IDENTIFICAZIONEE ANALISI DEL RISCHIO PROGETTO S1L5

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.

- EDR/xDR sui sistemi:Costo di licenza annuale: $20.000
- Personale e accessi: Amministratori di sistema: Numero di amministratori: 5 Costo medio annuale per amministratore: $100.000 Valore totale: $500.000
- Sviluppatori: Numero di sviluppatori: 50 Costo medio annuale per sviluppatore: $80.000 Valore totale: $4.000.000
- Personale di supporto tecnico: Numero di tecnici: 10 Costo medio annuale per tecnico: $60.000 Valore totale: $600.000
- Consulenti esterni: Numero di consulenti: 20 Costo medio giornaliero per consulente: $1.000 Valore totale (per mese): $600.000

IDENTIFICAZIONE DEL RISCHIO: PROCESSO PER DETERMINARE E DOCUMENTARE IL RISCHIO CHE DEVE ESSERE AFFRONTATO.

- **Identificazione del rischio**: Un possibile rischio per TechnoCorp potrebbe essere un attacco di phishing mirato (spear phishing) ai suoi amministratori di sistema. Gli aggressori potrebbero cercare di ingannare gli amministratori per ottenere le loro credenziali di accesso e quindi ottenere l'accesso non autorizzato all'infrastruttura IT dell'azienda.

- **Analisi degli asset**: Gli asset coinvolti in questo scenario includono:

- **Amministratori di sistema**: Sono una risorsa critica per l'azienda poiché hanno accesso totale all'infrastruttura. Il loro valore può essere stimato considerando il costo della loro formazione, il loro salario e il costo per sostituirli in caso di perdita di fiducia o di licenziamento a seguito di un attacco riuscito.
- **Infrastruttura IT**: Include server interni, applicazioni aziendali critiche, database, sistemi di archiviazione dati, cloud pubblici (AWS, Azure), rete wireless, dispositivi personali (BYOD), laptop e workstation, sito web aziendale, firewall perimetrale e EDR/xDR. Il valore di questi asset può essere calcolato considerando il costo di acquisizione, manutenzione, aggiornamento e, in caso di compromissione, il costo di ripristino e di eventuale downtime.
- **Dati sensibili dei clienti**: Questi includono informazioni finanziarie, dati personali di dipendenti/clienti, proprietà intellettuale. Il valore di questi dati può essere molto elevato, considerando il potenziale impatto di una violazione dei dati sulla reputazione dell'azienda, la perdita di clienti, le possibili multe per la violazione delle leggi sulla privacy e il costo di gestire una violazione dei dati.

ANALISI DEGLI ASSET

- Dati sensibili dei clienti (finanziari, personali, proprietà intellettuale):
- Numero di record: 100.000 Valore medio per record: $500
- Valore totale: $50.000.000
- Infrastruttura IT: Server interni con dati aziendali critici: Numero di server: 10 Valore medio per server: $20.000
- Valore totale: $200.000
- Cloud pubblici (AWS, Azure): Costo mensile medio: $5.000 Rete wireless e dispositivi BYOD:
- Numero di dispositivi: 200 Valore medio per dispositivo: $1.000 Valore totale: $200.000
- Laptop e workstation: Numero di dispositivi: 300
- Valore medio per dispositivo: $2.000 Valore totale: $600.000
- Sito web aziendale: Costo annuale di hosting: $10.000
- Firewall perimetrale: Costo di implementazione: $50.000

Analisi delle vulnerabilità (VulnerabilityAnalysis)è un processo che processo che permette di identificare e classificare le vulnerabilità. La valutazione delle vulnerabilità potrebbe includere l'esame di tutti gli aspetti di un asset o capacità per determinare eventuali vulnerabilità presenti,comprese le vulnerabilità fisiche, tecniche e operative proprie dell'asset**.** : Le vulnerabilità potrebbero includere:

