute a un singolo attacco DDoS e utilizzare il bilanciamento del carico per gestire in modo efficiente il traffico.

Pianificazione di Risposta agli Incidenti: Implementare un piano di risposta agli incidenti dettagliato che includa procedure per gestire gli attacchi DDoS in corso, comprese le modalità di comunicazione con i fornitori di servizi Internet e le autorità competenti.

Mancata Adozione delle Politiche di Sicurezza

In questo scenario, un dipendente interno potrebbe essere ingannato da e-mail fasulle o siti web fraudolenti, compromettendo involontariamente le credenziali di accesso o consentendo l'accesso non autorizzato a sistemi o dati sensibili. Questo può portare a violazioni della sicurezza, perdita di dati sensibili, danni alla reputazione e perdite finanziarie per l'azienda. Gli insider possono rappresentare una minaccia particolarmente insidiosa poiché già hanno accesso privilegiato ai sistemi e ai dati aziendali.

Controlli e Raccomandazioni per la Mitigazione:

Consapevolezza e Formazione del Personale: Fornire formazione regolare sulle pratiche di sicurezza informatica e sulla consapevolezza del phishing per educare i dipendenti sugli schemi di attacco e come riconoscerli.

Politiche di Sicurezza dei Dati: Implementare politiche di sicurezza dei dati che regolamentino l'accesso e l'uso dei dati sensibili e definiscano procedure per la gestione delle credenziali e delle autorizzazioni.

Autenticazione Multifattore (MFA) e politiche di gestione delle password: Entrambe tecniche utilizzate dall'azienda per mitigare possibili accessi non autorizzati e salvaguardia delle password.

Monitoraggio delle Attività Utente: Implementare strumenti di monitoraggio delle attività degli utenti per rilevare comportamenti anomali o accessi non autorizzati ai sistemi e ai dati sensibili.

Verifica delle E-mail: Utilizzare filtri antispam e soluzioni di verifica delle e-mail per identificare e bloccare messaggi di phishing prima che raggiungano i destinatari.

Implementando queste misure di sicurezza e promuovendo una cultura aziendale consapevole della sicurezza, è possibile mitigare il rischio di attacchi di phishing e proteggere i dati aziendali sensibili dagli insider minacciosi.

Violazioni dei Dati nei Servizi Cloud

Le violazioni dei dati nei servizi cloud rappresentano una minaccia significativa per la sicurezza delle informazioni aziendali quando i dati sensibili vengono archiviati o elaborati su piattaforme cloud esterne. Queste violazioni possono includere accessi non autorizzati ai dati, perdite di dati, esfiltrazione di dati sensibili e interruzioni del servizio. Le conseguenze possono essere gravi e includere danni alla reputazione dell'azienda, perdite finanziarie e possibili sanzioni legali.

Controlli e Raccomandazioni per la Mitigazione:

Valutazione del Fornitore di Servizi Cloud: Condurre valutazioni approfondite dei fornitori di servizi cloud per garantire che rispettino gli standard di sicurezza e protezione dei dati e che dispongano di adeguate misure di sicurezza in loco.

Crittografia dei Dati: Utilizzare la crittografia dei dati per proteggere le informazioni sensibili durante la memorizzazione e il trasferimento su piattaforme cloud, garantendo che solo gli utenti autorizzati possano accedervi.

Gestione degli Accessi e delle Autorizzazioni: Implementare controlli rigorosi per gestire gli accessi e le autorizzazioni agli ambienti cloud, garantendo che solo gli utenti autorizzati possano accedere ai dati sensibili e che i privilegi di accesso siano limitati al minimo necessario.

Backup e Ripristino dei Dati: Eseguire regolarmente backup dei dati archiviati su piattaforme cloud e stabilire procedure per il ripristino dei dati in caso di violazioni o perdite.

Dispositivi BYOD

L'azienda ha implementato una politica BYOD che consente ai dipendenti di utilizzare i propri dispositivi personali per accedere alle risorse aziendali. Tuttavia, questa flessibilità ha portato a una serie di sfide legate alla sicurezza delle informazioni.

Uno dei dipendenti di TechnoCorp utilizza il suo smartphone personale per accedere al sistema aziendale tramite una connessione Wi-Fi non protetta in un caffè locale o è cascato in un attacco di phishing.

Possibili Minacce e Vulnerabilità:

Malware sul Dispositivo: L'applicazione malevola installata sul dispositivo BYOD può rubare informazioni sensibili, come credenziali di accesso aziendali, o compromettere la sicurezza della rete aziendale.

Accesso non Autorizzato ai Dati Aziendali: L'utente potrebbe involontariamente consentire l'accesso non autorizzato ai dati aziendali memorizzati sul dispositivo BYOD a causa del malware presente.

Phishing e Inganno: Il dispositivo BYOD potrebbe essere vulnerabile agli attacchi di phishing o ingegneria sociale, mettendo a rischio la sicurezza delle credenziali di accesso aziendali.

Possibili Impatti:

Violazioni della Sicurezza dei Dati: Il malware sul dispositivo BYOD potrebbe causare violazioni della sicurezza dei dati aziendali, compromettendo la riservatezza e l'integrità delle informazioni sensibili.

Perdite Finanziarie e Danneggiamento della Reputazione: Una violazione dei dati aziendali a causa di un dispositivo BYOD compromesso potrebbe portare a perdite finanziarie e danneggiare la reputazione dell'azienda.

Il livello di rischio è stato classificato come “ Moderato “.

Controlli e Raccomandazioni per la Mitigazione:

Politiche BYOD Chiare e Definite: Implementare politiche BYOD chiare e definite che stabiliscano requisiti di sicurezza per i dispositivi personali utilizzati per scopi aziendali.

Formazione degli Utenti: Fornire formazione agli utenti sui rischi associati all'uso di dispositivi BYOD e sulle migliori pratiche per ridurre tali rischi.

Gestione dei Dispositivi Mobile: Implementare soluzioni di gestione dei dispositivi mobili (MDM) per monitorare e gestire dispositivi BYOD, inclusi controlli di sicurezza e politiche di accesso.