- **Email di phishing**: Gli amministratori di sistema potrebbero essere ingannati da email di phishing.
- **BYOD (Bring Your Own Device)**: I dispositivi personali potrebbero non essere adeguatamente protetti o aggiornati, rendendoli vulnerabili.
- **Accesso dei consulenti**: I consulenti e i collaboratori esterni potrebbero avere accesso all'infrastruttura IT, il che potrebbe presentare un rischio se le loro credenziali venissero compromesse.
- **Analisi delle minacce**: Le minacce potrebbero includere:

- **Attacchi di phishing**: Gli aggressori potrebbero cercare di ingannare gli amministratori per ottenere le loro credenziali.
- **Malware**: Potrebbe essere introdotto nell'infrastruttura IT attraverso email di phishing o dispositivi personali non protetti.
- **Attacchi DDoS**: Il sito web aziendale potrebbe essere preso di mira da attacchi DDoS.
- **Modellazione delle minacce**: Gli aggressori potrebbero essere hacker esterni che cercano di accedere ai dati sensibili dei clienti. Potrebbero utilizzare tecniche come il phishing e l'introduzione di malware per compromettere l'infrastruttura IT.

- **Scenari di rischio**: Uno scenario di rischio potrebbe essere un attacco di phishing riuscito che porta a un accesso non autorizzato all'infrastruttura IT. Questo potrebbe portare alla compromissione dei dati sensibili dei clienti, causando danni alla reputazione dell'azienda e possibili multe legali.

L'ANALISI DELLE MINACCE, ATTRAVERSO LA DEFINIZIONE DI PROBABILITÀ E IMPATTO, MIRA A STABILIRE UNA PRIORITÀ E CONCENTRARE GLI SFORZI SULLE MINACCE PIÙ RILEVANTI PER L'ORGANIZZAZIONE.

- **Attacchi di phishing**: Gli aggressori potrebbero cercare di ingannare gli amministratori per ottenere le loro credenziali.
- **Malware**: Potrebbe essere introdotto nell'infrastruttura IT attraverso email di phishing o dispositivi personali non protetti.
- **Attacchi DDoS**: Il sito web aziendale potrebbe essere preso di mira da attacchi DDoS.
- **Modellazione delle minacce**: Gli aggressori potrebbero essere hacker esterni che cercano di accedere ai dati sensibili dei clienti. Potrebbero utilizzare tecniche come il phishing,attacchi DDOS e l'introduzione di malware per compromettere l'infrastruttura IT.

MODELLAZIONE DELLE MINACCE (THREATMODELLING):PROCESSO DI IDENTIFICAZIONE DEI RISCHI CHE PREVEDE L'ESAME DI OGNI POSSIBILE ATTORE MALEVOLO,AZIONE O EVENTO,VETTORE DI ATTACCO E VULNERABILITÀ PER UN DETERMINATO SISTEMA,BENE O PROCESSO

- Phishing:
- Attaccante: Potrebbe essere un individuo malintenzionato o un gruppo di hacker che mira a ottenere accesso non autorizzato alle credenziali dei dipendenti o ai dati sensibili dell'azienda.
- Vettore di attacco: Gli attaccanti possono inviare e-mail o messaggi di testo contraffatti che sembrano provenire da fonti attendibili, come colleghi o partner commerciali. Questi messaggi potrebbero contenere link dannosi o allegati infetti.
- Rischio potenziale: Se un dipendente viene ingannato e fornisce le proprie credenziali o apre un file dannoso, gli attaccanti potrebbero ottenere accesso non autorizzato ai sistemi aziendali, ai dati sensibili dei clienti o alle informazioni finanziarie.
- Contromisure:
- Sensibilizzazione degli utenti: Formazione periodica sui rischi associati al phishing e all'importanza di verificare attentamente la provenienza dei messaggi e-mail.
- Filtraggio degli e-mail: Implementare filtri anti-phishing che riconoscono e bloccano messaggi sospetti prima che raggiungano le caselle di posta dei dipendenti.
- Autenticazione a due fattori: Richiedere l'autenticazione a due fattori per l'accesso a sistemi e dati sensibili, riducendo così l'efficacia dei tentativi di phishing.

DDoS (Distributed Denial of Service):

- Attaccante: Gruppi di hacker o individui con l'obiettivo di interrompere o compromettere i servizi online dell'azienda.
- Vettore di attacco: Gli attaccanti potrebbero sfruttare botnet o altri mezzi per sovraccaricare la rete aziendale o i server con un'elevata quantità di traffico, rendendo così i servizi inaccessibili agli utenti legittimi.
- Rischio potenziale: Un attacco DDoS potrebbe interrompere le operazioni aziendali, causando perdite finanziarie e danneggiando la reputazione dell'azienda.
- Contromisure:
- Implementazione di firewall e sistemi di rilevamento delle intrusioni (IDS/IPS) per filtrare il traffico dannoso in arrivo.
- Utilizzo di servizi di mitigazione DDoS forniti da fornitori terzi per proteggere la rete aziendale da picchi di traffico dannoso.
- Monitoraggio costante della rete per individuare anomalie nel traffico e rispondere prontamente agli attacchi in corso.

Malware:

- Attaccante: Hacker o gruppi di cybercriminali che distribuiscono software dannoso per compromettere i sistemi aziendali o rubare dati sensibili.
- Vettore di attacco: Il malware potrebbe essere distribuito tramite e-mail di phishing, siti web compromessi, dispositivi USB infetti o exploit di vulnerabilità dei software.
- Rischio potenziale: Il malware potrebbe compromettere i dati aziendali, danneggiare i sistemi IT, causare interruzioni delle operazioni e violare la privacy dei clienti.
- Contromisure:
- Utilizzo di software antivirus e antimalware aggiornati su tutti i dispositivi aziendali per rilevare e rimuovere minacce.
- Applicazione regolare di patch e aggiornamenti di sicurezza per proteggere i sistemi da vulnerabilità note.
- Limitazione dei privilegi di accesso per ridurre la superficie di attacco e mitigare gli effetti dei malware che ottengono l'accesso ai sistemi.

SCENARIO DI RISCHIO DOPOAVER IDENTIFICATO GLI ASSET, LE MINACCE, LE VULNERABILITÀ,POSSIAMO DEFINIRE LO SCENARIO DI RISCHIO,COME LA RAPPRESENTAZIONE TANGIBILE E VALUTABILE DEL RISCHIO

- Un gruppo di hacker mira a ottenere accesso non autorizzato ai sistemi e ai dati sensibili di TechnoCorp utilizzando un attacco di phishing mirato.
- **Attacco** : Gli hacker inviano e-mail contraffatte ai dipendenti di TechnoCorp, facendole sembrare provenire da fonti attendibili come colleghi o partner commerciali.
- Le e-mail contengono link malevoli o allegati infetti che sembrano legittimi, ad esempio un documento di Microsoft Word con macro dannose.
- Un dipendente ignaro apre l'e-mail e clicca sul link o apre l'allegato, consentendo agli hacker di compromettere il suo dispositivo e ottenere le sue credenziali di accesso.
- **Rischio Potenziale**: Gli hacker ottengono accesso non autorizzato ai sistemi e ai dati di TechnoCorp utilizzando le credenziali rubate.
- Possono esplorare l'infrastruttura IT dell'azienda, accedere a dati sensibili dei clienti come informazioni finanziarie o dati personali e compromettere la sicurezza complessiva dell'azienda.
- La reputazione dell'azienda potrebbe essere danneggiata e potrebbero subire perdite finanziarie a seguito della violazione dei dati.

Impatto:

- Perdita di dati sensibili:
- Gli hacker potrebbero accedere e rubare informazioni finanziarie dei clienti, dati personali dei dipendenti e proprietà intellettuale dell'azienda.
- Interruzione delle operazioni: Se gli hacker riescono a compromettere sistemi critici, potrebbe verificarsi un'interruzione delle operazioni aziendali, causando perdite finanziarie e danneggiando la fiducia dei clienti.
- Danno alla reputazione: Una violazione della sicurezza potrebbe danneggiare la reputazione di TechnoCorp e la fiducia dei clienti e dei partner commerciali nell'azienda. Possibili conseguenze legali: TechnoCorp potrebbe affrontare conseguenze legali, incluse sanzioni e multe, se la violazione dei dati viola le leggi sulla protezione dei dati.

Contromisure:Formazione sulla sicurezza informatica: Fornire formazione regolare ai dipendenti su come riconoscere e evitare gli attacchi di phishing.

- Filtraggio delle e-mail: Implementare filtri anti-phishing per bloccare e-mail sospette prima che raggiungano le caselle di posta dei dipendenti.
- Autenticazione a due fattori: Richiedere l'autenticazione a due fattori per l'accesso ai sistemi e ai dati sensibili, riducendo l'impatto delle credenziali compromesse.
- Monitoraggio degli accessi: Monitorare e registrare gli accessi ai sistemi per rilevare attività sospette e rispondere prontamente agli incidenti di sicurezza.

- Un gruppo di hacker o un individuo malintenzionato intende compromettere l'operatività e la sicurezza di TechnoCorp utilizzando un attacco DDoS e diffondendo malware attraverso la rete aziendale.

Attacco DDoS: Gli hacker utilizzano una botnet per lanciare un attacco DDoS contro i server di TechnoCorp, generando un volume massiccio di traffico dannoso che sovraccarica la rete e i server dell'azienda.Il flusso di traffico dannoso è così elevato che i sistemi di TechnoCorp diventano inaccessibili per gli utenti legittimi, causando interruzioni delle operazioni e perdite finanziarie.

Rischio Potenziale - Attacco DDoS:

- Interruzione dei servizi: Gli attacchi DDoS rendono inaccessibili i servizi online di TechnoCorp, inclusi il sito web aziendale, le applicazioni critiche e i servizi cloud, causando interruzioni delle operazioni e perdite finanziarie.
- Danno alla reputazione: L'incapacità di fornire servizi affidabili ai clienti danneggia la reputazione di TechnoCorp e la fiducia dei clienti nell'azienda.

Contromisure - Attacco DDoS:

- Servizi di mitigazione DDoS: Utilizzare servizi di mitigazione DDoS forniti da fornitori terzi per filtrare il traffico dannoso in arrivo e mantenere i servizi online durante gli attacchi.
- Monitoraggio del traffico di rete: Implementare sistemi di monitoraggio del traffico di rete per rilevare e rispondere prontamente agli attacchi DDoS in corso.
- Ridondanza dei server: Distribuire server ridondanti e scalabili per garantire la disponibilità dei servizi anche durante gli attacchi DDoS.

Attacco Malware:

- Gli hacker diffondono malware attraverso e-mail di phishing, siti web compromessi o dispositivi USB infetti, mirando ai dispositivi e ai sistemi di TechnoCorp.
- Il malware compromette i sistemi aziendali, ruba dati sensibili, danneggia i file di sistema e compromette la sicurezza complessiva dell'azienda.

Rischio Potenziale - Attacco Malware:

- Perdita di dati: Il malware potrebbe compromettere e rubare dati sensibili dei clienti, informazioni finanziarie, proprietà intellettuale e dati personali dei dipendenti di TechnoCorp.
- Danneggiamento dei sistemi: Il malware danneggia i file di sistema, compromette la sicurezza e l'integrità dei sistemi aziendali, causando interruzioni delle operazioni e perdite finanziarie.
- Violazione della privacy: La diffusione di malware può violare la privacy dei clienti e dei dipendenti, esponendoli al rischio di furto di identità e altri crimini informatici.

Contromisure - Attacco Malware:

- Software antimalware/antivirus: Utilizzare software antimalware e antivirus aggiornato su tutti i dispositivi e i sistemi aziendali per rilevare e rimuovere il malware.
- Aggiornamenti di sicurezza: Applicare regolarmente patch e aggiornamenti di sicurezza per proteggere i sistemi da vulnerabilità note e minacce di malware.
- Limitazione dei privilegi di accesso: Limitare i privilegi di accesso dei dipendenti e implementare il principio del privilegio minimo per ridurre la superficie di attacco e mitigare gli effetti del malware.

L'ANALISI SEMI-QUANTITATIVA CONFERMA CHE UN ATTACCO INFORMATICO MIRATO AI SERVER INTERNI RAPPRESENTA UN RISCHIO SIGNIFICATIVO PER TECHNOCORP, CON UN PUNTEGGIO DI RISCHIO RESIDUO PARI A 0.6 SU UNA SCALA DA 0 A 10. È FONDAMENTALE IMPLEMENTARE LE MISURE DI MITIGAZIONE IDENTIFICATE PER RIDURRE ULTERIORMENTE QUESTO RISCHIO E PROTEGGERE L'AZIENDA E I SUOI CLIENTI.

Probabilità di accadimento dell'evento:

Alta probabilità: considerando il numero crescente di attacchi informatici e la crescente sofisticazione degli attaccanti, è ragionevole assumere un'alta probabilità di un attacco informatico mirato ai server interni contenenti dati critici. Si stima una probabilità del 70%.

- Impatto finanziario dell'evento:
- Valore dei dati sensibili dei clienti: $50.000.000
- Valore dell'infrastruttura IT e del personale coinvolto: $6.980.000 (somma dei valori quantitativi)
- Possibili costi aggiuntivi per ripristino, perdite operative e multe: stimati in un valore aggiuntivo di $3.000.000
- Considerando l'ampio impatto finanziario potenziale, si stima un impatto medio-alto. Si assegna un punteggio di impatto del 4 su una scala da 1 (basso) a 5 (molto alto).
- Rischio residuo:
- Rischi residui dopo l'attuazione delle misure di mitigazione: la presenza di politiche di sicurezza, firewall, soluzioni di rilevamento e risposta agli incidenti, e formazione del personale può ridurre significativamente la probabilità e l'impatto di un attacco informatico. Si stima una riduzione del rischio del 50% dopo l'attuazione di queste misure.
- Il rischio residuo è quindi il prodotto tra la probabilità residua dell'evento (30%) e l'impatto residuo (2 su 5).
- Rischio residuo = 30% (probabilità residua) * 2 (impatto residuo) = 0.6

- V=30% (Moderate riferimento tabella G-4) I= 0,6% (Very Low riferimento tabella H-3) per il livello finale del nosto analisi del rischio che corrisponde a moderate very low (riferimento tabella I-2)

TABLE G-4: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT RESULTING IN ADVERSE IMPACTS

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	If the threat event is initiated or occurs, it is **almost certain** to have adverse impacts.
High	80-95	8	If the threat event is initiated or occurs, it is **highly likely** to have adverse impacts.
Moderate	21-79	5	If the threat event is initiated or occurs, it is **somewhat likely** to have adverse impacts.
Low	5-20	2	If the threat event is initiated or occurs, it is **unlikely** to have adverse impacts.
Very Low	0-4	0	If the threat event is initiated or occurs, it is **highly unlikely** to have adverse impacts.

TABLE I-2: ASSESSMENT SCALE – LEVEL OF RISK (COMBINATION OF LIKELIHOOD AND IMPACT)

Likelihood (Threat Event Occurs and Results in Adverse Impact)	Level of Impact				
	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

TABLE H-3: ASSESSMENT SCALE – IMPACT OF THREAT EVENTS

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	The threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.
Moderate	21-79	5	The threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
Low	5-20	2	The threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Very Low	0-4	0	The threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.